Appendix

1. Internal documents and communications from the Department of Justice

2. Letter from Chairman Darrell Issa and Subcommittee Chairman Jim Jordan to Attorney General Eric Holder (Jan. 8, 2014)

3. Response Letter from the Department of Justice to Chairman Darrell Issa and Subcommittee Chairman Jim Jordan (Jan. 24, 2014)

4. Letter from Assistant Attorney General Stuart Delery to the American Bankers Association and the Electronic Transaction Association (Jan. 22, 2014)

5. Letter from Representative Blaine Luetkemeyer and thirty Members of Congress to Attorney General Holder and FDIC Chairman Gruenberg (Aug. 22, 2014)

6. Response Letter from the Department of Justice to Representative Blaine Luetkemeyer (Sept. 12, 2013)

7. Submission of the Financial Service Centers of America to the House Committee on Financial Services (Apr. 8, 2014)

Mission Statement for
Consumer Protection Working Group of the
Financial Fraud Enforcement Task Force

Co-Chairs:

Andre Birotte, United States Attorney, CDCA
Tony West, Assistant Attorney General, Civil Division, DOJ
Richard Cordray, Nominee for Director, Consumer Financial Protection Bureau
David Vladeck, Director, Bureau of Consumer Protection, FTC
Lanny Breuer, Assistant Attorney General, Criminal Division, DOJ

Members:

EOUSA, FBI, OCC, USPIS, FDIC, FRB, FinCEN, Treasury, DOEd-OIG, USTP, IRS-CI, NAAG (AG Roy Cooper--NC) and Greg Zoeller--IN), NACHA, and [USSS, NCUA--waiting for confirmation]

Working Group's Purpose and Priorities:

The Consumer Protection Working Group will fill a void of financial fraud cases not currently addressed by the Task Force. Financial fraud targeting consumers can cause billions of dollars in losses, financially cripple some of our most vulnerable consumers, wreak havoc on our economy, and, in some instances, threaten the safety and soundness of financial institutions. In an effort to address this burgeoning problem, this new Working Group will examine a wide variety of areas where consumers may be vulnerable to fraud. Those may include: identity theft, third-party payment processors and other payment fraud, student-consumer fraud, cramming, business opportunity schemes, data privacy, payday lending, counterfeiting, and schemes targeting servicemembers and their families.

Proposed Activities:

Enhance civil and criminal enforcement of consumer fraud through increased information-sharing among law enforcement and member agencies (including use of FBI's LEO system, the FTC's Consumer Sentinel Network system, and others); training and coordination among state and federal law enforcement, including creation and dissemination of a "best practices" tool-kit for DOJ and state AG's offices; and identification of legislative, regulatory, and policy initiatives.
Prevent fraud through public outreach and education, including articles, blogs, webinars, conferences, and media engagement.
Plan and execute national operations targeting specific types of consumer fraud, similar to the Mortgage Fraud Working Group's current initiative focused on foreclosure rescue scams.

From: Goldberg, Richard
Sent: Wednesday, May 23, 2012 12:49 PM
To: Soneji, Sabita J. (CIV); Bresnick, Michael J (ODAG) (JMD); Frimpong, Maame Ewusi-Mensah (CIV); Blume, Michael S.
Subject: RE: CPWG Update

Good afternoon. I spoke with Harris, who is checking into whether he can attend. He does not know whether FTC will pay for him to travel for the meeting and, in the alternative, he is checking to see if a past CLU chief or someone else can address his topic.

Re: my payment processor piece, I was anticipating a discussion of:

1) Cramming
    a. Progress on the cramming front re: voluntary compliance,
    b. FTC's case against BSG,
2) Targeting of third party payment processors,
    a. Reminder: these entities process victim payments through ACH, third party checks, credit cards, etc., despite notice of fraud,
    b. We are collecting a critical mass of agents and prosecutors to work cases,
    c. We are collecting cases with meat on the bones to handle/refer,
3) Money Service Businesses ("MSBs")
    a. Western Union, MoneyGram, Green Dot, and others are facilitating fraud by transmitting victim funds to offenders,
    b. MoneyGram is now under FTC order,
    c. There are isolated incidences of corrupt outlets set up to process payments,
    d. MSBs have information that may be helpful to law enforcement, including ID of recipient,
    e. MSB complaint data coming into Sentinel,
    f. MSBs may be willing to limit funds transmitted to certain countries based upon fraud emanating therefrom.

I have a call into Lois and will ask her if she'd like to put someone up to discuss any one of these topics, including FTC's BSG case or MSBs. Please let me know if these topics are what everyone has in mind. Thanks.

From: Soneji, Sabita J. (CIV)
Sent: Wednesday, May 23, 2012 12:17 PM
To: Bresnick, Michael J (ODAG) (JMD); Frimpong, Maame Ewusi-Mensah (CIV); Blume, Michael S.; Goldberg, Richard
Subject: CPWG Update

Hello CPWG Team –

Just wanted to let you know where things stand on the agenda. I think we are in good shape, but we may need a little more prodding in the coming days to make this come together.
Here are the leads for each part of the meeting:

1:00-1:05pm: Welcome and Introductory Remarks [Mike Bresnick or the Co-Chairs]

1:05-1:50pm: Short Term Priorities and Deliverables Discussion

- Third-Party Payment Processors [Rich Goldberg will take the lead. Joel Sweet is unavailable. Anyone else?]
- Payday Lending [I asked FTC to take the lead on this. Have not heard back yet.]
- Fraud on Servicemembers [Civil and CFPB can take the lead.]

1:50-2:10pm: Outreach Initiatives

- Co-Chair Andre Birotte to discuss recent consumer protection summit in Los Angeles
- FTC to discuss upcoming Common Ground Conference in Chicago [David Vladeck]
- USTP to discuss upcoming consumer protection event in Chicago [Mike Bresnick, Did you confirm Sandra Rasnak will join?]

2:10-2:20pm: Open Discussion/Next Steps

Meeting with Consumer Advocates

2:30-3:00pm: Consumer Advocate Presentation: Payday Lending [Ira Rheingold of NACA will take the lead.]

3:00-3:30pm: Appropriate Matters for Referral to Federal Law Enforcement [Mike Blume and Rich, Can you confirm Harris Senturia of the FTC and someone from Consumer Protection Branch will take the lead?]

Let me know if we have the right point people on these and if you have any additional suggestions.
Thanks!
Sabita

HOMEQ SERVICING

$20.00 Target GiftCard

Expiration Date
01/26/2005

Exclusively For

PHILADELPHIA PA 19144 3725

Please sign and return this reply form with your mortgage payment to get your $20.00 Target GiftCard and to activate your Great Fix privileges [illegible] free [illegible] membership during the [illegible] the low $9 monthly fee, [illegible] I [illegible] to my HomEq Servicing Corporation loan [illegible] for as long as I wish to enjoy the membership benefits [illegible] reported at all times. If I decide for any reason [illegible] Great Fix toll-free, 800-290-8633, to cancel. [illegible] After the free trial period, I may cancel at any time, for any reason [illegible] HomEq to provide Great Fix with my HomEq loan [illegible] additional. By signing below I authorize HomEq to provide Great Fix [illegible] number, name, address, and any other information required to activate my [illegible] benefits. Additionally I authorize the [illegible] HomEq loan.

[illegible]

X [signature]

SIGNATURE REQUIRED FOR PROCESSING

Sign and return this form to claim the
$20.00 Target GiftCard reserved for you
THIS FORM IS NOT REDEEMABLE AT ANY TARGET LOCATION

ZC7615 274349 [illegible] 0216 [illegible] 3 HEB 0303297089

WACHOVIA

P.O. Box 900001
Raleigh, NC 27675-9001

MORTGAGE STATEMENT

ACCOUNT INFORMATION:

Statement Date:	10/05/06
Loan Number:	
Interest Rate:	5.9900
NEXT PAYMENT DUE DATE:	11/01/06
Current Payment:	$949.28
Past Due Payment(s):	
Unpaid Late Charges:	
Other Charges:	
TOTAL AMOUNT DUE:	$949.28
Home Phone #:	(215)

Customer Service Fax: 1-866-260-3962
Customer Service Dept.: 1-866-642-9405

Philadelphia PA 19144-3725

Property Address:

PHILADELPHIA PA 19144

Activity Since Your Last Statement:

Date	Description	Principal	Interest	Escrow	Late Charge	Other	Total
08/01	Payment	$175.59	$764.69			$9.00	$949.28
09/01	Payment	$176.46	$763.82			$9.00	$949.28
10/02	Payment	$177.35	$762.93			$9.00	$949.28

Account Summary:

Loan Balance* As of 10/05/06	Interest Paid Year to Date	Escrow Balance As of 10/05/06	Taxes Paid Year to Date

Commerce Bank, NA
3-100/310

PharmAssist
45 E City Line Avenue PMB 463
Bala Cynwyd, PA 19004

No. 501586

Date: September 15, 2005

Pay to the Order of: [redacted] $ 15.00*

Fifteen Dollars and 00 cents ********** Dollars

MEMO

Carol Soble

⑈501586⑈ ⑆036001808⑆ 36 052225 8⑈ ⑈000001500⑈

Save 10% to 60% on Your Medications!

Save money on Dental Work, Doctor Visits, Extended Care, Chiropractic, Podiatry, Vision & Hearing Care... The list goes on and on!

Save at Pharmacies such as:

ACME
Costco
CVS/pharmacy
Eckerd
Kroger
Medicine Shoppe
Pathmark
Rite Aid
Safeway
TARGET

Plus 48,000 Others Including Independent Pharmacies Nationwide

Dear Roy [redacted],

Are the high costs of Prescription drugs getting to you? Are you tired of all the politicians talking about Prescription Drug savings but doing nothing? Are you tired of having to dig down deep into your wallet to pay for your families' prescription medicines?

Roy, we would like to let you in on a little secret that will allow you to save up to 60 percent on all your prescription drug needs. That's right, up to 60 percent!

Pharm Assist has the answer and would like you to cash the above check and activate the membership that has been reserved in your name. You've read the newspaper articles and seen the news stories on local and national television. Now it's time for you to start taking advantage of the low, low prices Pharm Assist has negotiated with National Pharmacy chains, your local pharmacy, and mail order pharmacies as well.

You'll receive the medications that your Doctor prescribes at your local Pharmacy and Pharm Assist's mail order division will provide you with even BIGGER discounts. Isn't it time you started saving money and stopped listening to the empty promises of politicians? Just present your FHS card at your Pharmacy when you drop off your prescriptions. It's that easy!... Not convinced?

As an extra incentive, we'll provide you with a $500.00 Emergency Cash Certificate* that you never need to pay back! See the back of this form for details.

IMPORTANT: BY CASHING OR DEPOSITING THIS CHECK I AGREE THAT I UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED A ONE TIME SET UP FEE OF $79.95 WHICH WILL INCLUDE THE FIRST MONTHS SERVICE. I ALSO UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED $19.95 PER MONTH COMMENCING APPROXIMATELY 30 DAYS AFTER FULFILLMENT AND EVERY 30 DAYS THEREAFTER ON AN ONGOING BASIS FOR MY MONTHLY MEMBERSHIP FEES. I UNDERSTAND THAT I MAY CANCEL THE FAMILY HEALTH SOLUTIONS MEMBERSHIP AT ANY TIME AND BE ENTITLED TO A REFUND OF THE CURRENT MONTH'S MEMBERSHIP FEE BY CALLING CUSTOMER SERVICE AT 1-888-755-0878. BY DEPOSITING OR CASHING THIS CHECK I AUTHORIZE THESE FEES TO BE DEBITED FROM MY CHECKING ACCOUNT AS OUTLINED ABOVE.

Sincerely yours,

Carol Soble
Director Membership Services

P.S. A limited number of participants have been chosen to receive this offer and you're one of the lucky ones. Cash or deposit your check NOW!

[redacted]
SAVINGS BANK

[redacted]
WYNNEWOOD, PA 19096-2121

2508

Date 11/26/2007

Pay to the Order of Payment Approval Center $ 9.99

nine 99/100 Dollars

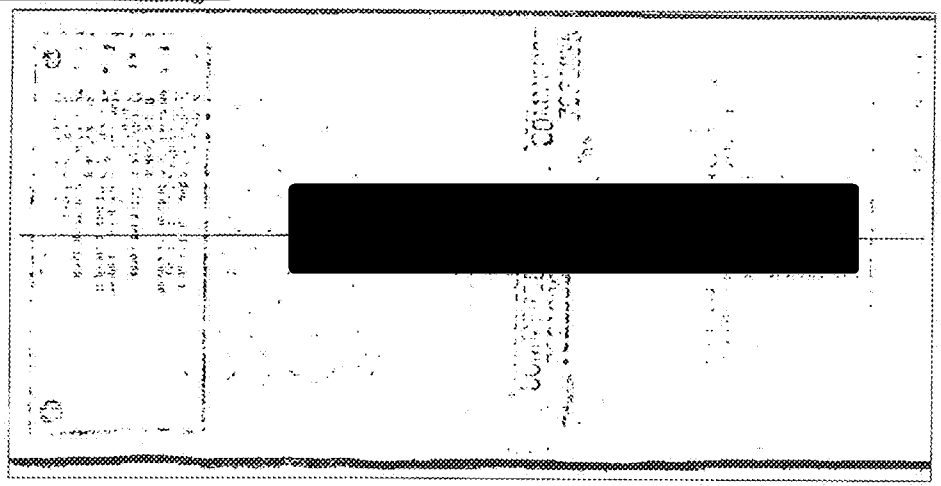
[redacted]

For [redacted]

⑈2360 [redacted]

11/29/2007 2508 $9.99

[redacted]



[redacted]
WYNNEWOOD, PA 19096-2121

2501

Date 11/29/2007

Pay to the Order of Cash Prize Headquarters $ 9.99

nine 99/100 Dollars

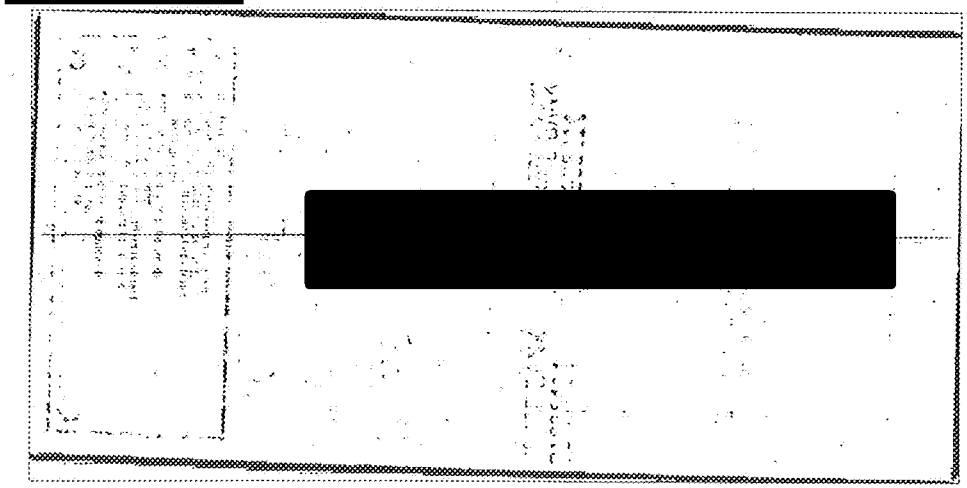
[redacted]

For [redacted]

⑈2360 [redacted]

11/29/2007 2501 $9.99

[redacted]



Prime Time Checking

Account Number: [redacted]
Statement Date: October 31, 2007
Page 1 of 3

[redacted]

- For Customer Service during business hours call **215.864.6730** or e-mail us at **info@BeneficialSavingsBank.com**
- For 24-hour account information call DirectLink at **215.864.1799** or **1.800.784.8490**
- For other information visit us at **www.BeneficialSavings.com**

Account Summary

Previous Statement Balance As Of 09/30/07	1,864.08
Total Withdrawals/Charges	2,625.50
Total Deposits/Credits	2,560.02
Ending Balance	1,798.60

Annual Percentage Yield Earned: 0.50%

Check Summary

Checks Enclosed: 7

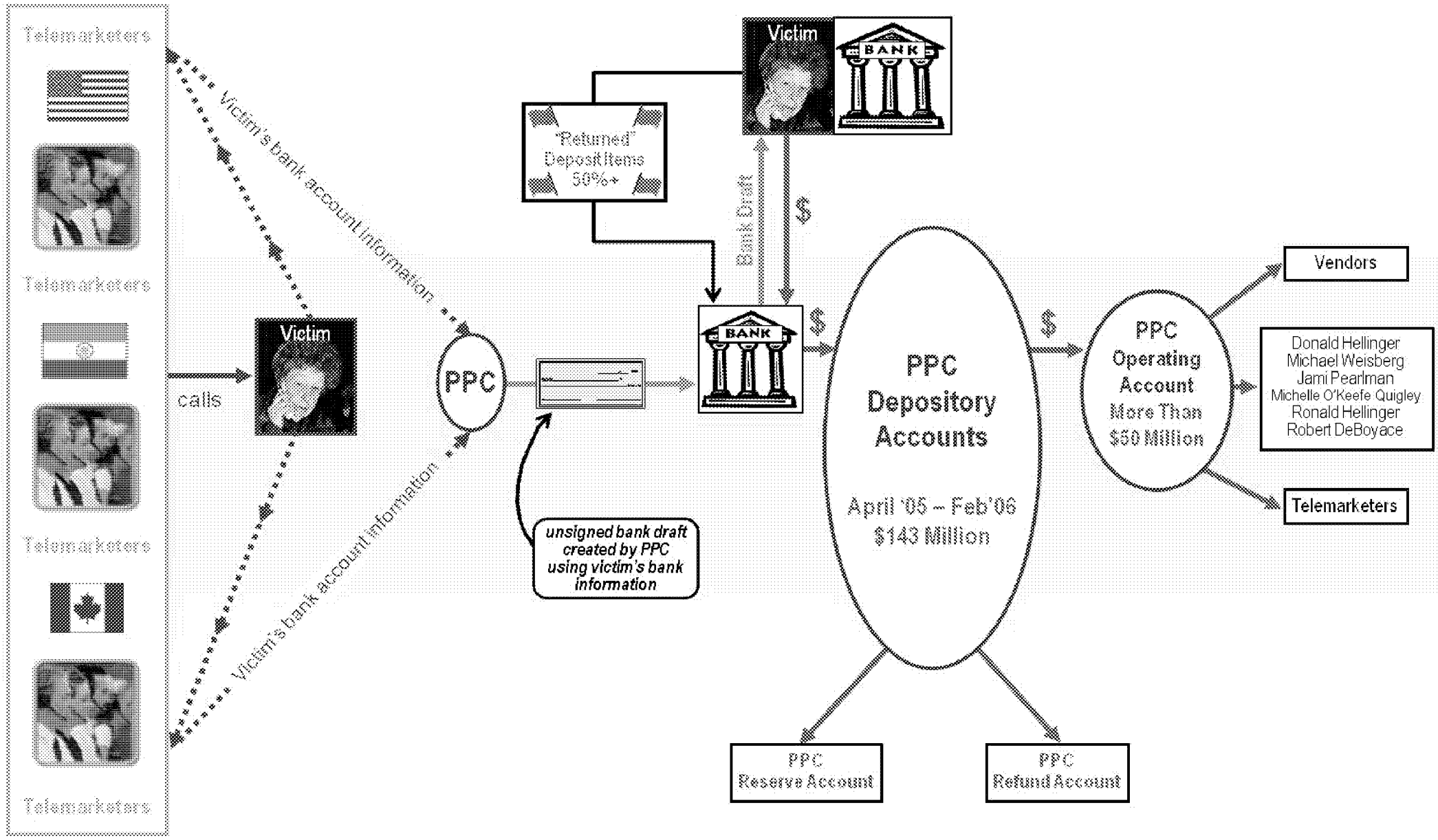
Date	Chk No.	Amount	Date	Chk No.	Amount	Date	Chk No.	Amount
10/01	2439	40.00	10/18	2463	438.50	10/18	2466	237.30
10/10	2463	11.86	10/19	2464	159.46	10/26	2470	8.95
10/24	2460*	10.00						

* Denotes Gap In Check Number Sequence

Other Transactions

Date	Description	Deposit(+) Withdrawal(-)
10/02	Ac-Us Treasury 303 -Soc Sec	568.00+
10/02	Ac-Us Treasury 303 -Soc Sec	1,194.00+
10/02	Ac-Csr -Convcheck Ck-0000000000002444	24.99-
10/02	Ac-Pdd -Convcheck Ck-0000000000002448	27.99-
10/02	Ac-Pnd -Convcheck Ck-0000000000002447	33.99-
10/02	Ac-App -Convcheck Ck-0000000000002448	34.99-
10/03	Ac-Pin -Convcheck Ck-0000000000002445	25.99-
10/05	Ac-Sdrd -Convcheck Ck-0000000000002450	21.99-
10/05	Ac-Dcd Main Office -Convcheck Ck-0000000000002449	24.99-
10/05	Ac-Met Life Ins. Co-Aarpkcod	212.00-
10/05	Ac-Aarp Health Care-Premium	434.52-
10/08	Ac-Chase -Check Pymt Ck-00002456	222.75-
10/10	Ac-Pdd -Convcheck Ck-0000000000002451	29.99-
10/10	Ac-Cpod Main Office-Convcheck Ck-0000000000002462	31.99-
10/12	Deposit	800.00+
10/12	Ac-Reporting Data C-Convcheck Ck-0000000000002454	24.99-
10/12	Ac-Fpr -Convcheck Ck-0000000000002455	27.99-
10/17	Ac-Arrd -Convcheck Ck-0000000000002463	25.99-
10/17	Ac-Ppa -Convcheck Ck-0000000000002452	27.99-
10/17	Ac-Son -Convcheck Ck-0000000000002458	23.99-
10/19	Ac-At&T Consumer -Checkpaymt Ck-00002461	77.66-
10/23	Ac-Rdo -Convcheck Ck-0000000000002467	31.99-
10/23	Ac-Aprd -Convcheck Ck-0000000000002466	13.50-
10/24	Ac-Ss -Convcheck Ck-0000000000002465	28.00-
10/24	Ac-Cpod Main Office-Convcheck Ck-0000000000002469	31.99-
10/26	Ac-Reporting Data Q-Convcheck Ck-0000000000002471	24.99-

[redacted]


Telemarketers
Telemarketers
Telemarketers
Telemarketers
Victim's bank account information
calls
Victim
PPC
Victim
BANK
"Returned" Deposit Items 50%+
Bank Draft
$
BANK
$
unsigned bank draft created by PPC using victim's bank information
PPC Depository Accounts
April '05 – Feb'06
$143 Million
$
PPC Operating Account More Than $50 Million
Vendors
Donald Hellinger
Michael Weisberg
Jami Pearlman
Michelle O'Keefe Quigley
Ronald Hellinger
Robert DeBoyace
Telemarketers
PPC Reserve Account
PPC Refund Account

LMC
RCC

[redacted] Bank [redacted]

Merchant Underwriting Worksheet

Merchant Name: [redacted] Tax ID: 27[redacted] Date: 4/27/2010

Primary Address: [redacted] Evanston, WY 82930 # Of Locations: 1

Underwriting Information

					60-day Avg:
$ Volume Month 1:	$525,000.00		$ Volume Month 2:	$525,000.00	
$ Returns Month 1:	$362,250.00	69.00%	$ Returns Month 2:	$362,250.00	69.00%	69.00%
$ Unath'd Month 1:	$5,250.00	1.00%	$ Unath'd Month 2:	$5,250.00	1.00%	1.00%
# Volume Month 1:	12,000		# Volume Month 2:	12,000	
# Returns Month 1:	8,000	66.67%	# Returns Month 2:	8,000	66.67%	66.67%
# Unath'd Month 1:	120	1.00%	# Unath'd Month 2:	120	1.00%	1.00%

Transaction Information

	Trans	$Volume
Expected Volumes:	12000	$525,000

Per Item Limit: $50

Daily $ Volume Limit: $17,500

Monthly $ Volume Limit: $525,000

Settlement Hold Days: 1

Reserve Required: $0

Reserve Calulation:
0

Deposit Balances:

Hold Period: 2

Avg DDA Balance: $32,200
(divide mo. Sales by 30, less returns)

Minimum Reserve Amt: $0

Total Deposit Amount: $32,200

Fees:

Transaction Fee: $0.25

Return Fee: $1.00

Unauthorized Fee: $2.00

Revenue:

Total Transaction Revenue: $3,000
(Avg Mo Tran * Trans Fee)

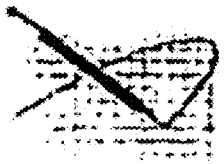
Total Monthl Deposit Revenuee: $81
(Tot Dep Amt * 0.25% Annual)

Return Revenue: $8,240

Total Monthly Revenue: $11,321

Total Annual Revenue: $135,846

Bank Terminated 2/24/11



08/23/2005 06:35 PM

To

cc

Subject Guardian Marketing # 2000027007068

Tom,
Bob, Tim & I need to huddle with you on this account relationship. It is a Business Banking account, it has been actively making deposits since 6/23/05 and there is a current balance of $743,000+ in the account. The account came to us from B of A (so we are advised by in Bus. Bnkg.) and she is monitoring the account. The rub is there has already been 3,430 chargebacks this month and 4,579 since the account "got rolling". 4,579 chargebacks in 2 months. YIKES!!!! Now, the crux of the problem (in case you haven't already guessed) is that ALL their deposits are THIRD PARTY DRAFTS!!! DOUBLE YIKES!!!! Moreover, the drafts that are being deposited and are charging back, are not $99.99; these items are all over the place in terms of their amount. Moreover, there is another account, Suntasia, #2000027027721. Same address, same principals. $ from the Guardian acct is transferred to Suntasia and then the $ is wired out to Bank of America (funny, I thought I said they were leaving B of A at the beginning of this note, didn't I??). And, there is more, but nothing more that I want to put into a note. Bob and I really need to talk o you on tomorrow, 8/24/05. My number is below and Bob's number is

Thanks,

Loss Management
954-788-

From: Delery, Stuart F. (CIV)
Sent: Wednesday, October 17, 2012 6:03 PM
To: Bresnick, Michael J (ODAG) (JMD); Olin, Jonathan F. (CIV); Blume, Michael S.; Goldberg, Richard
Subject: RE: payment processors

Follow Up Flag: Follow up
Flag Status: Completed

Thanks, Mike.

From: Bresnick, Michael J (ODAG) (JMD)
Sent: Wednesday, October 17, 2012 5:28 PM
To: Delery, Stuart F. (CIV); Olin, Jonathan F. (CIV); Blume, Michael S.; Goldberg, Richard
Subject: payment processors

Stuart,

I understand that you're going to the Philly USAO next week. I wanted to let you know about a great case that Joel Sweet, an AUSA in the Civil Division there, is close to resolving. It involves the expected filing of FIRREA charges, with a related consent decree, against the First Bank of Delaware, resulting from the bank's business relationship with several unscrupulous third party payment processors. The $15M penalty, I understand, is one of the largest ever to be paid under FIRREA. Joel, who also criminally prosecuted several individuals associated with a fraudulent payment processor earlier this year and was involved in the DPA against Wachovia (which agreed to pay $160M for, among other things, failing to have proper AML procedures to guard against fraudulent processors), is somewhat of an expert in the area. He also has spoken to Mike Blume, Rich Goldberg, and me about possibly coordinating an effort to investigate more banks for potential FIRREA violations resulting from their relationships with processors. Since this is a priority of the Consumer Protection Working Group, I thought you might be interested in knowing about it. Please let me know if you have any questions.

Thanks,
Mike

From: Olin, Jonathan F. (CIV)
Sent: Wednesday, October 17, 2012 6:51 PM
To: Bresnick, Michael J (ODAG) (JMD)
Subject: RE: payment processors

Thanks Mike. Can I give you a call tomorrow afternoon?

From: Bresnick, Michael J (ODAG) (JMD)
Sent: Wednesday, October 17, 2012 5:28 PM
To: Delery, Stuart F. (CIV); Olin, Jonathan F. (CIV); Blume, Michael S.; Goldberg, Richard
Subject: payment processors

Stuart,

I understand that you're going to the Philly USAO next week. I wanted to let you know about a great case that Joel Sweet, an AUSA in the Civil Division there, is close to resolving. It involves the expected filing of FIRREA charges, with a related consent decree, against the First Bank of Delaware, resulting from the bank's business relationship with several unscrupulous third party payment processors. The $15M penalty, I understand, is one of the largest ever to be paid under FIRREA. Joel, who also criminally prosecuted several individuals associated with a fraudulent payment processor earlier this year and was involved in the DPA against Wachovia (which agreed to pay $160M for, among other things, failing to have proper AML procedures to guard against fraudulent processors), is somewhat of an expert in the area. He also has spoken to Mike Blume, Rich Goldberg, and me about possibly coordinating an effort to investigate more banks for potential FIRREA violations resulting from their relationships with processors. Since this is a priority of the Consumer Protection Working Group, I thought you might be interested in knowing about it. Please let me know if you have any questions.

Thanks,
Mike

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Monday, November 05, 2012 4:09 PM
To: Delery, Stuart F. (CIV)
Cc: Olin, Jonathan F. (CIV)
Subject: Proposal for Detail
Attachments: Operation Choke Point (2).pdf.pdf

Hi Stuart –

I understand you have already spoken to Joel Sweet about his proposal to be detailed to the Consumer Protection Branch to bring a number of actions concerning third-party payment processors. Please see his proposal attached. (I have also sent it up for approval through the normal process with a cover from Mike through me.)

I (and Mike) are happy to discuss at your convenience. Given the importance of the third-party payment processors work to much of what we do at the Consumer Protection Branch, given that it is one of the high-priority areas of the CPWG, and given the great experiences we have had working with Joel in this area, I wholeheartedly support the proposal. Thank you for considering it.

Regards,
Maame

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

UNITED STATES DEPARTMENT OF JUSTICE - CIVIL DIVISION NOV-05-2012
CORRESPONDENCE TRACKING SYSTEM
COVER SHEET

CIVIL NO:	167662	DOCUMENT TYPE:	PERS	DATE RECEIVED:	NOV-05-2012
FILECODE:	OCL	DOCUMENT DATE:	NOV-02-2012	RESPONSE DUE:	ASAP
XREF:		RESPONDING UNIT:	CONS	DATE CLOSED:	FYI
REVIEWER:	Michael S. Blume				
DRAFTER:				CIVIL DUE DATE:	
EXSEC NO:				SG DUE DATE:	

TO: Stuart F. Delery, A/AAG, Civil Division

FROM: Michael S. Blume, Director, Consumer Protection Branch

SUBJECT: Proposed Detail of Assistant United States Attorney Joel Sweet, of the Eastern District of Pennsylvania, to the Consumer Protection Branch

COMMENTS: Maame Ewusi-Mensah Frimpong: Review and initial (information only)
Stuart F. Delery: Review and initial Memorandum (information only)

ACTIONS: ASSIGNED TO		DATE ASSIGNED	DATE FINISHED
Maame Ewusi-Mensah Frimpong		NOV-05-2012	5 Nov 2012
Stuart F. Delery	SFD	NOV 5 2012	1/10/13
[redacted]		JAN 11 2013	JAN 11 2013
Michael S. Blume		JAN 11 2013	

COMMENTS: Stuart – I recommend that you approve moving forward on this proposal to detail an AUSA to the Consumer Protection Branch to lead a targeted operation concerning third party payment processors. As you know, this is one of the CPWG's priority areas & Rich has been doing a superb job in this area even before formation of the CPWG. It seems though that given where we are in the development of this work, & the growing momentum around it, now is the right time to design and execute a specific operation. Joel is the perfect person to do this & Mike & Rich fully support this. It is a way to augment capacity efficiently within existing resources

U.S. Department of Justice

Civil Division

Washington, DC 20530

NOV 2 2012

MEMORANDUM

TO: Stuart F. Delery
Acting Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: Proposed Detail of Assistant United States Attorney Joel Sweet, of the Eastern District of Pennsylvania, to the Consumer Protection Branch

Attached is a thoughtful proposal from Assistant United States Attorney Joel Sweet, of the Eastern District of Pennsylvania, for a detail to the Consumer Protection Branch. Joel's proposal, which speaks for itself, would create an opportunity for the Branch to initiate cases involving banks that enable payment processors and their merchant clients to facilitate fraudulent transactions. The proposal offers important advantages to the Branch, including: (1) a focused, singular attention on an important area of enforcement in its germinal stages; (2) building capacity within the Branch to expand our reach into financial fraud; and (3) strengthening the Branch's relationship with banking regulators and other agencies that address financial fraud.

I have worked with Joel on payment processing cases. So, too, has Assistant Director Richard Goldberg. Joel is an expert in the field, one of the few (if the only) such experts in the United States Attorney community. (Rich is similarly expert in this area.)

Joel is enthusiastic and aggressive—in a measured way. I would welcome the opportunity to have him detailed to the Branch.

Memorandum

Subject	**OPERATION CHOKE POINT**: A proposal to reduce dramatically mass market consumer fraud within 180 days	Date	November 5, 2012
To	Stuart F. Delery Acting Assistant Attorney General Civil Division	From	Joel M. Sweet Assistant United States Attorney

OPERATION CHOKE POINT

I propose that I be detailed to the Consumer Protection Branch to implement a strategy to attack Internet, telemarketing, mail, and other mass market fraud against consumers, by choking fraudsters' access to the banking system. This objective can be achieved promptly and efficiently through a proven strategy of incremental enforcement, which will:

- achieve results within months;
- provide prospective protection to the most vulnerable of victims;
- efficiently use resources;
- attract multi-agency support and cooperation (already pledged);
- promote a culture of compliance among banks regarding Bank Secrecy Act/Anti-Money Laundering obligations;
- provide groundwork for civil and criminal prosecutions against banks, payment processors, and fraudsters; and
- recover FIRREA penalties.

This proposal will substantially further the goals of the Consumer Protection Working Group of the Financial Fraud Enforcement Task Force, which has prioritized addressing third-party payment processor involvement in consumer fraud.

The Problem

Fraudulent merchants are able to take money from their victims' bank accounts only if they have a relationship with a bank, and thus access to the nation's banking system. Banks are reluctant to establish direct relationships with such merchants due to significant legal, financial, and reputational risks. To overcome this obstacle, fraudulent merchants create *indirect* relationships with banks through third-party payment processors. In many cases, these processors are unlicensed, unregulated, and owned or controlled by the fraudulent merchants. By using processors as conduits to gain access to the banking system, fraudulent merchants can evade and frustrate statutes and regulations designed to require banks to know their clients, and to prevent their clients from using the banking system to further criminal activity.

Consumers continue to endure substantial harm from fraudulent merchants who can operate only through third-party payment processors. I learned while civilly and criminally prosecuting a payment processor and its bank, namely Payment Processing Center, LLC, and Wachovia, N.A., that a single bank servicing only a few processors can result in a staggering number of fraud-tainted transactions in a short period. In that case, Wachovia Bank originated transactions for four payment processors and caused $162 million in consumer losses in an 18-month period. We believe that the Wachovia prosecution caused many larger banks to closely evaluate third-party processor risk, and that much of the illegal conduct may have migrated to smaller banks. This is supported by my experience prosecuting First Bank of Delaware (a FIRREA action anticipated to be resolved within days), where a small bank in Philadelphia originated transactions for five third-party payment processors and facilitated more than $150 million in suspected consumer losses during a 12-month period.[1] While we do not know the number of banks involved in this activity, we know that mass market consumer fraud continues, and that most victim losses pass through a bank. Operation Choke Point will powerfully affect the entire banking industry and will further limit fraudsters' ability to access consumers' bank accounts.

The government's efforts to address third-party payment processor-related consumer fraud would benefit substantially from a vertical investigation model, as well as greater and more intensive coordination with other agencies engaged in the fight against consumer fraud. For example, presently the FTC focuses its attention primarily on fraudulent merchants and processors. The FTC's considerable efforts are hampered, however, by inadequate civil injunctive remedies and by creative defendants who rapidly change corporate identifies so that they can continue to prey upon consumers. Bank regulators have begun to address third-party payment processor risk. But a regulatory examination approach is not intended or designed to identify and address consumer fraud. DOJ has not targeted fraudulent merchants and processors criminally (I suspect due to challenges that I am available to discuss with you), and there have been few civil actions in this area. By extending our investigations to include the fraudulent merchant, the payment processor, and the bank, and by focusing our efforts on choking off the flow of money to the fraudulent merchants, we can overcome existing limitations.

The Solution

In a short time and with relatively few resources, we can disrupt fraud-tainted payment channels and protect consumers from future harm by identifying banks with problematic third-party payment processor relationships. Banks are sensitive to the risk of civil/criminal liability and regulatory action. Where we have evidence that a bank is processing payments for fraudulent merchants, we can communicate with the bank – for example, by sending a letter to a

[1] In addition to consumer fraud, third-party payment processors pose a Bank Secrecy Act/Anti-Money Laundering risk. I am aware of a bank that transferred hundreds of millions of dollars to and from the United States and foreign countries though accounts of suspicious third-payment payment processors.

senior bank executive inquiring whether the bank is aware of its merchants' return rates (a red flag of potential fraud), or by serving a FIRREA subpoena for data concerning a suspected processor or merchant. If prior experience is a guide, we can expect the bank to scrutinize immediately its relationships with third-party payment processors and fraudulent merchants and, if appropriate, to take necessary action (which may include restitution to victims). Legitimate banks will become aware of perhaps unrecognized risk, and corrupt banks will be exposed. This approach can yield almost immediate prospective protection of the public at an extremely low cost. If we find a bank or processor that knew, or turned a blind eye, toward fraudulent transactions, my experience could be brought to bear to initiate legal action.

Eliminating even one bank's fraud-tainted payment channel can prevent hundreds of fraudulent merchants from accessing the bank accounts of hundreds of thousands of consumers. Moreover, by approaching a bank at the outset of an investigation with an opportunity to self-evaluate processor relationships and to cooperate with the government, we can obtain evidence without relinquishing potential civil and criminal prosecution opportunities. Depending on the evidence, banks may be subject to civil FIRREA claims (for civil money penalties) and criminal Bank Secrecy Act and/or wire fraud charges. Third-party payment processors may be subject to the same, as well as criminal charges for bank fraud and/or operating an illegal money transmission business.[2]

As further described below, I propose that we identify and engage ten suspect banks within 150 days. This alone is likely to cause banks to scrutinize their account relationships and, if warranted, to terminate fraud-tainted processors and merchants. Assuming cooperation of USAOs and our other partners, in 180 days we can dramatically curtail consumer fraud across the nation by choking the fraudulent merchants' ability to access victims' bank accounts. Moreover, our efforts will positively sensitize the banking industry to third-party payment processor risks.

DOJ, through the Consumer Protection Branch, should take the lead in implementing this strategy. Partner agencies should include the FTC, FDIC, OCC, FinCEN (Treasury), Federal Reserve Banks, NAAG, CFPB, FBI, and USPIS – all of which are members of the President's Financial Fraud Enforcement Task Force, most of which have been my partners in past efforts, and several of which already support this proposal. We can reasonably expect partner agencies to provide investigative resources to the effort. For example, the FBI already has offered staff to review SARS for references to third-party payment processors. FinCEN has an agent willing to set up and maintain a LEO database. The FTC already works closely with me and others to identify banks that are processing fraud-tainted transactions. Likewise, I am engaged in a

---

[2] Disrupting payment relationships between banks and fraudulent merchants provides immediate benefits to the public, and captures evidence that can be used to prosecute cases. In some case, where a conventional approach is preferred, we might request that a bank keep particular accounts open for investigative purposes. While that option always will remain available, it is not part of the strategy I am proposing because of the substantial time and investment of agent resources required.

productive discussion with the Federal Reserve Bank (Atlanta) to identify banks originating transactions for suspected fraudulent merchants.

Execution Time Line

We can achieve our objectives within this time frame:

60 days — Identify ten (10) target banks by analyzing return rate data, flow of money from victims' accounts to fraudster accounts, and SAR review; create a Law Enforcement On-line (FBI) database to map relationships among fraudulent merchants (beneficial owners and trade names), third-party payment processors, and banks (FinCEN).

120 days — After identifying target banks, reach out to USAOs in the jurisdictions of the banks and offer training to promote and support investigations. Training to include overview of: (1) mass marketing fraud schemes and payment systems; (2) relevant civil and criminal statutes (Anti-Injunction Statute, 18 U.S.C. § 1345; FIRREA, 31 U.S.C. § 1833a; Operating an Illegal Money Transmission Business, 18 U.S.C. § 1960; etc.); (3) regulatory guidance; (4) available investigative resources; (5) templates for subpoenas, complaints, settlement agreements, etc.

150 days — Engage banks identified as having problematic practices: (1) to request opportunity to discuss banks' relationships with processors and/or fraudulent merchants; (2) request voluntary production of documents; or (3) if appropriate, to serve FIRREA subpoenas. Provide banks with existing regulatory guidance on processors (FDIC, FinCEN, OCC).

180 days — For the 10 target banks, based on investigative results, decide whether to negotiate a prospective compliance agreement, file a FIRREA complaint, open a GJ investigation, or close the file; assess status of prosecutions (civil/criminal) against third-party payment processors and fraudulent merchants.

Detail to the Consumer Branch

I propose that I be detailed to the Consumer Protection Branch to implement this strategy. The Consumer Protection Branch has existing expertise to address third-party payment processors, as well as the capability to attack these schemes with both civil and criminal tools. I have been working with the Consumer Protection Branch, in particular with Assistant Director Richard Goldberg, to advance the Department's efforts at attacking unscrupulous payment processors. The Consumer Protection Branch lacks, however, an available prosecutor with the necessary experience, knowledge, and professional relationships who can dedicate himself/herself full time to this intensive effort. Michael Blume, Director of the Consumer

Protection Branch, is supportive of the strategy described above, and of my detail to the Consumer Protection Branch for this purpose.

I am qualified and well-suited to lead this effort. During nine years as an AUSA, I have led successful civil and criminal prosecutions of third-party payment processors and banks, including: (1) United States v. First Bank of Delaware (anticipated to be filed within days in the E.D. Pa.) (FIRREA action anticipated to result in $15 million CMP); (2) United States v. Hellinger, et al., Criminal Action No. 11-0083 (E.D. Pa.) (successful criminal prosecution under 18 U.S.C. § 1960 of six owners of a payment processor); (3) United States v. $2,562,618 in U.S. Currency, Civil Action No. 09-1603 (E.D. Pa.) (forfeiture action against $2.7 million in Internet gambling proceeds retained by third-party payment processor); (4) United States v. Wachovia Bank, N.A., 10-20165 (S.D. Fla.) (BSA charge resolved with deferred prosecution agreement in conjunction with DOJ's Asset Forfeiture Money Laundering Section and another USAO); and (5) United States v. Payment Processing Center, Civil Action No. 06-0725 (E.D. Pa.) (anti-fraud injunction against third-party processor under 18 U.S.C. § 1345, leading to $160 million in victim restitution). See also Faloney v. Wachovia Bank, N.A., 254 F.R.D. 204, 216 (E.D. Pa. 2008) (district court decision crediting class action plaintiffs' success, in part, to evidence uncovered during "Assistant United States [Attorney] Sweet's dogged pursuit of PPC, Wachovia, and the telemarketing industry.")

Currently, my open matters include civil and criminal investigations of banks and processors. I confer regularly with government attorneys and agents on consumer fraud issues. Moreover, I have close working relationships with our partner agencies, including the FTC, FDIC, and FinCEN. I lecture several times each year at the Financial Crimes Seminar of the Federal Financial Institutions Examination Council, where state and federal bank examiners learn about consumer fraud and risks posed by third-party payment processors.

I am prepared to accept a detail to the Consumer Protection Branch to implement this strategy. I am available at your convenience to discuss this matter further.

cc: Gary Grindler, Chief of Staff to the Attorney General
Michael Bresnick, Executive Director, Financial Fraud Enforcement Task Force
Michael S. Blume, Director, Consumer Protection Branch

From: USDOJ-Office of Public Affairs (SMO) (JMD)
Sent: Monday, November 19, 2012 2:35 PM
To: USDOJ-Office of Public Affairs (SMO) (JMD)
Subject: DEPARTMENT OF JUSTICE ANNOUNCES $15 MILLION SETTLEMENT WITH DELAWARE BANK ACCUSED OF CONSUMER FRAUD

Department of Justice

United States Attorney Zane David Memeger
Eastern District of Pennsylvania

FOR IMMEDIATE RELEASE
MONDAY, NOVEMBER 19, 2012
WWW.JUSTICE.GOV/USAO/PAE

CONTACT: PATTY HARTMAN
215-861-8525

DEPARTMENT OF JUSTICE ANNOUNCES $15 MILLION SETTLEMENT WITH DELAWARE BANK ACCUSED OF CONSUMER FRAUD

PHILADELPHIA – First Bank of Delaware today was charged with, and settled, civil claims brought by the U.S. Department of Justice in connection with a scheme to defraud consumers through the Internet and other means. Under a settlement reached with First Bank of Delaware, the bank will pay a civil money penalty of $15 million to the U.S. Treasury. The bank also will maintain an account with $500,000 to pay consumer claims arising from the alleged conduct. Today's settlement and related regulatory actions were announced by U.S. Attorney for the Eastern District of Pennsylvania Zane David Memeger, Department of the Treasury Financial Crime Enforcement Network (FinCEN) Director Jennifer Shasky Calvery and the Federal Deposit Insurance Corporation (FDIC). The Department of Justice's allegations against the bank and the terms of that settlement are set forth in a civil complaint and a settlement agreement filed in the U.S. District Court for the Eastern District of Pennsylvania.

The Department of Justice alleges that from 2009 to 2011, First Bank of Delaware violated the Financial Institutions Reform, Recovery and Enforcement Act (FIRREA) by originating withdrawal transactions on behalf of fraudulent merchants and causing money to be taken from the bank accounts of consumer victims. The government alleges that the bank knew – or turned a blind eye to the fact – that consumer authorization for the withdrawals had been obtained by fraud.

"We are committed to protecting consumers from unscrupulous merchants who use Internet and telemarketing schemes to defraud them. Such merchants need payment processors and banks to help them obtain the victim consumers' money. This settlement should serve as notice to the banking community that when banks allow themselves to be used to perpetrate these frauds, we will target our enforcement efforts accordingly to hold the banks accountable," stated U.S. Attorney Memeger.

"To make money, First Bank of Delaware entered into risky lines of business and chose to disregard its Bank Secrecy Act (BSA) responsibilities," said FinCEN Director Jennifer Shasky Calvery. "As a result of its

failure to implement systems and controls to identify and report suspicious activities, as required by the BSA, financial predators were able to victimize consumers."

Banks are a critical key in many consumer fraud schemes. After a fraudster obtains bank account information from a consumer, the fraudster still needs to gain access to the banking system in order to take the consumer's money. Fraudulent merchants have a difficult time opening their own bank accounts because of laws designed to prevent criminals from accessing the banking system. To overcome this obstacle, fraudulent merchants often obtain indirect access to the banking system through a third-party payment processor that can more easily establish a relationship with a bank.

The Department of Justice alleges that First Bank of Delaware established direct relationships with several fraudulent merchants and third-party payment processors working in cahoots with a large number of additional fraudulent merchants. On behalf of the processors and fraudulent merchants, First Bank of Delaware originated hundreds of thousands of debit transactions against consumers' bank accounts. The payment processors named in the complaint include Automated Electronic Checking Inc., Check Site Inc., Check 21.com LLC and Landmark Clearing, Inc.

First Bank of Delaware originated many of the debit transactions using "remotely-created checks" – a transaction instrument widely-known in the banking industry and by the consumer protection and law enforcement community to be favored by fraudulent merchants. At the time of the conduct alleged, First Bank of Delaware and the rest of the banking industry were well-aware of the consumer fraud risks posed by third-party processors and remotely-created checks. The Department of Justice alleges that First Bank of Delaware was aware of significant red flags warning the bank that the debit transactions were tainted by fraud. For example, First Bank of Delaware ignored high rates of returned or charged-back debit transactions. This is a significant fraud indicator about which federal bank regulators have consistently warned the banking industry. First Bank of Delaware's third-party payment processors had aggregate return rates for remotely-created checks exceeding 50 percent during the period 2009 to 2011, compared to the average return rate of one-half of one percent for all checks processed by the Federal Reserve. Where a high number of purportedly legitimate transactions are rejected by consumers and their banks, it is likely that consumers are being defrauded.

Congress enacted FIRREA in 1989 as part of a comprehensive legislative plan to reform and strengthen the banking system and the federal deposit insurance system that protects the public from bank failures. FIRREA provides that the United States may recover civil penalties of up to $1 million per violation of certain criminal statutes, or, for a continuing violation, up to $1 million per day or $5 million, whichever is less. The statute further provides that the penalty can exceed these limits to permit the United States to recover the amount of any gain to the violator, or the amount of the loss to victims, up to the amount of the gain or loss. The Department of Justice alleges that First Bank of Delaware engaged in wire fraud affecting federally-insured financial institutions by originating debit transactions for third-party payment processors and fraudulent merchants who the bank knew were engaged in fraud against consumers, or that the bank remained willfully blind to that fact.

Under the settlement reached between the Department of Justice and First Bank of Delaware, the bank will pay a $15 million penalty to the U.S. Treasury. The payment also satisfies penalties imposed upon the bank by the FDIC and FinCEN, each of which has entered into a separate agreement with the bank relating to Bank Secrecy Act violations. The bank also will maintain an account with $500,000 to pay consumer claims for losses arising from the conduct alleged in the complaint. Any money remaining in the restitution account after all consumer claims have been paid will be transferred to the U.S. Treasury.

The case was investigated and prosecuted for the Department of Justice by Assistant U.S. Attorneys Joel M. Sweet, Susan Dein Bricklin and Judith A. Amorosa, and U.S. Attorney's Office Auditor Allison Barnes, in coordination with the FDIC and FinCEN.

Today's announcement is part of efforts by the Consumer Protection Working Group of President Obama's Financial Fraud Enforcement Task Force, which was established to wage an aggressive, coordinated and proactive effort to investigate and prosecute financial crimes. The Consumer Protection Working Group brings together federal, state, and local law enforcement agencies, regulators, and other stakeholders to protect consumers from fraud that can devastate victims and cause widespread economic harm. Consumer fraud comes in many forms and can be found in fraud on our nation's service members, payday lending, high-pressure telemarketing schemes, internet scams, business opportunity scams, and unscrupulous third party payment processors. Scam artists often target vulnerable populations such as the elderly, students, the unemployed, and those already struggling with debt. Through this partnership, the Consumer Protection Working Group is working to strengthen consumer protection efforts, leverage resources, enhance civil and criminal enforcement of consumer fraud, and educate the public in an effort to prevent consumers from being victimized. To learn more about the President's Financial Fraud Enforcement Task Force, please visit www.stopfraud.gov.

# # #

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Thursday, November 29, 2012 3:12 PM
To: Delery, Stuart F. (CIV)
Cc: Olin, Jonathan F. (CIV)
Subject: Joel Sweet TPs
Attachments: Talking Points for Call with ZM 11.26.12.docx

Follow Up Flag: Follow up
Flag Status: Completed

Hi Stuart –

Here are the draft Talking Points for the call with Joel Sweet that I gave you Monday. Let me know if you have any questions or need anything further before you call the US Attorney.

Thanks!

Regards,
Maame

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

Talking Points for AAG Call with U.S. Attorney Zane D. Memeger (EDPA) re Third Party Payment Processors Detail

Draft 11.26.12

Introduction

- As you know, we have been very involved with the Financial Fraud Enforcement Task Force, and have been largely leading the Consumer Protection Working Group.
- The Working Group has three priority areas for its near term focus, and I wanted to approach you about a partnership between CIV and EDPA on one of those priority areas, namely third-party payment processors.
- Specifically, I wanted to explore with you the possibility of doing a detail with Joel Sweet from your office to work with the Consumer Protection Branch to do a concentrated enforcement effort to address the problem of banks who allow payment processors to use them to enable fraud.
- We have done great work with Joel, and he has been a real asset on this issue and in this working group, and it would be great to work more intensely with your office on this.

Background/Context on the Third Party Payment Processors Issue

- Fraudsters and their enablers exploit holes in the electronic payment system
  - Doing so allows for massive frauds at low costs
- Dealing with that problem must be a national priority of the government
  - It is one of three priorities of the Consumer Protection Working Group
  - It is a priority of the FTC, FDIC, FRB, FinCEN, and others
- We need to step up enforcement in this area
- Civil and criminal prosecutions of players exploiting the electronic payments systems are complex
  - We need a focused attention on the cases
- We need to develop expertise

Philadelphia's Leadership in These Cases

- Philadelphia has been on the cutting edge in DOJ of addressing players in the financial system who exploit holes in the electronic payment system to benefit fraudsters
  - The USAO brought criminal charges against individuals who processed payments for gamblers
  - The USAO shut down a payment processor that enabled telemarketing fraudsters to take money from consumers' bank accounts
  - The USAO helped broker a settlement with Wachovia, worth upwards of $160 million, for its role in allowing a payment processor to use its bank to help fraudsters
    - The Wachovia settlement changed the way major banks deal with payment processors

- The USAO shut down a bank and obtained a $15 million penalty for the bank's role in allowing fraudulent payment processors to operate

Specifics of the Proposal

- Joel Sweet would be detailed to the Consumer Protection Branch to work with Rich Goldberg and others in the Branch for a period of 6-9 months.
- In that period of time, the team would identify several target banks, provide training and support to USAOs interested in opening investigations, and engage banks either for purposes of filing FIRREA complaint or negotiating some acceptable resolution.

Positive Features of the Proposal

- Joel and Rich are experts in this, and will build upon that expertise, existing contacts (especially with the financial regulators), and ongoing work.
- Joel has already been working with Rich and Mike Bresnick and Mike Blume in this area.
- The proposal will build capacity at DOJ -- at the USAO in Philadelphia and CPB in Washington
  - It will firmly place Philadelphia in the lead of this effort
  - It will allow Philadelphia to create a model for enforcement in this area
    - Philadelphia can then "spread the word"
- We imagine that as many cases as appropriate would go back to Philadelphia.

UNITED STATES DEPARTMENT OF JUSTICE - CIVIL DIVISION

CORRESPONDENCE TRACKING SYSTEM

Cover Sheet Date: 2/8/2013

ID:	**66780**	Document Date:	**02/08/2013**
Document Type:	**Subpoenas**	Date Received:	**02/08/2013**
File Code:	**Office of Consumer Litigation**		**At Earliest Convenience**
Responding Unit:	**Office of Consumer Litigation**	Response Due:	**02/15/2013**
Reviewer:	**Michael S. Blume**	Date Closed:	
Drafter:	**Richard Goldberg**	Civil Due Date:	
Executive Sec #		SG Due Date:	

TO: **Stuart F. Delery, PDAAG, Civil Division**

FROM: **Michael S. Blume, Director, CPB; thru: Maame Ewusi-Mensah Frimpong, DAAG**

Subject: **Payment Processor Investigation -- Request for Issurance of Subpoenas to Payment Processors and Banks used to Process Fraudulent Payments**

Comments: *Maame Ewusi-Mensah Frimpong: Review, comment, initial Memorandum*
Stuart F. Delery: Sign subpoenas [redacted]
Requesting approval by February 15, 2013. There are no external deadlines.

Actions:

Assigned To	Initials	Date Assigned	Finished
Maame Ewusi-Mensah Frimpong		**02/08/2013**	14 Feb 2013
Stuart F. Delery	SFD	FEB 14 2013	2/15/13
[redacted]		FEB 15	
Michael S. Blume			

NOTES

Stuart – I recommend you authorize the issuance of the attached FIRREA subpoenas as the first step in the Third Party Payment Processors Initiative. The parties we have identified appear to be doing business with fraudulent entities & should have good information on their dealings with them. This will likely show whether they have been intentionally aiding the fraudulent entities, deliberately ignorant, or neither.

U.S. Department of Justice

Civil Division

Washington, DC 20530

February 8, 2013

TO: Stuart F. Delery
Principal Deputy Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: Payment Processor Investigation -- Request for Issuance of Subpoenas to Payment Processors and Banks used to Process Fraudulent Payments

Time Frame

We request your approval by February 15, 2013. There are no external deadlines.

Recommendation

We seek authorization to issue subpoenas under the Financial Institutions Reform, Recovery and Enforcement Act of 1989, 12 U.S.C. § 1833a(g)(1)(C) ("FIRREA"). The subpoenas would be directed to seven entities described further below.

Case Summary

We are launching Operation Choke Point—a multi-agency effort to combat mass market consumer fraud by focusing on payment systems. The Payment Processor Working Group of the Financial Fraud Enforcement Task Force held several meetings over the past few weeks with the purpose of planning investigations of the payment processing industry. We have assembled a team composed of the Consumer Protection Branch and its forthcoming detailee, AUSA Joel Sweet; the Postal Inspection Service; the FBI; the Federal Trade Commission; and other agencies (including bank regulators) with jurisdiction over entities that help fraudulent merchants to take money from consumers. The group of investigations will focus on payment processors that are known to have helped fraudulent merchants and the banks that have provided accounts to those

processors and merchants. As discussed below, the requested FIRREA subpoenas seek information from those institutions.[1]

Discussion

Fraudulent Internet merchants and telemarketers frequently mask their identities by employing a variety of short-lived business names, by incorporating off-shore, and by selling a large number of different, constantly changing products. These techniques impose significant investigative obstacles for law enforcement by making it more difficult to identify the merchant responsible for a particular consumer complaint and to determine the scope of injury caused by the merchant. The requested subpoenas are designed to surmount these hurdles by giving us information about fraudulent sellers as well as the payment processors and banks that provide them with crucial assistance.

In order to have access to consumers' checking accounts, fraudulent merchants open merchant accounts with payment processors. The processors typically require their merchant clients to provide copies of their sales scripts, information on the merchants' principals, financial information, the consumer bank account numbers to be debited, and the amounts of the requested debits. In the course of business, the processors calculate the "return rate" for each merchant, in order to charge the merchants for items returned through the check clearing system. The "return rate" refers to the percentage of attempted debit transactions that are returned out of the total number of attempted debits. In general, a high return rate incurred by a single merchant commonly indicates the presence of deceptive or fraudulent practices, because either the consumer never authorized the debit or the consumer authorized the debit, but the authorization was based on deceptive representations or omissions that the consumer later discovers. In sum, payment processing firms possess useful information that can assist in establishing the identity of fraudulent merchants and the scope of the merchants' fraud.

In recent years, fraudulent merchants have increasingly turned to the fraudulent use of remotely created checks (RCCs) and an electronic version of RCCs, referred to herein as a "remotely created payment order" ("RCPO"), as the preferred payment mechanisms for debiting consumers' bank accounts. RCPOs are often referred to as "electronic payment orders," "non-check echecks," or "electronic RCCs."

An RCC is an unsigned paper check, or demand draft, that is created by the payee (*e.g.*, a merchant, seller or telemarketer). In place of a signature, the RCC bears a statement that the account holder authorized the check. Any person who obtains a consumer's bank routing and account number can print an RCC with the proper equipment or the help of a third party payment processor, and deposit it in any account at any bank for clearing. In some cases, a person can deposit an RCC by scanning a digital image of the check onto a computer, and then transmitting that image to the bank - a practice known as remote deposit or remote deposit capture. The bank treats the RCC like an ordinary signed check, and it causes the RCC to be submitted to the consumer's bank for payment from the consumer's account. An RCC is distinct from an RCPO

[1] We anticipate requesting authority to issue additional FIRREA subpoenas to financial institutions in the coming weeks.

in that it originates as a paper-based transaction, even if it later becomes scanned or electronically imaged.

An RCPO is created when a merchant or processor enters bank account and routing numbers into an electronic check template that is converted into an electronic file for deposit into the check clearing system. RCPOs are similar to RCCs in that they are typically initiated with Internet or telephone instructions from the consumer and bear no direct evidence of the customer's authorization. When printed out, RCPOs and RCCs look almost identical. However, unlike RCCs, RCPOs do not begin with a paper item. Unlike the return rates of ACH transactions, which are closely monitored by NACHA, the return rates of RCCs and RCPOs are not subject to any monitoring by the check clearing system.

The payment processors and banks that are the subjects of our proposed subpoenas are believed to have transacted business in RCCs and RCPOs in the past. Based upon information we have collected from Payment Processor Working Group members, we believe merchants used these firms to commit fraud. Our goal is to determine who knowingly committed fraud, or was deliberately ignorant of fraud, committed against consumers.

I. Bank subpoenas

[redacted]

[redacted]

II. Processor Subpoenas

[redacted]

[redacted]

[redacted]

Conclusion

We request that you sign the attached FIRREA subpoenas. (Goldberg)

From: Bresnick, Michael J (ODAG)
Sent: Tuesday, March 19, 2013 6:56 PM
To: Delery, Stuart F. (CIV); Olin, Jonathan F. (CIV); Harwood, Charles A. [redacted]@ftc.gov)
Subject: remarks
Attachments: Remarks to Exchequer Club--3-20-13 (draft 3-19-13).docx

Stuart, Jon, and Chuck,

Sorry for the very late notice, but I'll be giving a speech tomorrow around noon at the Exchequer Club of D.C. I plan to discuss some of the recent accomplishments of Task Force members, as well as to address some priorities for the year. I spend a significant amount of time addressing the Consumer Protection WG's review of financial institutions' and third-party payment processors' roles in mass-marketing fraud schemes, as well as internet payday lenders. I sent Mike Blume, Joel Sweet, and Rich Goldberg a draft, and wanted to make sure you had a chance to make comments as well. Sorry, again, for sending this so late.

Mike

REMARKS

OF

MICHAEL J. BRESNICK
EXECUTIVE DIRECTOR
FINANCIAL FRAUD ENFORCEMENT TASK FORCE
OFFICE OF THE DEPUTY ATTORNEY GENERAL
U.S. DEPARTMENT OF JUSTICE

AT THE

EXCHEQUER CLUB OF WASHINGTON, D.C.

ON

WEDNESDAY, MARCH 20, 2013

ST. REGIS HOTEL
WASHINGTON, D.C.

Good afternoon. Thank you for that kind introduction, and thank you all for having me here today. I'd especially like to thank John Ryan, my friend and President and Chief Executive Officer of the Conference of State Bank Supervisors, for inviting me to speak.

As you heard, I am the Executive Director of President Barack Obama's Financial Fraud Enforcement Task Force. It has been my great pleasure to lead this Task Force for the past year and a half, and to work closely with Attorney General Eric Holder, Deputy Attorney General James Cole, Acting Associate Attorney General Tony West, and so many others throughout government. The Task Force was created in 2009 with the understanding that no matter the office or agency -- federal, state, or local; law enforcement or regulatory -- all of us within government share a common desire and have a core obligation to do everything that we can to protect the American public from the often devastating effects of financial fraud, whether it be mortgage fraud or investment fraud, grant or procurement fraud, consumer fraud or fraud in lending. And we know that we can accomplish so much more by working together than by working in isolated, compartmentalized silos. Through the efforts of the Financial Fraud Enforcement Task Force, that's exactly what we've done.

Today I'm going to start by telling you about some of our recent accomplishments -- which were only made possible by our working together -- and then move on to a few priorities we will be focusing on in the coming year.

Just recently Task Force members announced the filing of parallel civil complaints -- by the Department of Justice and more than ten states -- against the ratings agency Standard and Poor's, shedding a powerful light on conduct that went to the heart of the recent financial crisis. The Department alleged that from at least 2004 to 2007, S&P lied about its objectivity and independence. The evidence revealed that S&P promised investors and the public that their ratings were based on data and analytical models reflecting the company's true credit judgment. In fact, internal S&P documents made clear that the company regularly altered, or delayed altering, its ratings models to suit the company's own business interests. We also alleged that from at least March 2007 to October 2007, S&P issued ratings for certain CDOs that it knew were inflated at the time it issued them. By working closely with the states, and coordinating our collective efforts, we have never been more strategic, or effective.

Moreover, in Fiscal Year 2012, the Department, in close partnership with the U.S. Department of Housing and Urban Development and its Office of Inspector General, sued for or settled claims with banks for losses related to the mortgage crisis totaling over $2 billion, including recovering nearly $500 million from settlements with Deutsche Bank AG, CitiMortgage and Flagstar Bank.

Through the Task Force's Non-Discrimination Working Group, in coordination with our partners at the OCC, Federal Reserve, and many others, our enforcement of fair lending laws has never been more robust. Since 2010 the Civil Rights Division's Fair Lending Unit has filed or resolved 24 lending matters under

the Fair Housing Act, the Equal Credit Opportunity Act, and the Servicemembers Civil Relief Act. The resolutions in these matters provide for a minimum of $660 million in monetary relief for impacted communities and for more than 300,000 individual borrowers.

The Residential Mortgage-Backed Securities Working Group is actively investigating fraud in the securitization and sale of residential mortgage-backed securities -- conduct that contributed to the financial crisis. Mortgage Fraud Working Group members are creating training sessions for federal and state prosecutors and civil attorneys, as well as arming distressed homeowners with the information they need to avoid becoming victims of fraud. And efforts by the Consumer Protection Working Group to protect servicemembers and their families from predators targeting them as vulnerable marks includes recently creating and disseminating enforcement tool-kits to state attorneys general, U.S. Attorneys' Offices, and JAG legal assistance officers that provide an overview of common scams targeting members of the military, available federal and state laws to address these schemes, opportunities for support from federal and state partners, and sample legal materials.

As you can see, the Task Force, through its spirited and energetic members, is tackling financial fraud on many fronts, with a focus on enforcement, prevention, and victim assistance. And by working together, we are able to identify fraud trends occurring throughout the country, develop priorities and national fraud enforcement strategies, create and coordinate national initiatives, and establish

training events and guidance for our nation's criminal prosecutors and civil attorneys. It is an example of what we can accomplish when we eliminate unnecessary boundaries and work together towards a common goal.

While the Task Force has done, and continues to do, much in these and other areas, I'd now like to discuss three additional issues that we have prioritized.

First, Task Force members have focused intently on the government's ability to protect its interests and ensure that it does business only with ethical and responsible parties. According to a recent GAO report, in Fiscal Year 2010 government spending on contracted goods and services was more than $535 billion. Accordingly, we are encouraging greater cooperation with government agencies involved in the suspension and debarment process, actions taken to exclude businesses or individuals who are not behaving in an ethical and lawful manner from receiving contracts.

Second, the Non-Discrimination Working Group has placed an increased focus on enforcement of discrimination by auto lenders. Currently, the law does not require auto lenders to give consumers the best interest rate they qualify for, and does not prohibit lenders from basing compensation on the ability to charge higher interest rates. As we found in the mortgage context, however, this practice may violate the fair lending laws if it causes minorities to be charged more than similarly qualified white borrowers. The Department's Civil Rights Division is working closely with Consumer Financial Protection Bureau on this issue.

And third, the Consumer Protection Working Group has prioritized the role

of financial institutions in mass marketing fraud schemes -- including deceptive payday loans, false offers of debt relief, fraudulent health care discount cards, and phony government grants, among other things -- that cause billions of dollars in consumer losses and financially destroy some of our most vulnerable citizens. The Working Group also is investigating the businesses that process payments on behalf of the fraudulent merchants -- financial intermediaries referred to as third-party payment processors. It's this third priority that I'd like to discuss in a little more detail.

The reason that we are focused on financial institutions and payment processors is because they are the so-called bottlenecks, or choke-points, in the fraud committed by so many merchants that victimize consumers and launder their illegal proceeds. For example, third-party payment processors are frequently the means by which fraudulent merchants are able to get paid. They provide the scammers with access to the national banking system and facilitate the movement of money from the victim of the fraud to the scam artist. And financial institutions through which these fraudulent proceeds flow, we have seen, are not always blind to the fraud. In fact, we have observed that some financial institutions actually have been complicit in these schemes, ignoring their BSA/AML obligations, and either know about -- or are willfully blind to -- the fraudulent proceeds flowing through their institutions.

Our prioritization of this issue is based on this principle: If we can eliminate the mass-marketing fraudsters' access to the U.S. financial system -- that is, if we

can stop the scammers from accessing consumers' bank accounts -- then we can protect the consumers and starve the scammers. This will significantly reduce the frequency of and harm caused by this type of fraud. We hope to close the access to the banking system that mass marketing fraudsters enjoy -- effectively putting a chokehold on it -- and put a stop to this billion dollar problem that has harmed so many American consumers, including many of our senior citizens.

Sadly, what we've seen is that too many banks allow payment processors to continue to maintain accounts within their institutions, despite the presence of glaring red flags indicative of fraud, such as high return rates on the processors' accounts. High return rates trigger a duty by the bank and the third-party payment processor to inquire into the reasons for the high rate of returns, in particular whether the merchant is engaged in fraud.

Nevertheless, we have actually seen instances where the return rates on processors' accounts have exceeded 30%, 40%, 50%, and, even 85%. Just to put this in perspective, the industry average return rate for ACH transactions is less than 1.5%, and the industry average for all bank checks processed through the check clearing system is less than one-half of one percent. Return rates at the levels we have seen are more than red flags. They are ambulance sirens, screaming out for attention.

A perfect example of the type of activity I'm talking about is the recent complaint against the First Bank of Delaware filed by the Department in the Eastern District of Pennsylvania, in Philadelphia. There, investigators found that

in just an eleven-month period from 2010 to 2011, the First Bank of Delaware permitted four payment processors to process more than $123 million in transactions. Amazingly, more than half of the withdrawal transactions that the bank originated during this time were rejected, either because the consumer complained that the transaction was unauthorized, there were insufficient funds to complete the transaction, or the account was closed, each of which may indicate potential fraud and trigger the need for further inquiry. But the bank did nothing. Nothing, but continue to collect its fees per transaction, while consumers continued to get gouged by unscrupulous scam artists. Ultimately, the government alleged that the bank was engaged in a scheme to defraud under the Financial Institutions Reform, Recovery, and Enforcement Act and the bank agreed to pay a civil money penalty before surrendering its charter and closing its doors.

Underscoring the importance of this case, in the press release announcing a parallel action with the Financial Crimes Enforcement Network, the Acting Chairman of the FDIC, Martin Gruenberg, said, "Effective Bank Secrecy Act and anti-money laundering programs that are commensurate with the risk profile of the institution are vital to protecting our financial system." He added that "[t]he significant penalty assessed in this case emphasizes the importance of having strong internal controls to assure compliance with anti-money laundering regulations and to detect and report potential money laundering or other illicit financial activities."

So, the First Bank of Delaware is a model of irresponsible behavior by a

bank.

Of course, this conduct is completely unacceptable. And it is receiving the full attention of the Department of Justice. In fact, we have established within the Civil Division a dedicated team of attorneys and investigators to address similar unlawful conduct, and we will not hesitate to act when we see evidence of wrongdoing. Our message to banks is this: Maintaining robust BSA/AML policies and procedures is not merely optional or a polite suggestion. It is absolutely necessary, and required by law. Failure to do so can result in significant civil, or even criminal, penalties under the Bank Secrecy Act, FIRREA, and other statutes.

Consequently, banks should endeavor not only to know their customers, but also to know their customers' customers. Before they agree to do business with a third-party payment processor, banks should strive to learn more about the processors' merchant-clients, including the names of the principals, the location of the business, and the products being sold, among other things. If they are going to allow their institutions to be used by others as a gateway to access the bank accounts of our nation's consumers, banks need to know for whom they are processing payments. Because if they don't, they might be allowing some unscrupulous scam artist to be taking the last dollars of a senior citizen who fell prey to another fraud scheme, and hundreds of millions of dollars of additional proceeds of fraud to flow through their institutions. And in that case, they might later find themselves in the unfortunate position of the First Bank of Delaware.

In addition, as part of our focus on the role of financial institutions and third-

party payment processors in mass-marketing fraud schemes, we naturally also are examining banks' relationship with the payday lending industry, known widely as a subprime and high-risk business. We are aware, for instance, that some payday lending businesses operating on the Internet have been making loans to consumers in violation of the state laws where the borrowers reside. And, as discussed earlier, these payday lending companies are able to take the consumers' money primarily because banks are originating debit transactions against consumers' bank accounts. This practice raises some questions.

As you know, the Bank Secrecy Act demands that banks have effective compliance programs to prevent illegal use of the banking system by the banks' clients. Bank regulatory guidance exhorts banks to collect information sufficient to determine whether a client poses a threat of criminal or other unlawful conduct.

Banks, therefore, should consider whether originating debit transactions on behalf of Internet payday lenders -- particularly where the loans may violate state laws -- is consistent with their BSA obligations.

Understandably, it may not be so simple a task for a bank to determine whether the loans being processed through it are in violation of the state law where the borrower resides. The ACH routing information, for example, may not indicate to the bank in which state the consumer lives, and variations in state laws could preclude blanket conclusions. Yet, at a minimum, banks might consider determining the states where the payday lender makes loans, as well as what types of loans it offers, the APR of the loans, and whether it make loans to consumers in

violation of state, as well as federal, laws. By asking these questions, a bank may become aware of certain red flags, inviting further scrutiny and further action. The bury-your-head-in-the-sand approach, to the contrary, is certain to result in no action, even where some might be warranted, and is fraught with danger to consumers.

It comes down to this: When a bank allows its customers, and even its customers' customers, access to the national banking system, it should endeavor to understand the true nature of the business that it will allow to access the payment system, and the risks posed to consumers and society regarding criminal or other unlawful conduct.

As I said at the outset, we in government share a unity of purpose and a common resolve to tackle the most pressing financial fraud issues of our time, and know that we must work together if we are to be successful in protecting the American public from harm. We are committed to doing so, and are approaching these issues in a smart, systematic, and coordinated way.

It has been a pleasure to address this distinguished group today. I thank you, again, for the opportunity, and now look forward to addressing any questions you may have.

U. S. Department of Justice

Civil Division

FILE

Washington, D.C. 20530

April 17, 2013

TO: Stuart F. Delery
Acting Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

MB/RG
CG
4/17/13

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: OPERATION CHOKE POINT: EIGHT-WEEK STATUS REPORT

This memo addresses our efforts during the past eight weeks to combat mass-market consumer fraud by focusing on payment systems vulnerabilities. Our goal is to protect consumers and stave off scammers by focusing on the payment processors and banks that enable fraudulent merchants to access consumers' bank accounts.

I. CASES UNDER INVESTIGATION

U. S. Department of Justice

Civil Division

Washington, D.C. 20530

April 17, 2013

TO: Stuart F. Delery
Acting Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume MB/RC
Director
Consumer Protection Branch

SUBJECT: OPERATION CHOKE POINT: EIGHT-WEEK STATUS REPORT

This memo addresses our efforts during the past eight weeks to combat mass-market consumer fraud by focusing on payment systems vulnerabilities. Our goal is to protect consumers and stave off scammers by focusing on the payment processors and banks that enable fraudulent merchants to access consumers' bank accounts.

I. CASES UNDER INVESTIGATION

[redacted]

[redacted]

F. Additional Matters

We are in a target-rich environment. We anticipate within the coming weeks that we will request authority to serve subpoenas upon additional banks.

Even without serving additional subpoenas, however, new potential investigations arrive regularly. [redacted]

[redacted]

II. ENGAGEMENT WITH OTHER AGENCIES

A. The Federal Reserve Bank – Atlanta ("FRB-A")

FRB-A is one of the nation's two clearing houses for ACH transactions, and also is a major clearing house for checks. FRB-A also acts as a primary or secondary regulator for many of the nation's banks. In its role as an ACH clearinghouse, FRB-A monitors banks with high return volume. We learned during the investigation of First Bank of Delaware that FRB-A communicates with banks experiencing abnormal ACH activity. Indeed, in that investigation, communications between FRB-A and First Bank of Delaware (obtained through a FIRREA subpoena to the FRB-A) provided strong evidence that First Bank of Delaware had knowledge that it was furthering fraud.

Richard M. Fraher, Vice President and Counsel to the Retail Payments Office, is supportive of our efforts. He has invited our team to Atlanta for a working session with the business and operations side of FRB-A so that we can better understand how the ACH and checks systems operate, assess opportunities to obtain evidence from the FRB-A (including data and tailored reports), and consider how FBD-A can better support law enforcement efforts. If travel funding is available, we would like to take advantage of Fraher's offer. We believe this opportunity can substantially further our existing investigations and, perhaps more importantly, our goal of surveilling for ongoing schemes so that we can promptly engage suspect banks.

B. NACHA/CLEARING HOUSE

We are arranging training from NACHA or an associated entity relating to ACH rules, particularly as they relate to third-party processors. We plan to invite FTC attorneys and investigators, and potentially other interested agencies, to participate.

C. CFPB

In late February, we met with representatives of the CFPB to discuss payday lending. Although we have differing thoughts as to an appropriate legal theory to pursue, we agreed with CFPB that the payment system (payment processors and banks) deserves closer scrutiny. We offered to work with CFPB to identify appropriate targets and to pursue a joint investigation. We suggested factors that would best support a civil case involving DOJ, including for example payday lenders targeting military families. CFPB has not responded to our proposal for a joint investigation. Recent communications concerning payday lending have received no response.

D. FDIC – Consumer Protection Division

On February 24, 2013, the New York Times reported that banks are providing services to payday lenders, and the banks are not responding appropriately to consumers' complaints concerning related unauthorized withdrawals. In the wake of the article, attorneys from the FDIC's Division of Consumer Protection contacted us to share ideas about the laws relating to payday lending and potential investigative approaches. We are scheduled to meet shortly with Marguerite Sagatelian, head of the Compliance and Enforcement group of the FDIC's Division of Depositor and Consumer Protection, to continue this discussion.

E. FDIC – Office of Inspector General

We met on April 16 with Matthew Alessandrino, Special Agent/Assistant Inspector General for Investigations, and others from his staff, to discuss our initiative and the opportunity for the FDIC to assign agents to work on our cases. We developed a structure for further cooperation, including information exchanges and potential allocation of further resources to our investigations.

F. State Banking Regulators

State banking officials in Florida [redacted] and Kentucky [redacted] have offered assistance in our investigations.

III. STAFFING/RESOURCES

Our core team consists of CPB Assistant Director Richard Goldberg, CPB Trial Attorney [redacted], CPB Trial Attorney/Detailee Joel Sweet (USAO-EDPA); CPB Analyst/Detailee [redacted]; USPIS Inspector [redacted];[2] USPIS Investigative Analyst [redacted]; and CPB Paralegal [redacted].

The FBI had committed to assigning an analyst to regularly review newly-filed SARS for references to mass market consumer fraud and third-party payment processors. An analyst was assigned and performed that duty for a short time before leaving the FBI. Although the FBI is committed to finding a replacement, it is our understanding that it may take many weeks before this activity resumes. This impedes our effort to proactively identify and staunch ongoing mass market fraud. We are exploring alternatives in the event FBI staffing is not forthcoming.

IV. TRAINING TO DEVELOP DOJ EXPERTISE

Travel funding and time permitting, we hope to offer U.S. Attorney Offices training in payment systems/mass market fraud prosecution under FIRREA.

---

[2] Inspector [redacted] will be leaving CPB in June. USPIS has pledged to assign a replacement Inspector.

V. RELATED AREAS OF INQUIRY

In addition to evaluating the payday lending industry, we are attempting to develop a better understanding of consumer fraud risk posed by emerging payment systems. For example, mobile-to-mobile payment and virtual currency (*e.g.*, Bitcoin) transactions are on the rise. In some cases, these payments travel through credit card channels. Other emerging technologies use the checking channel, and yet others the ACH system. Each of these channels is governed by a different set of rules and regulations, and each presents different consumer fraud vulnerabilities.

Consider, for example, stored-value prepaid debit cards. As described in "Banks barreling into the prepaid debit card market," The Washington Post (April 11, 2013) http://www.washingtonpost.com/business/economy/banks-barreling-into-the-prepaid-debit-card-market/2013/04/10/28d99dd6-963c-11e2-894a-b984ebdff2e6_story.html, banks and other financial institutions and moving into the prepaid debit card market at a fast pace. These cards are designed to service the approximately 17 million people (and growing) who are "unbanked," or living outside the banking system. A consulting firm predicts that in 2013 Americans will put $202B on reloadable debit cards, compared to $28.6B in 2009. Consumer advocates are concerned that prepaid card users will be forced to pay high and hidden fees – an issue for the CFPB to address. It does not appear that significant attention is being paid to consumer fraud vulnerabilities. Most of these cards are not governed by rules and protections that apply to bank deposits and transactions using ACH and checks, traditional fraud indicators may not be present. Moreover, card issuers may not be obligated to mitigate or address consumer fraud risk.[3] We have no doubt that fraudsters will attempt to find vulnerabilities in this emerging payment system.

Last month, American Express announced that the FDIC had agreed to insure prepaid debit cards that it plans to issue through Wal-Mart. See "American Express prepaid debit cards get FDIC insurance," The Washington Post, March 26, 2013) http://articles.washingtonpost.com/2013-03-26/business/38026618_1_reloadable-prepaid-cards-mercator-advisory-group-load-money. This is a significant event in the development of this payment instrument. Through a relationship we have with senior management at American Express, we are considering engaging in a discussion concerning consumer fraud risk with these cards, perhaps along with the FDIC.

(Sweet/[redacted]/Goldberg)

---

[3] Michael Bresnick has researched this issue and learned that prepaid debit cards generally are not governed by Regulations E or Z (which address ACH and other electronic payment systems). For example, the cards are not "credit" and are not subject to the Truth in Lending Act, since they do not entitle consumers to defer payment of a debt or to incur debt and defer its payment. They also generally are not subject to Electronic Funds Transfer Act since they are not considered an "electronic funds transfer" or tied to an "account." Many of the other consumer protections associated with traditional bank instruments do not apply.

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Wednesday, April 24, 2013 3:20 PM
To: Soneji, Sabita J. (CIV); Bresnick, Michael J (ODAG); Sorgente, Natalia (CIV)
Subject: RE: Payday Lending

Perfect. Thanks! I will share with Joel, et al, as the 3PPP initiative is working on pay day now.

From: Soneji, Sabita J. (CIV)
Sent: Wednesday, April 24, 2013 3:18 PM
To: Bresnick, Michael J (ODAG); Frimpong, Maame Ewusi-Mensah (CIV); Sorgente, Natalia (CIV)
Subject: Payday Lending

Team –
Not sure where the CPWG payday lending group is, but found this interesting and relevant to some of our discussions:
http://dealbook.nytimes.com/2013/04/23/crackdown-expected-on-big-banks-payday-loans/?nl=todaysheadlines&emc=edit_th_20130424

Sabita

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Monday, April 22, 2013 3:53 PM
To: Olin, Jonathan F. (CIV); Blume, Michael S.
Subject: Re: 3PPP

Yes. Stuart should have gotten the memo I sent up last week. I can forward a scanned copy to you.

From: Olin, Jonathan F. (CIV)
Sent: Monday, April 22, 2013 03:49 PM
To: Frimpong, Maame Ewusi-Mensah (CIV); Blume, Michael S.
Subject: 3PPP

Any materials Stuart should review before tomorrow's meeting?

Jonathan Olin
Chief of Staff, Civil Division
U.S. Department of Justice
[redacted]
[redacted]@usdoj.gov

UNITED STATES DEPARTMENT OF JUSTICE - CIVIL DIVISION
CORRESPONDENCE TRACKING SYSTEM

ID: 67183 Executive Sec #:
Document Type: Litigation
File Code: Deputy for Consumer Protection Branch
Responding Unit: Consumer Protection Branch
Reviewer: Richard Goldberg
Drafter: Joel Sweet
To: Stuart F. Delery; Thru: Maame Ewusi-Mensah Frimpong
From: Michael S. Blume

Cover Sheet Date: 04/29/2013
Document Date:
Date Received: 04/29/2013
Response Due: ~~04/29/2013~~ ASAP
Date Closed:
SG Due: expedite not necessary Response by 5/6/13 is sufficient.

Subject: Payment Processor Investigation -- Request for Issuance of Subpoenas in Connection with Investigation of Payment Processors and Banks used to Process Fraudulent Payments

Comments: Maame Frimpong to review.
Stuart Delery to sign subpoenas.

Actions: Assigned To	Initials	Date Assigned	Finished
Maame Ewusi-Mensah Frimpong		04/29/2013	30 April 2013
Stuart F. Delery	SFD	APR 30 2013	5/1/13
[redacted]		MAY 1 2013	MAY 1 2013
Mike Blume		MAY 1 2013	

Notes: Stuart – I recommend you sign these FIRREA Subpoenas. We are expanding Operation Choke Point to include entities that transact business on behalf of pay day lenders.

↗ Approval by May 6 is sufficient. Thank you!

U.S. Department of Justice

Civil Division

Washington, DC 20530

APR 29 2013

TO: Stuart F. Delery
Acting Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: Payment Processor Investigation -- Request for Issuance of Subpoenas in Connection With Investigation of Payment Processors and Banks used to Process Fraudulent Payments

Time Frame

We request your approval by April 29, 2013. There are no external deadlines.

Recommendation

We seek authorization to issue subpoenas under the Financial Institutions Reform, Recovery and Enforcement Act of 1989, 12 U.S.C. § 1833a(g)(1)(C) ("FIRREA"). The subpoenas would be directed to three entities described further below.

Case Summary

As part of Operation Choke Point – a multi-agency effort to combat mass market consumer fraud by focusing on payment systems – we are investigating third-party payment processors and banks engaged in originating debit transactions against consumers' bank accounts on behalf of suspected fraudulent Internet and telemarketing merchants. We are expanding our efforts to include banks and processors that transact

debits against consumers' accounts on behalf of predatory Internet-based payday lenders. Pursuant to your authorization, we already have served a number of subpoenas.

[redacted]

[redacted]

Conclusion

We request that you sign the attached FIRREA subpoenas. (Goldberg/Sweet)

UNITED STATES DEPARTMENT OF JUSTICE - CIVIL DIVISION
CORRESPONDENCE TRACKING SYSTEM

ID: 67264 Executive Sec #:

Cover Sheet Date: 05/14/2013
Document Date: 05/14/2013
Date Received: 05/14/2013
Response Due:
~~EXPEDITE~~
Date Closed:
SG Due: ~~ASAP~~ as soon as practicable

Document Type: Litigation
File Code: Deputy for Consumer Protection Branch
Responding Unit: Consumer Protection Branch
Reviewer: [redacted] Goldberg Richard
Drafter: Joel Sweet [redacted]
To: Stuart F. Delery, A/AAG, Civil Division
From: Michael S. Blume, Director, Consumer Protection Branch thru:
Maame Ewusi-Mensah Frimpong, DAAG, Civil Division

Subject: Payment Processor Investigation - Request for Issuance of Subpoenas to Banks

Comments: Maame Ewusi-Mensah Frimpong: Review and comment
Stuart F. Delery: Sign [redacted] subpoenas under the Financial Institutions Reform, Recovery and Enforcement Act of 1989.
Time Frame: "We request your approval by May 24, 2013. There are no external deadlines."

Actions: Assigned To	Initials	Date Assigned	Finished
Maame Ewusi-Mensah Frimpong		05/14/2013	15 May 2013
Stuart F. Delery	SFD	MAY 16 2013	5/16/13
[redacted]		MAY 17 2013	MAY 17 2013
Michael S. Blume		MAY 17 2013	

Notes:

Stuart - I recommend that you authorize & sign these subpoenas. We have identified additional banks that are or may be processing payments on behalf of fraudulent entities. These banks have been identified through the FTC's investigations, work by the FDIC, and our own investigation

U.S. Department of Justice

Civil Division

Washington, DC 20530

May 14, 2013

TO: Stuart F. Delery
Acting Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: Payment Processor Investigation – Request for Issuance of Subpoenas to Banks

Time Frame

We request your approval by May 24, 2013. There are no external deadlines.

Recommendation

We seek authorization to issue [redacted] subpoenas under the Financial Institutions Reform, Recovery and Enforcement Act of 1989, 12 U.S.C. § 1833a(g)(1)(C) ("FIRREA"). The subpoenas would be limited in scope and directed to the entities described below.

Case Summary

In furtherance of Operation Choke Point, a multi-agency initiative combating mass-market consumer fraud through a focus on payment systems, in February 2013, we served subpoenas upon five banks and three third-party payment processors. Based upon information obtained in response to those subpoenas and from other sources, we have opened investigations against several of these entities.

As described below, our investigation to date and coordination with other federal agencies has revealed other banks engaged in conduct worthy of investigation. We have methodically identified additional banks that we suspect are processing payments on behalf of fraudsters, or that have been identified by payment processors as prospects for

originating such transactions. Our objective is to further identify gateways used by scammers to gain access to the national payment systems. Where appropriate and resources permit, we will open investigations into banks that knowingly permit their infrastructure to be used by fraudsters (or that remain willfully blind to that conduct), and possibly processors and fraudulent merchants.

Discussion

Fraudulent merchants and predatory Internet payday lenders access consumers' bank accounts through relationships with third-party payment processors and banks. Upon instruction from a fraudulent merchant or payday lender, a third-party processor instructs a bank to access the national payments systems (automatic clearing house ("ACH") and check transactions) to debit money from the bank accounts of consumer victims. In some cases, the bank is aware of (or has remained intentionally blind to) the fact that purported consumer authorizations for debit transactions were obtained through fraud. In other cases, banks may have been misled by the third-party processor and/or the merchant as to the true nature of the activity, or the validity of the consumer authorization.

Using a variety of sources, we have identified [redacted] banks that originated debit transactions against consumers' accounts on behalf of fraudulent merchants, or engaged in discussions with suspected scammers about such activity. Some of the banks also processed debit transactions on behalf of Internet payday lenders who collect potentially unlawful debts in violation of state and possibly federal laws and regulations.

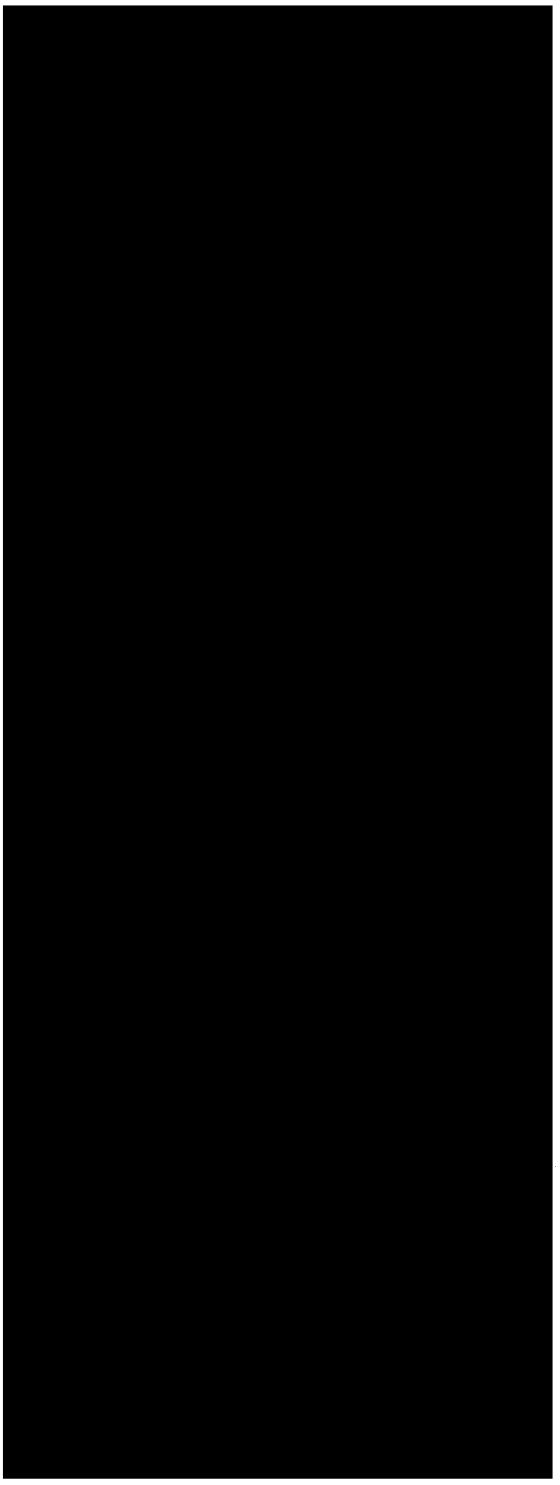
We have carefully tailored the subpoenas so that responses will identify third-party processors and fraudulent merchants that harm consumers. We also seek evidence of red flags that indicate that a bank had actual or constructive knowledge of consumer fraud. We have deliberately omitted broad requests -- including requests for "all documents" and for large amounts of data -- that would make compliance burdensome and expensive for banks, and that would require substantial resources for our team to review. After evaluating the responses to the subpoenas, if warranted, we may request authority to serve additional subpoenas to particular banks.

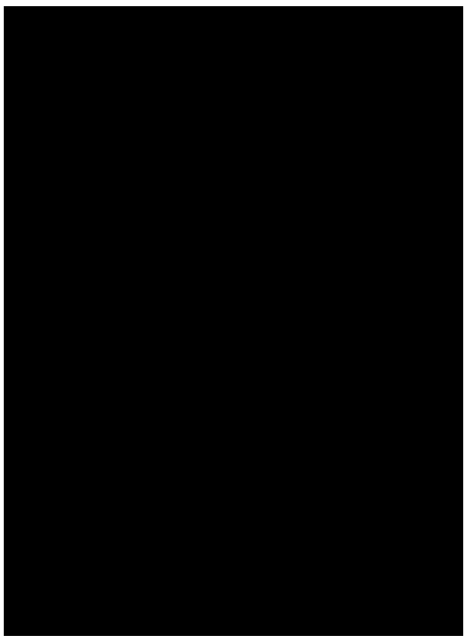
Following are the banks from which we seek documents. The banks are organized by the source from which we obtained information justifying the service of an investigatory subpoena.

Federal Trade Commission

The Federal Trade Commission investigates and pursues civil injunctive actions against entities that defraud, deceive, and/or mislead consumers. The FTC's attorneys and investigators, as part of a regular practice, identify payment processors and banks associated with fraudulent schemes. The FTC has provided us with emails in which processors and/or merchants discuss banks that are providing access to the payment

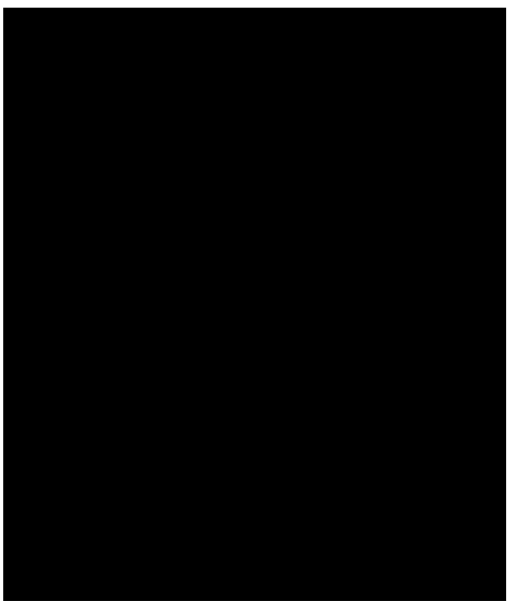
system, and also prospective banks that may be willing to originate debit transactions against consumers' accounts to further their schemes. Banks identified in the FTC documents include:





Federal Reserve Bank -- Atlanta

Pursuant to a FIRREA subpoena that the USAO-EDPA served last year upon the Federal Reserve Bank – Atlanta, we have received regularly-created "Dashboard Reports" addressing high return rates among banks originating ACH transactions. High return rates are an important indication of potential fraud against consumers. The Dashboard Reports are created specifically to identify and monitor banks with high return rates. Dashboard Reports for the period January through June 2012 identify the following banks with outlier high return rates:



[redacted]

[redacted]

[redacted]

We intend to serve each subpoena upon the respective bank's CEO with a transmittal letter stating that the subpoena has been issued in connection with an investigation of consumer fraud. To assist the bank and its counsel to understand the nature of our investigation, we will include a copy of a recent FinCEN Advisory and bank regulator guidance concerning risks associated with third-party payment processors.

Conclusion

We request that you sign the attached FIRREA subpoenas.

(Goldberg/Sweet/[redacted]

United States of America
v.
Payment Processing Center

A Case Study of Remotely Created Check Abuse and Payment System Vulnerabilities

Joel M. Sweet, Trial Attorney, Consumer Protection Branch, DOJ
(detailee from United States Attorney's Office for the Eastern District of Pennsylvania)

Disclaimer

Any opinions reflected in this presentation are those of the presenter and are not necessarily those of the Department of Justice, or any government official, agency, department, or branch.

The information in this presentation is from public sources.

Mass Market Consumer Fraud – a National Scourge

Bernie Madoff swindled more than $40B from a select group of mostly wealthy investors.

Fraudsters steal more than $40B from consumers – mostly the elderly and those in the lower middle class – every year!

Which is most likely to receive attention from law enforcement, regulators, and the press: a single theft of $100 million, or one million thefts of $100?

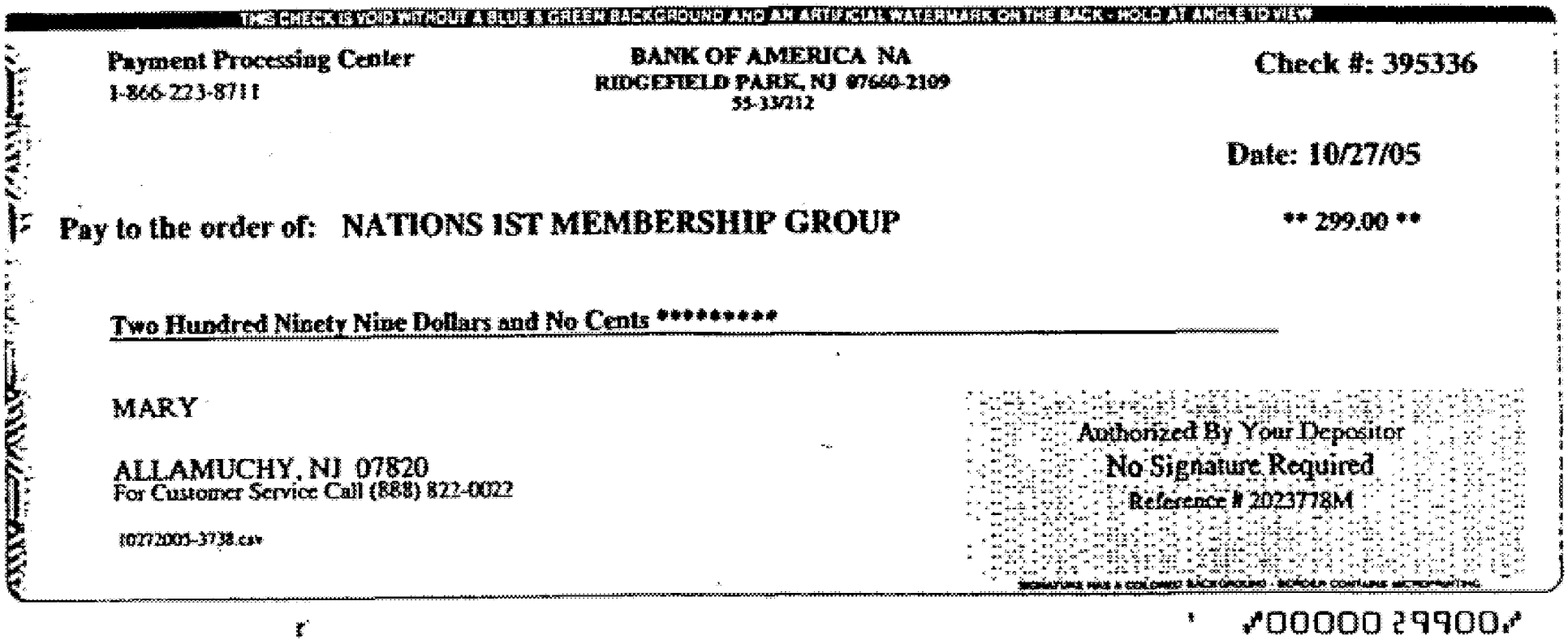
Common Methods of Payment System Abuse

- Debit transactions originated by payment processors and banks on behalf of telemarketing and Internet fraudsters
- Phone company bills used to originate unauthorized charges ("cramming")
- Mortgage payment mechanisms used to originate unauthorized charges

Law Enforcement Challenges to Prosecuting Telemarketing/Internet Fraud

- Jurisdictional limitations (state and international)
- Fraudsters change corporate identities and law enforcement plays "whack-a-mole"
- Victims are dispersed geographically
- Victims cannot identify fraudsters – no face-to-face contact
- Plausible deniability – cross-pointing among call centers, mail houses, fulfillment centers, payment processors, and banks
- Limited investigative and prosecutorial resources
- Limited reach of State Attorneys General and FTC

A Remotely Created Check ("RCC")



THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK. HOLD AT ANGLE TO VIEW

Payment Processing Center
1-866-223-8711

BANK OF AMERICA NA
RIDGEFIELD PARK, NJ 07660-2109
55-13/212

Check #: 395336

Date: 10/27/05

Pay to the order of: NATIONS 1ST MEMBERSHIP GROUP

** 299.00 **

Two Hundred Ninety Nine Dollars and No Cents *********

MARY

ALLAMUCHY, NJ 07820
For Customer Service Call (888) 822-0022

10272005-3738.csv

Authorized By Your Depositor
No Signature Required
Reference # 2023778M

SIGNATURE HAS A COLORED BACKGROUND - BORDER CONTAINS MICROPRINTING

⑈00000 29900⑈

RCC Fraud: Well-Known to Banks

"Demand drafts can be misused to commit check fraud. This practice involves the misuse of account information to obtain funds from a person's bank account without that person's signature on a negotiable instrument. . . **demand drafts have been used by deceptive telemarketers who obtain bank account information and withdraw unauthorized funds from consumers' bank accounts,** without their realizing that such withdrawals are occurring. . . ."

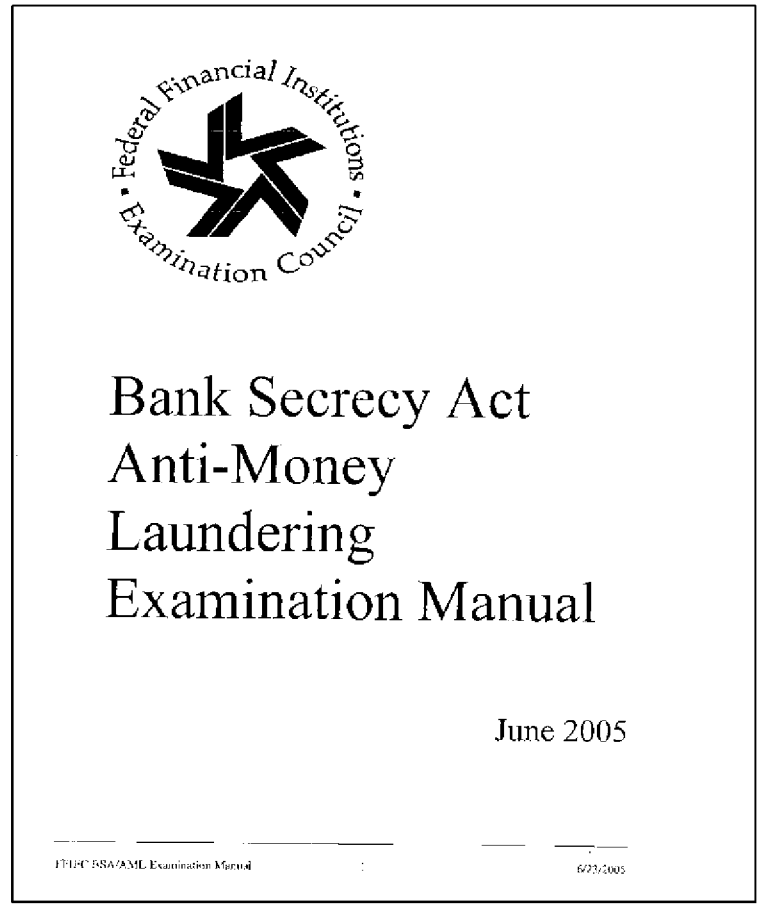
A Guide to Checks and Check Fraud, published by **Wachovia,** 2003

RCC Fraud: Well-Known to State Law Enforcement and FRB

- In 2005, 35 state attorneys general jointly request that the Federal Reserve ban RCCs from the payments system:
  - "demand drafts are frequently used to perpetrate fraud on consumers"
  - "such drafts should be eliminated" in favor of other forms of payment
  - If not eliminated, mandatory marking of RCCs and other measures to protect consumers

RCC Fraud: Well-Known to Bank Regulators

BSA/AML Examination Manual (FRB, FDIC, NCUA, OCC, and OTS)



Expanded Overview – Third-Party Payment Processors

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with its relationships with third-party payment processors, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Non-bank, or third-party, payment processors (processors) are bank customers that provide payment-processing services to merchants and other business entities.

Traditionally, processors contracted primarily with retailers that had physical locations in order to process the retailers' transactions. These merchant transactions primarily included credit card payments but also covered automated clearing house demand drafts[118] (also known as e-checks), and debit and stored value cards transactions. With the expansion of the Internet, retail borders have been eliminated. Processors may now service a variety of merchant accounts, including conventional retail and Internet-based establishments, prepaid travel, and Internet gaming enterprises.

RISK FACTORS

Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, and fraud schemes.

The bank's BSA/AML risks when dealing with a processor account are similar to risks from other activities in which the bank's customer conducts transactions through the bank on behalf of the customer's clients. When the bank is unable to identify and understand the nature and source of the transactions processed through an account, the risks to the bank and the likelihood of suspicious activity can increase. If a bank has not implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or sanctioned transactions.

[118] A demand draft is a substitute for a preprinted paper check. The draft is produced without a consumer signature but presumably with the consumer's authorization.

RISK MITIGATION

Banks offering account services to processors should develop and maintain adequate policies, procedures, and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. Verification and assessment of a processor can be completed by performing the following procedures:

- Reviewing the processor's promotional materials, including its web site, to determine the target clientele. (Businesses with elevated risk may include: offshore companies, online gambling-related operations, and online payday lenders). For example, a processor whose customers are primarily offshore would be inherently riskier than a processor whose customers are primarily restaurants.
- Determining whether the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization (ISO) opportunities" or "gateway" arrangements.[119]
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.
- Identifying the processor's major customers.
- Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.

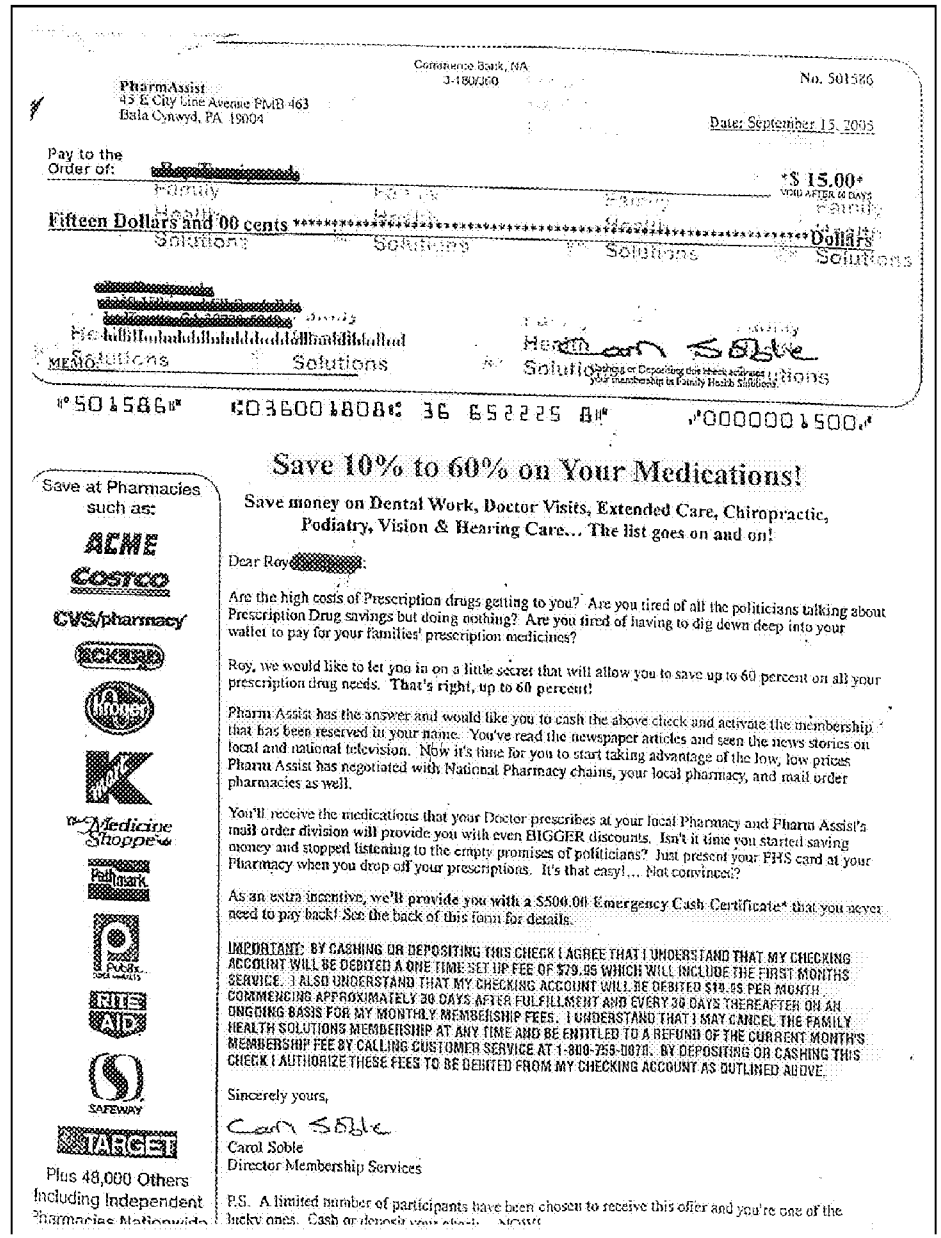
Banks that provide account services should monitor their processor relationships for any significant changes in the processors' business strategies that may affect their risk profile. Banks should periodically re-verify and update the businesses' profiles to ensure the risk assessment is appropriate.

In addition to adequate and effective account opening and due diligence procedures for processor accounts, management should monitor these relationships for unusual and suspicious activities. To effectively monitor these accounts, the bank should have an understanding of the following processor information:

- Merchant base.
- Merchant activities.
- Average number of dollar volume and number of transactions.
- "Swiping" versus "keying" volume for credit card transactions.
- Charge-back history.

[119] Gateway arrangements are similar to an Internet service provider with excess computer storage capacity who sells its capacity to a third party, who would then distribute computer service to various other individuals unknown to the provider. The third party would be making decisions about who would be receiving the service, although the provider would be providing the ultimate storage capacity. Thus, the provider bears all of the risks while receiving a smaller profit.

Incentives to Induce Authorization



Commerce Bank, NA
3-180/360

No. 501586

PharmAssist
45 E City Line Avenue PMB 463
Bala Cynwyd, PA 19004

Date: September 15, 2005

Pay to the Order of: [redacted]

$ 15.00
VOID AFTER 60 DAYS

Fifteen Dollars and 00 cents ********** Dollars

[redacted]

Solutions

Depositing this check activates your membership in Family Health Solutions.

⑈501586⑈ ⑆036001808⑆ 36 652225 8⑈ ⑈000001500⑈

Save at Pharmacies such as:

ACME
Costco
CVS/pharmacy
Eckerd
K
Medicine Shoppe
Pathmark
RITE AID
SAFEWAY
TARGET

Plus 48,000 Others Including Independent Pharmacies Nationwide

Save 10% to 60% on Your Medications!

Save money on Dental Work, Doctor Visits, Extended Care, Chiropractic, Podiatry, Vision & Hearing Care... The list goes on and on!

Dear Roy [redacted]:

Are the high costs of Prescription drugs getting to you? Are you tired of all the politicians talking about Prescription Drug savings but doing nothing? Are you tired of having to dig down deep into your wallet to pay for your families' prescription medicines?

Roy, we would like to let you in on a little secret that will allow you to save up to 60 percent on all your prescription drug needs. **That's right, up to 60 percent!**

Pharm Assist has the answer and would like you to cash the above check and activate the membership that has been reserved in your name. You've read the newspaper articles and seen the news stories on local and national television. Now it's time for you to start taking advantage of the low, low prices Pharm Assist has negotiated with National Pharmacy chains, your local pharmacy, and mail order pharmacies as well.

You'll receive the medications that your Doctor prescribes at your local Pharmacy and Pharm Assist's **mail order division will provide you with even BIGGER discounts.** Isn't it time you started saving money and stopped listening to the empty promises of politicians? Just present your FHS card at your Pharmacy when you drop off your prescriptions. It's that easy!... Not convinced?

As an extra incentive, **we'll provide you with a $500.00 Emergency Cash Certificate*** that you never need to pay back! See the back of this form for details.

IMPORTANT: BY CASHING OR DEPOSITING THIS CHECK I AGREE THAT I UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED A ONE TIME SET UP FEE OF $79.95 WHICH WILL INCLUDE THE FIRST MONTHS SERVICE. I ALSO UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED $19.95 PER MONTH COMMENCING APPROXIMATELY 30 DAYS AFTER FULFILLMENT AND EVERY 30 DAYS THEREAFTER ON AN ONGOING BASIS FOR MY MONTHLY MEMBERSHIP FEES. I UNDERSTAND THAT I MAY CANCEL THE FAMILY HEALTH SOLUTIONS MEMBERSHIP AT ANY TIME AND BE ENTITLED TO A REFUND OF THE CURRENT MONTH'S MEMBERSHIP FEE BY CALLING CUSTOMER SERVICE AT 1-800-755-0078. BY DEPOSITING OR CASHING THIS CHECK I AUTHORIZE THESE FEES TO BE DEBITED FROM MY CHECKING ACCOUNT AS OUTLINED ABOVE.

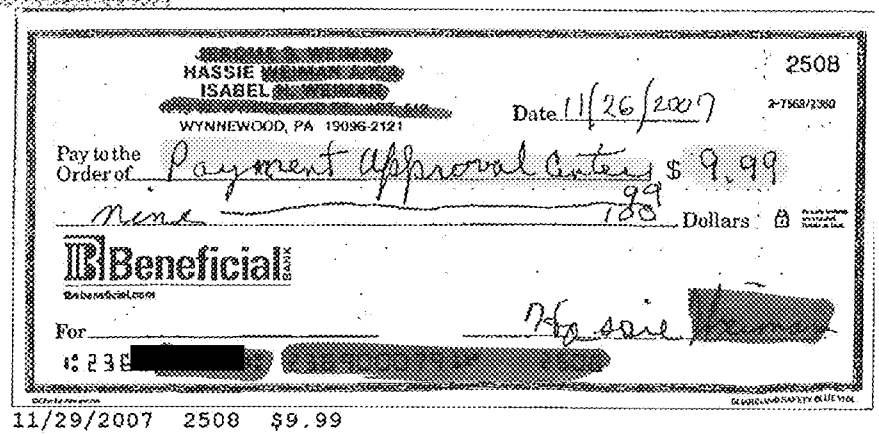
Sincerely yours,

Carol Soble
Director Membership Services

P.S. A limited number of participants have been chosen to receive this offer and you're one of the lucky ones. Cash or deposit your check... NOW!

Incentives for Purported Authorization

Beneficial SAVINGS BANK


HASSIE [redacted]
ISABEL [redacted]
WYNNEWOOD, PA 19096-2121

2508

Date 11/26/2007

Pay to the Order of Payment Approval Entry $ 9.99

nine 99/100 Dollars

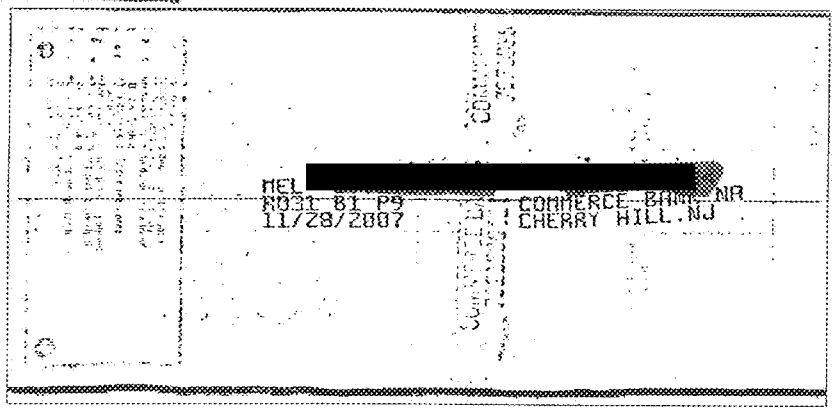
Beneficial

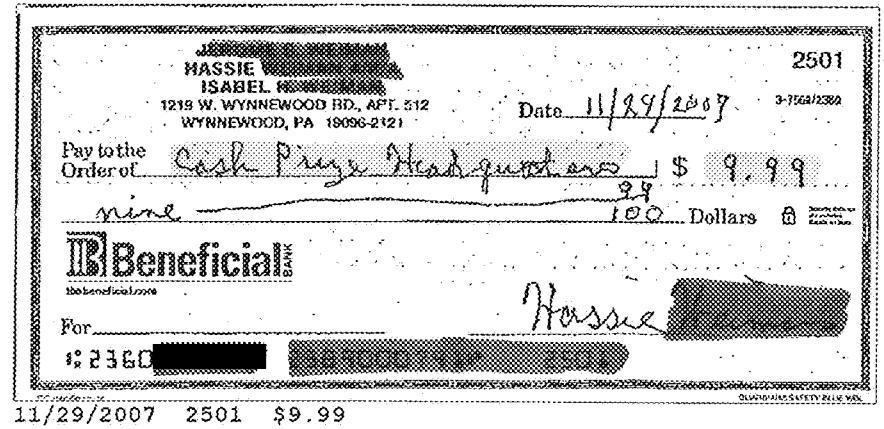
For

Hassie [redacted]

:0238[redacted]

11/29/2007 2508 $9.99


MEL [redacted]
R031 81 P9
11/28/2007
COMMERCE BANK NA
CHERRY HILL,NJ


HASSIE [redacted]
ISABEL [redacted]
1219 W. WYNNEWOOD RD., APT. 512
WYNNEWOOD, PA 19096-2121

2501

Date 11/29/2007

Pay to the Order of Cash Prize Headquarters $ 9.99

nine 99/100 Dollars

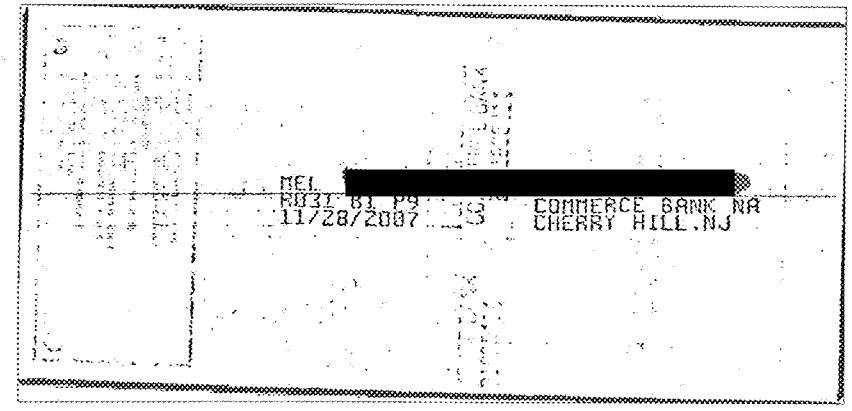
Beneficial

For

Hassie [redacted]

:02360[redacted]

11/29/2007 2501 $9.99


MEL [redacted]
R031 81 P9
11/28/2007
COMMERCE BANK NA
CHERRY HILL,NJ

Prime Time Checking

Account Number: [redacted]
Statement Date: October 31, 2007
Page 1 of 3

HASSIE [redacted]
ISABEL [redacted]
WYNNEWOOD PA 19096

- For Customer Service during business hours call **215.864.6730** or e-mail us at **info@BeneficialSavingsBank.com**
- For 24-hour account information call DirectLink at **215.864.1799** or **1.800.784.8490**
- For other information visit us at **www.BeneficialSavings.com**

Account Summary

Previous Statement Balance As Of 09/30/07	1,864.08
Total Withdrawals/Charges	2,625.50
Total Deposits/Credits	3,560.02
Ending Balance	3,798.60

Annual Percentage Yield Earned: 0.50%

Check Summary

Checks Enclosed: 7

Date	Chk No.	Amount	Date	Chk No.	Amount	Date	Chk No.	Amount
10/01	2439	40.00	10/18	2462	438.50	10/18	2466	237.00
10/10	2463	13.86	10/19	2464	159.46	10/26	2470	9.95
10/24	2460*	10.00						

* Denotes Gap in Check Number Sequence

Other Transactions

Date	Description	Deposit(+) Withdrawal(-)
10/02	Ac-Us Treasury 303 -Soc Sec	565.00+
10/02	Ac-Us Treasury 303 -Soc Sec	1,194.00+
10/02	Ac-Car -Convcheck Ck-000000000002444	24.99-
10/02	Ac-Ppd -Convcheck Ck-000000000002446	27.99-
10/02	Ac-Pnd -Convcheck Ck-000000000002447	27.99-
10/02	Ac-App -Convcheck Ck-000000000002448	34.99-
10/03	Ac-Pm -Convcheck Ck-000000000002445	25.99-
10/05	Ac-Sdrd -Convcheck Ck-000000000002450	23.99-
10/05	Ac-Dcd Main Office -Convcheck Ck-000000000002449	24.99-
10/17	Ac-Ppa -Convcheck Ck-000000000002457	27.99-
10/17	Ac-Sdn -Convcheck Ck-000000000002458	25.99-
10/19	Ac-At&T Consumer -Checkpaymt Ck-00002461	77.46-
10/23	Ac-Rda -Convcheck Ck-000000000002467	31.99-
10/24	Ac-Adrd -Convcheck Ck-000000000002468	19.99-
10/24	Ac-Sr -Convcheck Ck-000000000002465	25.00-
10/25	Ac-Dpd Main Office -Convcheck Ck-000000000002469	31.99-
10/25	Ac-Reporting Data D -Convcheck Ck-000000000002471	24.99-

From Target Gift Card to Automated Electronic Mortgage Payment

WACHOVIA

P.O. Box 900001
Raleigh, NC 27675-9001

MORTGAGE STATEMENT

ACCOUNT INFORMATION:

Statement Date:	10/05/06
Loan Number:	
Interest Rate:	5.9900
NEXT PAYMENT DUE DATE:	11/01/06
Current Payment:	$949.28
Pa	
Ur	
Ot	
TC	949.28
Ha	
Cu	
Cu	

Philadelphia PA 19144-3725

Property Address:

PHILADELPHIA PA 19144

Activity Since Your Last Statement:

Date	Description	Principal	Interest	Escrow	Other	tal
08/01	Payment	$175.59	$764.69		$9.00	$949.28
09/01	Payment	$176.46	$763.82		$9.00	$949.28
10/02	Payment	$177.35	$762.93		$9.00	$949.28

Account Summary:

Loan Balance* As of 10/05/06	Interest Paid Year to Date	Escrow Balance As of 10/05/06	Taxes Paid Year to Date

Incentives to Induce Authorization

HOMEQ SERVICING **$20.00 Target® GiftCard**

Expiration Date
01/26/2005

Exclusively For

PHILADELPHIA PA 19144 3725

Please sign and return this reply form with your mortgage payment to get your $20.00 Target GiftCard and to activate your Great Fun privileges [illegible] the free trial period, I may cancel at any time, for any reason [illegible] By signing below I authorize HomEq to provide Great Fun [illegible] benefits. Additionally I [illegible]

X ________ SIGNATURE REQUIRED FOR PROCESSING

Sign and return this form to claim the $20.00 Target GiftCard reserved for you
THIS FORM IS NOT REDEEMABLE AT ANY TARGET LOCATION

ZC7615 Z743475 [illegible] HCB 0303297089

HOGR-3PPP000080

Payment Processing Center, LLC

- Provides "end-to-end solutions" for telemarketing merchants

- Specializes in "Bank Draft origination for telephone **transactions that may be prohibited**" by NACHA rules

: lmeojhlihcbbcapbcmliiebhcaaa.justin@paymentprocessingcenter.com
= 0000000353
: 00000000D8B3FD5A785EC54E87ADC17FEBD9131424232100
: To the fine people that made hellish phone abuse a little more bearable,
Thank you for making my summer a little less tedious and a little more

, I am glad to have shared the daily death-threats, hate-filled rants, and ignorance with all of you. I think sometime in the next couple weeks I may almost (in some kind of sick way) miss the sound of shit-kickers screamed obsenities over the verification playback.

bacon-speckled tomato soup, dealt with a phonebook's worth of customer callbacks, and a lot of soggy bread from the sandwich club.
When you come into work on Monday don't be sad that my cute little ass isn't around, be happy... because finally one of us will get to know what daylight looks like during a weekday. Just remember my smiling face and boyish good

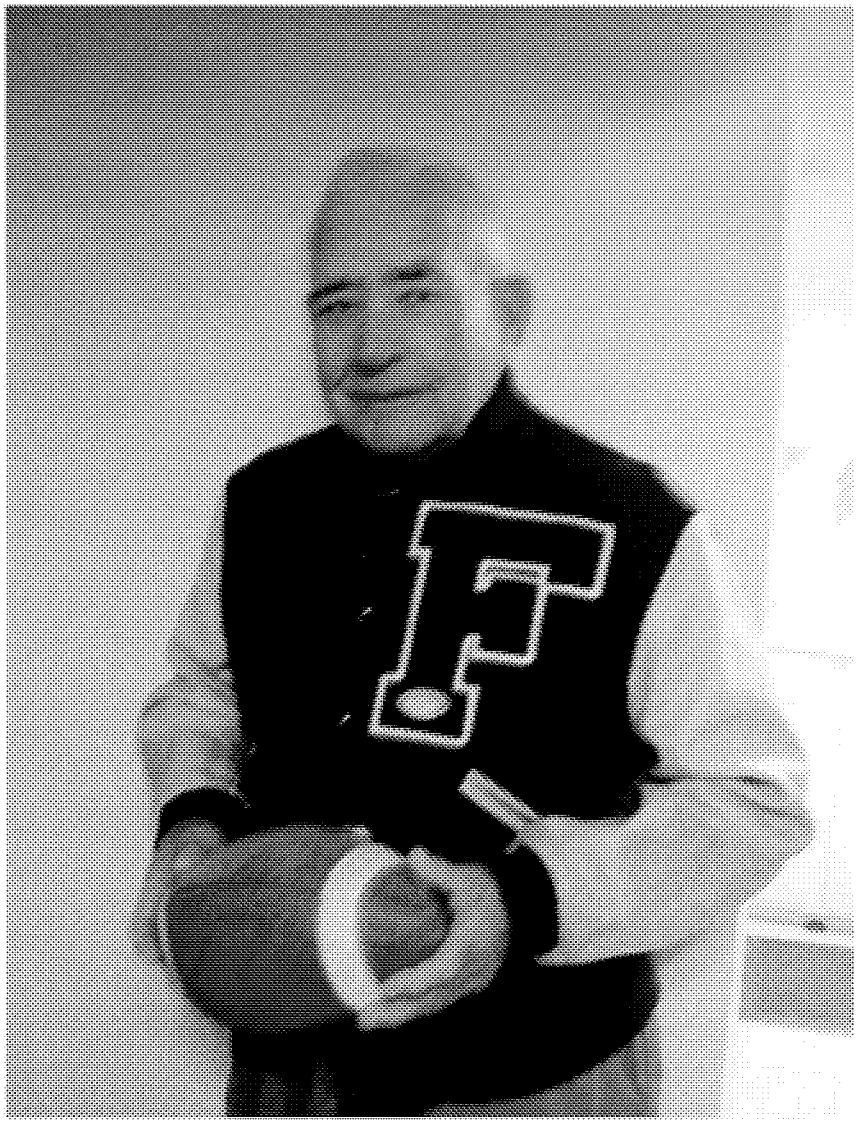
I know the customer service number and I'm not afraid to call with my bank rep on the line)

Now, as I hang up my Steno Pad and descend back in to a world of relative normality I would like to say THANK YOU to everyone.

Side note to Michael: How much exactly do I owe you for the knowledge that it takes a total of 16 combined brain cells and teeth to provide your bank account information to a stranger on the phone to order something with as stupid a name as Washballs? or; the knowledge that old people are just plain easy to trick?

stay in touch,
Justin

Purported Authorization Obtained By Telemarketer



David XXX, Sr.

1933-2006

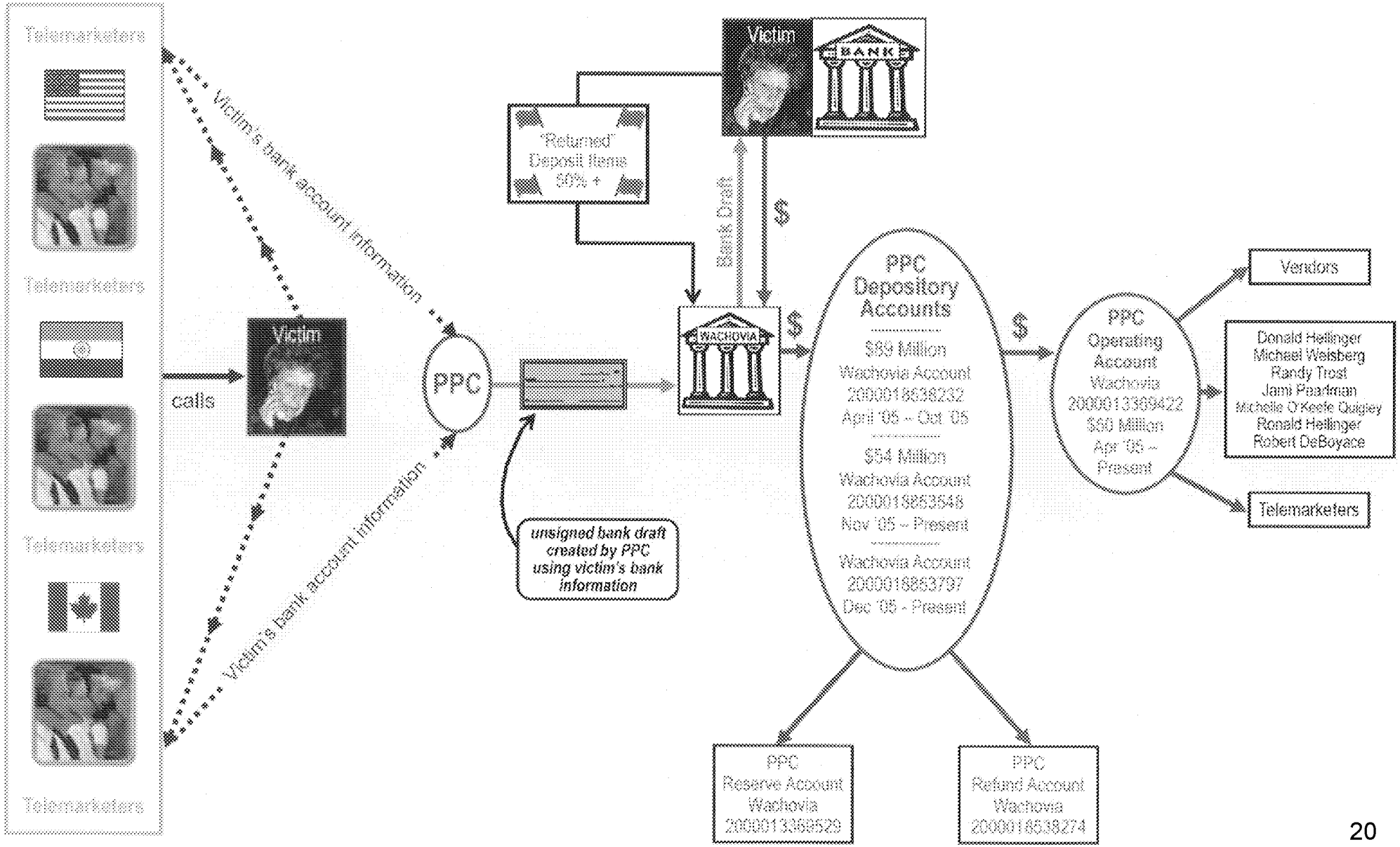
University Football Coach

Little League Coach

Sunday School Teacher

Husband, Father, Grandfather, Brother

The Payment Process

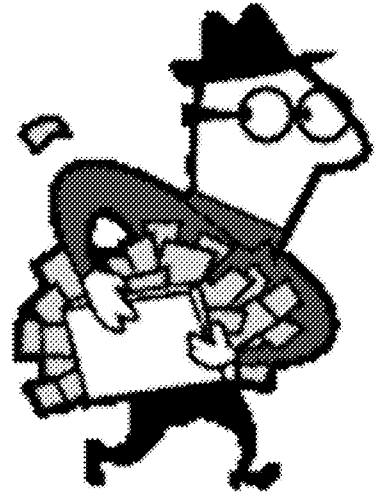


A Mutually Profitable Relationship!

Dollar value of RCCs deposited by PPC with Wachovia in 12-month period: **$162,000,000**

Income from RCC fees:

PPC – **approx. $8,000,000**
Bank – **approx. $1,900,000**



Wachovia: Victim or Participant?

- Knew or remained willfully blind to fact that PPC serviced mass market fraudsters
- Ignored glaring red flags
- Suppressed internal concerns
- Ignored express warnings from other banks
- Entered agreements with PPC to protect its own interests at the expense of the interests of other banks and their customers

Failure in Due Diligence
PPC's Telemarketing Merchants

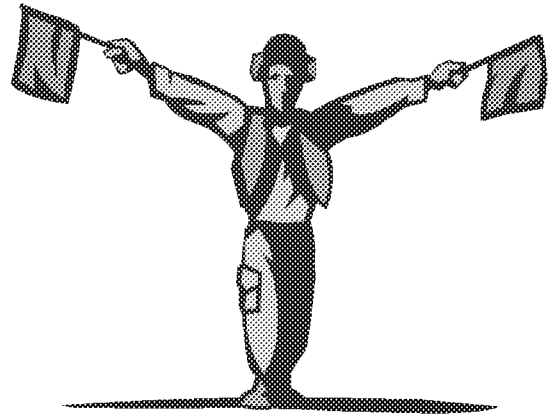
- Facially suspicious product offers and marketing scripts
  - Grant offers
  - Prescription discount cards
  - Travel Programs
  - Free Gift Cards
  - Free Computers
- Merchants mostly based overseas and/or using foreign banks
- Exploited names of legitimate companies, such as Wal-Mart, K-Mart, Home Depot, Carnival Cruises, AIG

Eyes Wide Shut

- PPC merchants were fraudsters well-known to Better Business Bureaus, state Attorneys General, and consumer protection websites
  - Star Communications
  - Advantage America
  - Suntasia
- As successive payment processers were shut down by law enforcement, Wachovia continued to process RCCs for same fraudulent merchants

Returns – Charge Backs

- At inception, Wachovia **anticipated returns exceeding 35 percent** (compared to approximately 1/2 of 1 percent for all checks)
- Actual returns exceeded **50 percent**
- Wachovia charged PPC substantial fee for returns
- Wachovia offered PPC volume discounts on return fees



Return Reasons

- More than 50 percent of PPC's returns facially identified as:
  - UNAUTHORIZED
  - FRAUD
  - REFER TO MAKER

- Every month Wachovia received and hand-processed thousands of **sworn affidavits from consumers alleging that PPC debit transactions were not authorized**

Banknorth, N.A.

AFFIDAVIT OF UNAUTHORIZED CONSUMER DRAFT

(Type or Print Neatly)

Bank: Banknorth Massachusetts
Banking Center: SW Commons/39
RC: 3390
Telephone #: (508) 754 - 6745

Use this form for drafts with the following tran codes only:
184 POD Check
187 Check

[redacted] Customer's Name
[redacted] Account Number
[redacted] Street
Apt. #
P.O. Box
Worcester City MA State 01604 Zip
[redacted] Daytime Telephone
Home Telephone

I declare, swearing under oath, that a draft charged to my account and appearing on my account statement is UNAUTHORIZED.

Check appropriate Section I OR Section II:

I. Draft Never Authorized:

☒ I have never authorized the company named above to debit my account

☐ I authorized the company named above to debit my account, but I revoked ** the authorization on _____ Date of Revocation in the manner specified in said authorization.

** Customer must provide Bank with a copy of the written revocation

I further declare that the above transaction was not initiated by me or by any person acting on my behalf. In signing this form, I understand that the Bank will reverse any credit(s) to my account if it receives proof from the payee of the draft that I, in fact, authorized this draft.

[redacted] Customer Signature (required)
5-17-05 Date
Banking Center Representative

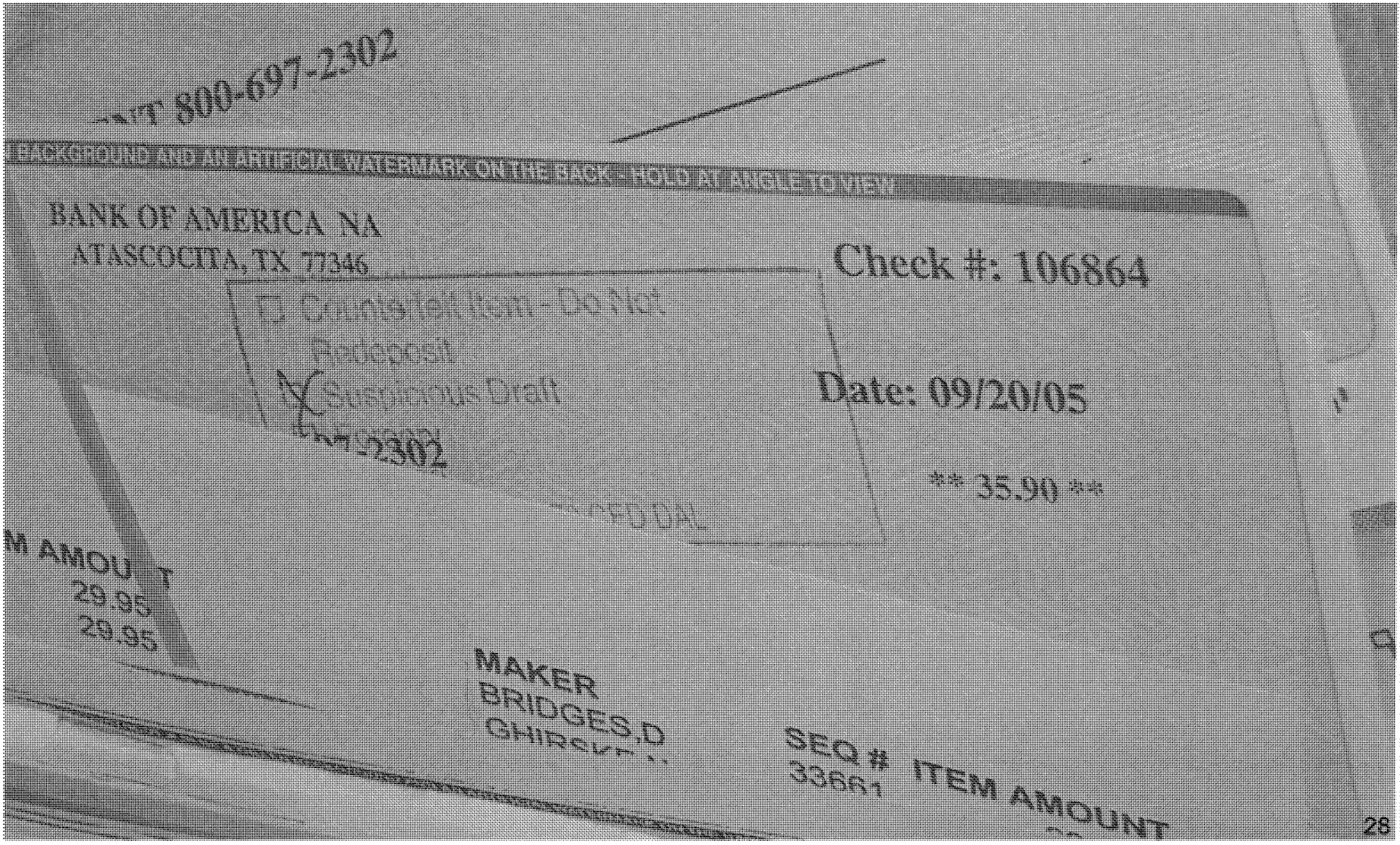
FOR USE ON PERSONAL ACCOUNTS ONLY

Instructions:

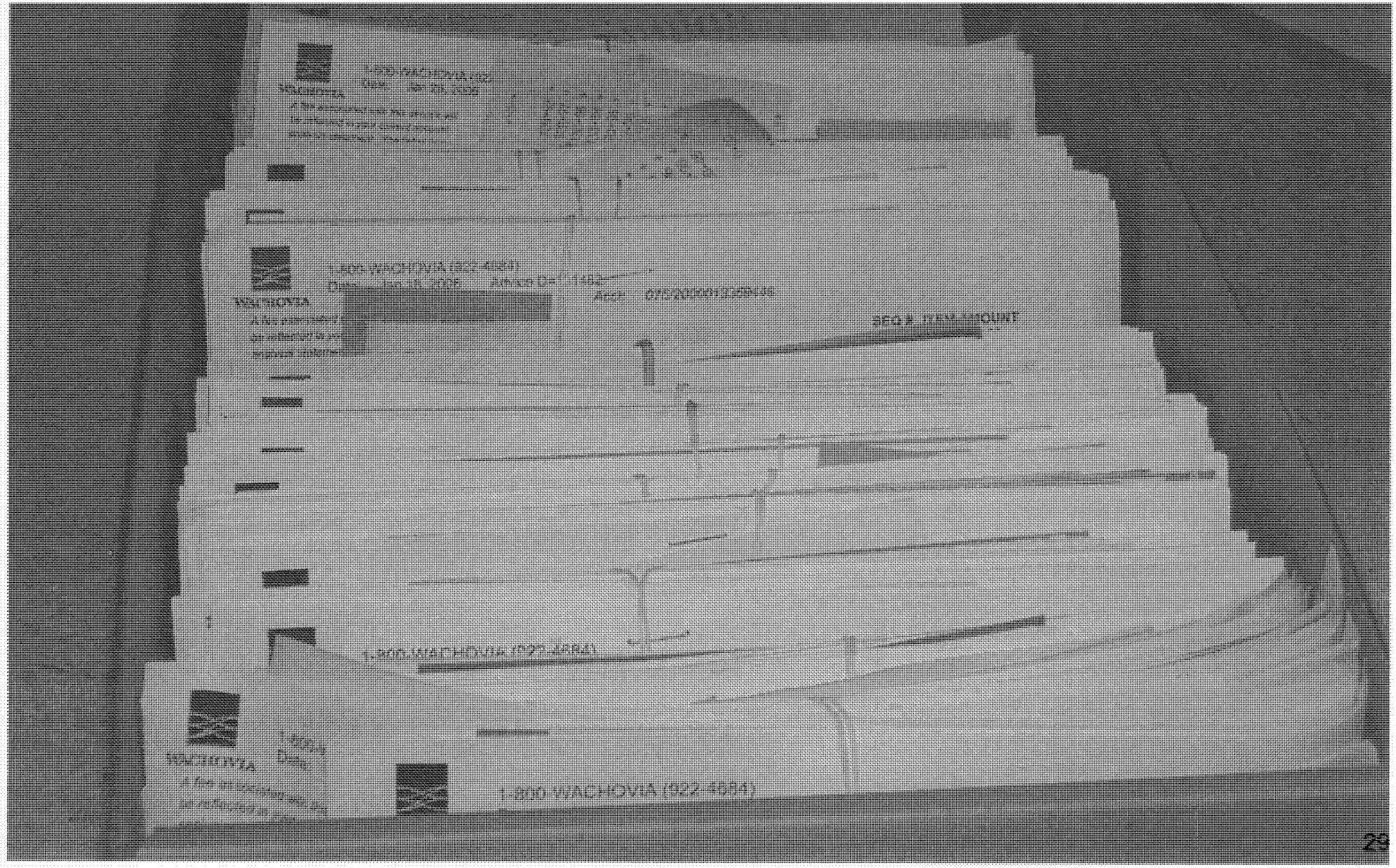
1. Fax to Adjustment Department 207-755-6315 OR Send a copy of the returned item (if available) and the signed affidavit through interoffice mail to: *Adjustment Department ME091-31*
2. Place a stop payment for the amount of the draft on the customer's account to prevent any future drafts from processing to the account. Have customer sign Stop Payment Order and remit form as usual.
3. Advise customer that provisional credit will NOT be granted on this transaction. Customer account will only be credited upon Bank receiving credit back from draft originator.

Affidavit of Unauthorized Consumer Draft Rev. 03/2004

A Returned Item



A Box of Returned Items

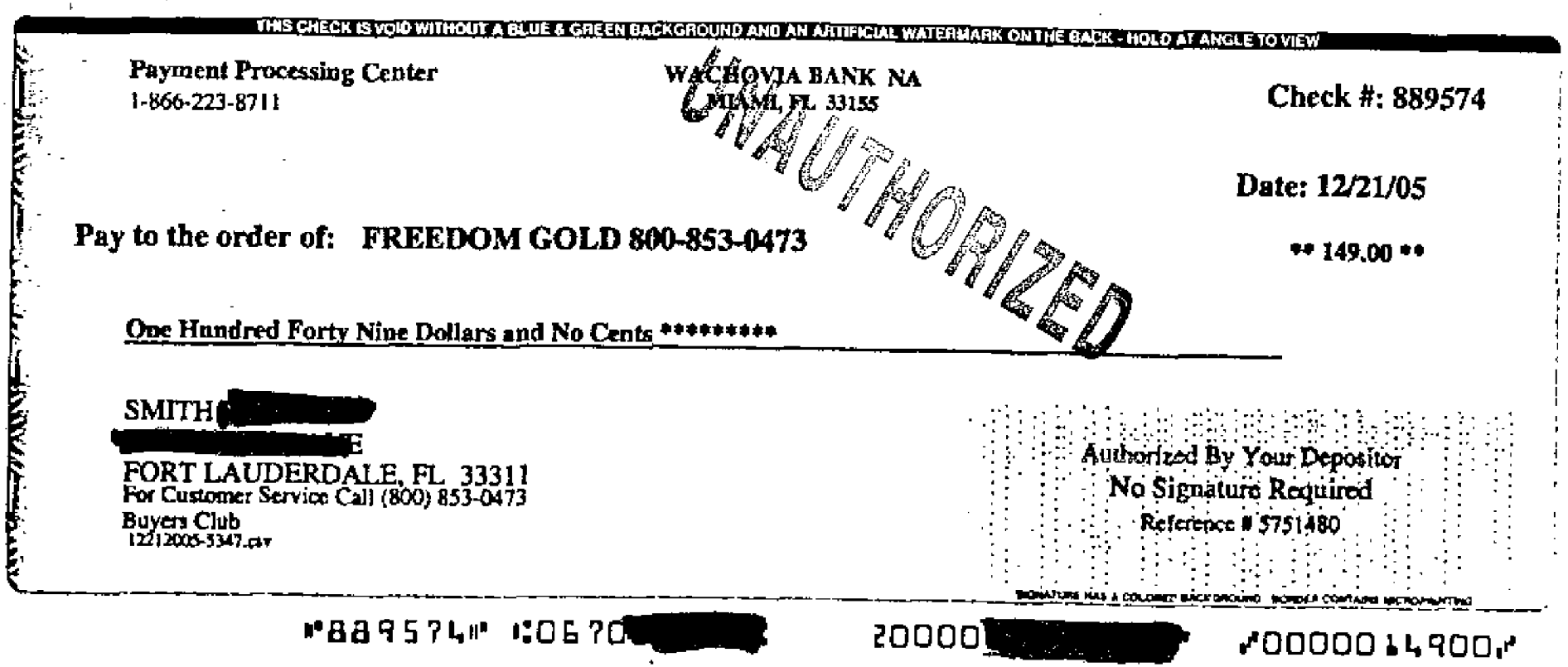


A Room of Boxes of Returned Items

Outlier Business Practices

- PPC regularly transferred large amounts of money to overseas accounts.
- Wachovia allowed PPC to deposit RCCs payable to third-party merchants into its own accounts – without agency agreements.
- The Wachovia/PPC business model was based on large volumes of returns – an ordinarily suspect and undesired result.
- Wachovia's own customers often treated differently than other banks' customers.

"On the House" Returns



THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK - HOLD AT ANGLE TO VIEW

Payment Processing Center
1-866-223-8711

WACHOVIA BANK NA
MIAMI, FL 33155

UNAUTHORIZED

Check #: 889574

Date: 12/21/05

Pay to the order of: FREEDOM GOLD 800-853-0473

** 149.00 **

One Hundred Forty Nine Dollars and No Cents *********

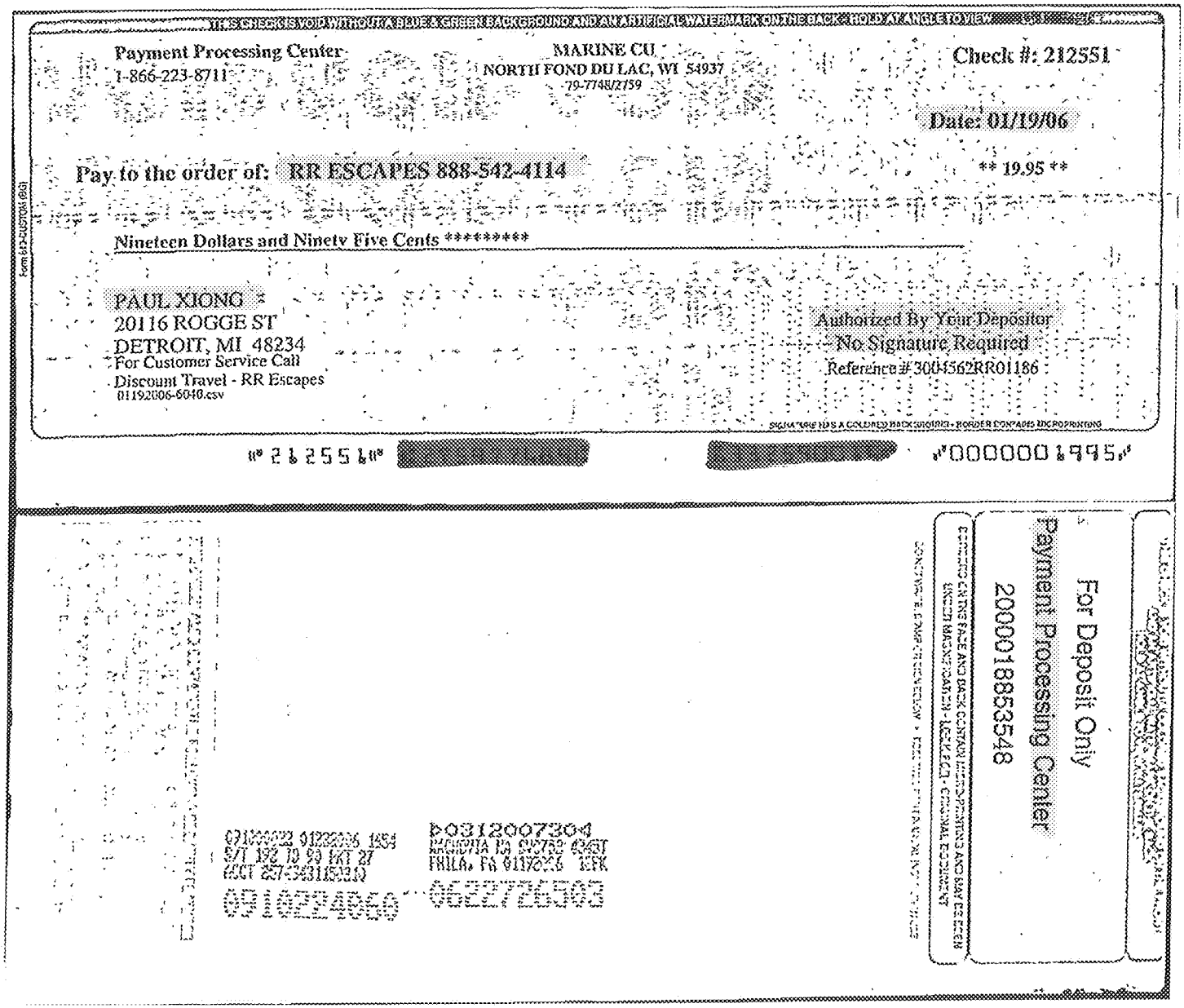
SMITH [redacted]
[redacted]E
FORT LAUDERDALE, FL 33311
For Customer Service Call (800) 853-0473
Buyers Club
12212005-5347.csv

Authorized By Your Depositor
No Signature Required
Reference # 5751480

SIGNATURE HAS A COLORED BACKGROUND BORDER CONTAINS MICROPRINTING

⑈889574⑈ ⑆0670[redacted] 20000[redacted] ⑈000001 4900⑈

"Whack-a-Mole"



Payment Processing Center
1-866-223-8711

MARINE CU
NORTH FOND DU LAC, WI 54937
79-7748/2759

Check #: 212551

Date: 01/19/06

Pay to the order of: RR ESCAPES 888-542-4114

** 19.95 **

Nineteen Dollars and Ninety Five Cents **********

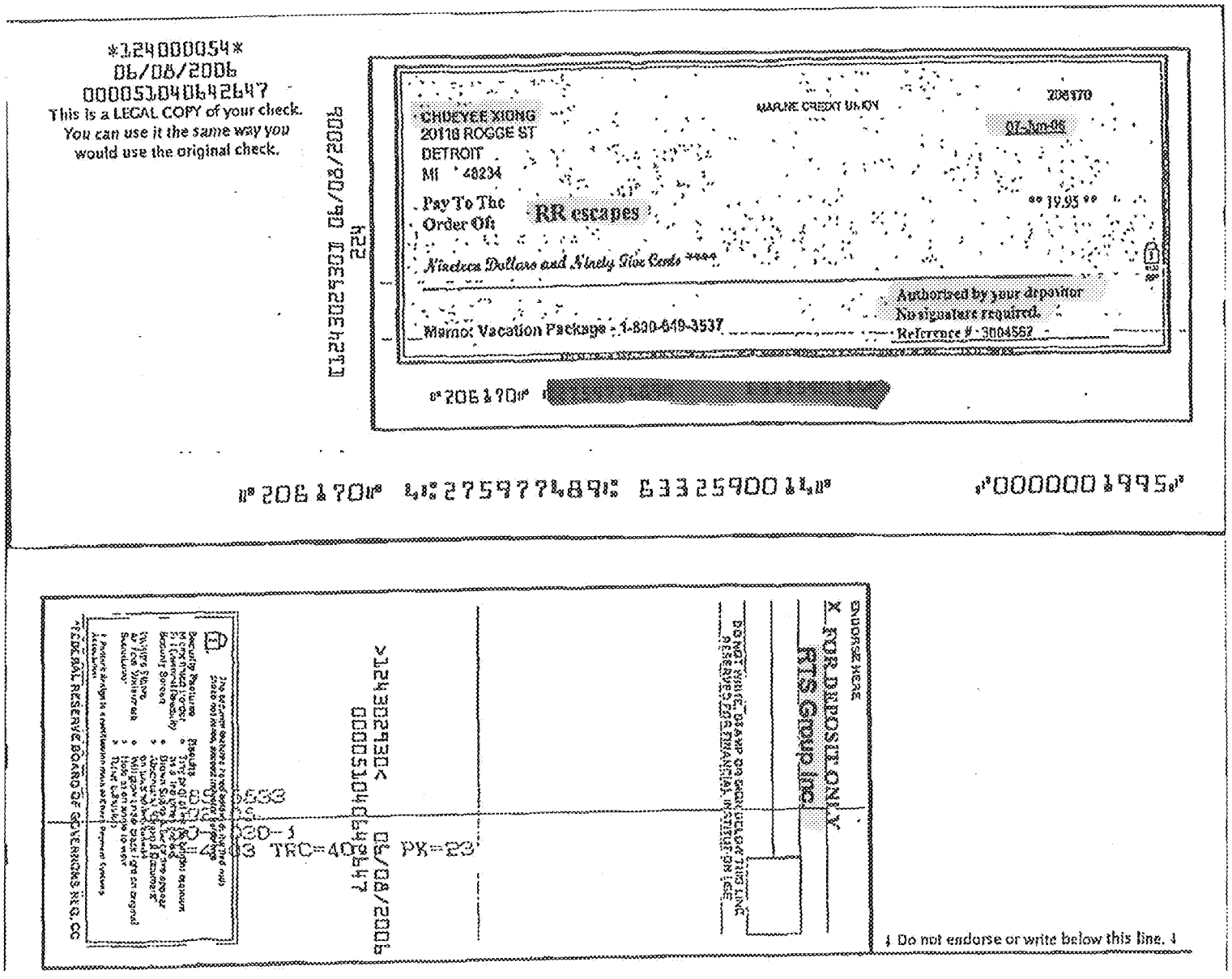
PAUL XIONG
20116 ROGGE ST
DETROIT, MI 48234
For Customer Service Call
Discount Travel - RR Escapes
01192006-6040.csv

Authorized By Your Depositor
No Signature Required
Reference#3004562RR01186

"212554" [redacted] [redacted] "000001995"

For Deposit Only
Payment Processing Center
200001885348

Migration from National Bank to Community Bank



Wachovia Ignored Internal Concerns

Return "volumes are tremendous" and "payment of these items is not our normal process"

Returns Operations Supervisor to VP of Loss Management

"Nothing [PPC] could ever do would make me comfortable . . ."

Bank Loss Management Official after learning about Bank relationship with PPC

After Loss Management official recommended closing PPC accounts, wrote "business line has assumed risk for the customer and decided to keep their accounts open"

Communication between Bank Loss Management Officials

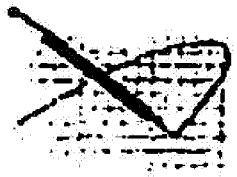
Wachovia Ignored Internal Concerns

"Please consider the regulatory and reputational risks involved here. **We have now been put on notice that accounts at [Bank] are being used . . . to further these schemes.**

"If PPC has in place 'a standing agreement with [Bank] to pay all claims without dispute,' then they know they have rogue telemarketers in their customer base."

Internal E-mail from Bank's In-house Counsel after receiving fraud warning from another bank

DOUBLE YIKES!!!!



08/23/2005 06:35 PM

To

cc

Subject Guardian Marketing # 2000027007068

Tom,
Bob, Tim & I need to huddle with you on this account relationship. It is a Business Banking account, it has been actively making deposits since 6/23/05 and there is a current balance of $743,000+ in the account. The account came to us from B of A (so we are advised by : n Bus. Bnkg.) and she is

ALL their deposits are THIRD PARTY DRAFTS!!! DOUBLE YIKES!!!!

YIKES!!!! Moreover, the drafts that are being deposited and are charging back, are not $99.99; these items are all over the place in terms of their amount. Moreover, there is another account, Suntasia, #2000027027721. Same address, same principals. $ from the Guardian acct is transferred to Suntasia and then the $ is wired out to Bank of America (funny, I thought I said they were leaving B of A at the beginning of this note, didn't I??). And, there is more, but nothing more that I want to put into a note. Bob and I really need to talk o you on tomorrow,

Thanks,

Wachovia Ignored Explicit Fraud Warnings From Other Banks

"The purpose of this message is to **put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam . . .** instigate an investigation into whether [PPC is] conducting legitimate business and whether [Bank is] getting **a high volume of return items on those accounts (that should place your bank on notice of potential fraud).**"

E-Mail from Citizens Bank

Bank's "Oral Agreement" With PPC To Pay All Returns

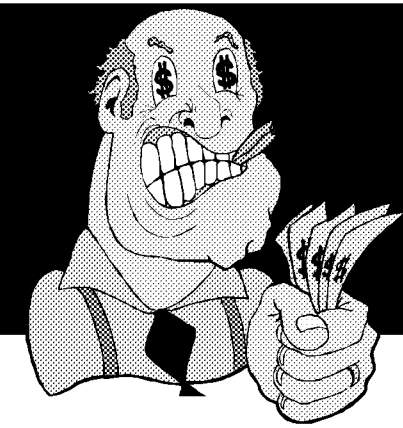
- Intended to protect Bank's reputation rather than consumers

"[I]f we can find a way to pay the returns . . . without sending them back to other banks, I think that will go a long way to preserve our reputation. **The sooner the complaint gets paid the quicker it goes away."**

Internal Bank e-mail

- Demonstrates that UCC warranty rule is not an effective anti-fraud tool

Money Motivates



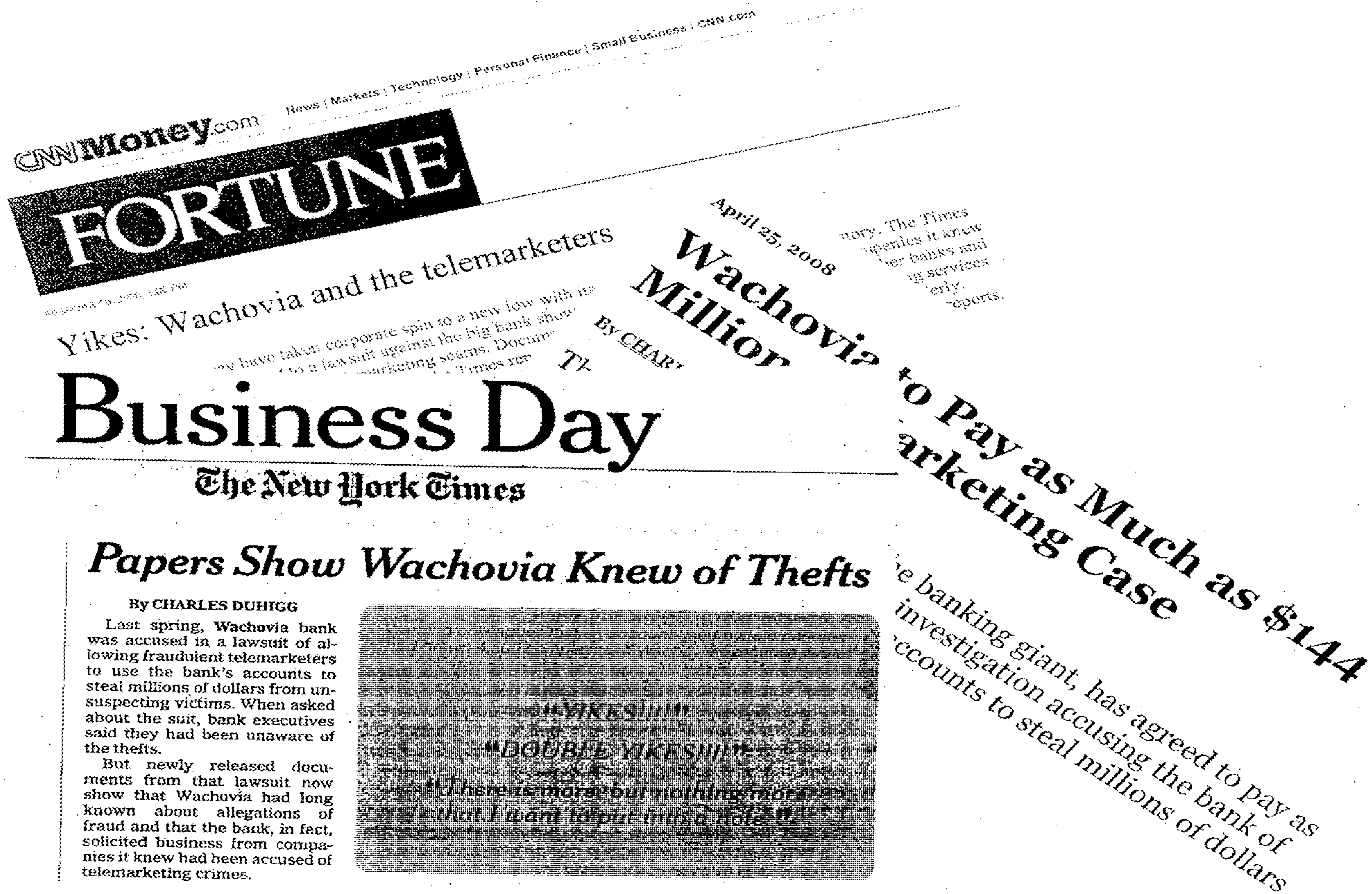
"[P]lease mark your calendar – we will take them somewhere nice for lunch. We are making a ton of money from them."

Bank Relationship Manager to Senior Business Development Officer

"[T]his is our most profitable account. $1mm per year in profit. They have asked for Eagle tickets. What can we do?? They deserve them with all we make from them."

Bank Relationship Manager to Senior Business Development Officer

What's a reputation worth?



CNNMoney.com News | Markets | Technology | Personal Finance | Small Business | CNN.com

FORTUNE

Yikes: Wachovia and the telemarketers

Business Day

The New York Times

April 25, 2008

Wachovia to Pay as Much as $144 Million ... Marketing Case

banking giant, has agreed to pay as ... investigation accusing the bank of ... accounts to steal millions of dollars

Papers Show Wachovia Knew of Thefts

By CHARLES DUHIGG

Last spring, **Wachovia** bank was accused in a lawsuit of allowing fraudulent telemarketers to use the bank's accounts to steal millions of dollars from unsuspecting victims. When asked about the suit, bank executives said they had been unaware of the thefts.

But newly released documents from that lawsuit now show that Wachovia had long known about allegations of fraud and that the bank, in fact, solicited business from companies it knew had been accused of telemarketing crimes.

"YIKES!!!!"

"DOUBLE YIKES!!!!"

"There is more but nothing more that I want to put into a note."

Yes – it *is* a crime.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 10-20165 CR - LENARD
31 U.S.C. § 5318(h)
31 U.S.C. § 5322(a)

MAGISTRATE JUDGE
BRANNON

UNITED STATES OF AMERICA

v.

WACHOVIA BANK, N.A.,

Defendant.

FILED by D.C.
MAR 12 2010
STEVEN M. LARIMORE
CLERK U. S. DIST. CT.
S. D. of FLA. – MIAMI

INFORMATION

The United States Attorney charges that:

GENERAL ALLEGATIONS

At all times material to this Information

1. Defendant **WACHOVIA BANK, N.A.** was a national banking association based in Charlotte, North Carolina.

It's not over until it's over.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	CRIMINAL NO. 11-
	:	DATE FILED: February 10, 2011
v.		
	:	VIOLATIONS:
DONALD HELLINGER		18 U.S.C. § 371 (conspiracy – 1 count)
RONALD HELLINGER	:	18 U.S.C. § 1960 (operating an illegal money
MICHAEL WEISBERG		transmission business – 1 count)
RANDY TROST	:	18 U.S.C. § 1955 (operating an illegal gambling
JAMI PEARLMAN		business – 1 count)
MICHELE QUIGLEY	:	18 U.S.C. § 1084 (transmission of wagers and
		wagering information – 8 counts)
	:	18 U.S.C. § 1956(a)(2)(A) (international money
		laundering – 3 counts)
	:	Notice of forfeiture

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES THAT:

At all times relevant to this indictment:

BACKGROUND

1. Defendants DONALD HELLINGER, RONALD HELLINGER, MICHAEL WEISBERG, RANDY TROST, JAMI PEARLMAN, and MICHELE QUIGLEY

Financial accountability -- thanks to federal agents, prosecutors, and bank regulators, class action attorneys, local and state law enforcement, *The New York Times*, and many determined victims of consumer fraud !

Important steps forward . . .

- Guidance to banks from FDIC, OCC and FinCEN
- United States v. First Bank of Delaware
- Financial Fraud Enforcement Task Force/Consumer Protection Branch efforts to choke-off fraudsters' access to payment systems (DOJ, FTC, FDIC-OIG, USPIS, FBI, and others)
- May 21, 2013: FTC Notice of Proposed Rulemaking would ban the use of RCCs in connection with telemarketing

New Regulatory Loophole

- Treasury Department regulation amended in 2011 arguably excludes third-party payment processors from the definition of "money transmitter" and thus is not a Money Services Business ("MSB).
  - A single-storefront check cashing business is a MSB and must register with FinCEN and comply with the BSA.
  - A "Bitcoin" exchange is a MSB and must register with FinCEN and comply with the BSA.
  - **But, because of the new loophole, a payment processor that originates tens of millions of dollars of debit transactions against consumers' bank accounts on behalf of Internet and telemarketing merchants is not an MSB and is not required to register with FinCEN or comply with the BSA.**

Thanks for your time and interest!

Questions?

Joel M. Sweet

[redacted]

[redacted]usdoj.gov

ACTUAL TELEMARKETING CALL WITH A CONSUMER (7 minutes- 54 seconds)

Automated Call Verifier:	*Thank you for calling the voice call verification system. Please enter the customers 10 digit[not audible] telephone number followed by the pound [# key]. The number you have entered is 4-7-8-9-2.*
Telemarketer:	Can you say your full name?
Victim:	David
Automated Call Verifier:	*After the tone, please read the long string of numbers at the bottom of your checkbook starting from left to right.*
	(peep)
Telemarketer:	Now read me the numbers because the *[not audible]*...to me one last time from extreme left to right. Yes?
Victim:	Yes. Hello.
Telemarketer:	Hello. Yeah. All the numbers from extreme left to right.
Victim:	061...Wait a minute... 06 dash, ok...
Telemarketer:	Yeah.
Victim:	000 xxx slash...umm, 1(one)...wait a minute, 000.
Telemarketer:	I'm sorry?
Victim:	000 xxx.
Telemarketer:	What is it?
Victim:	Say what?
Telemarketer:	You have to read me the second set of the numbers. The first set of the numbers is xxx 000 xxx, and then?
Victim:	Well one was a slash in there, you know.
Telemarketer:	Uh uh. Uh uh. And then the account number.
Victim:	Lets check that one.
Telemarketer:	And what is this number xxx xxx xxx xxx? You have to give me one number right?
Victim:	Well listen, I got numbers all over the bottom of this check.
Telemarketer:	OK. So just read me the first set of the number that is xxx xxx xxx. Ok. And that is it. And what is the second set of the number?

Victim:	Oh, the last number.
Telemarketer:	The second set of the number. Your account number.
Victim:	3-6-double 9.
Telemarketer:	Sir, you need to be sure... just...
Victim:	I tell you...hey, I tell you what dude, you send me the info and I'll send you a check ok, or I'll send you a money order.
Telemarketer	I'm having the information in front of me – you need not have to send a check. ...this amount will be charged to you in the next 5 days, I'm having the information in front of me, I'm just checking the number so that we have the right information for the proper amount, ok? So I would appreciate if you would read me the number for the one last time.
Victim:	Yeah, but I would appreciate you just let me send you a check, ok.
Telemarketer:	You need not have to send a check sir.
Victim:	Huhh?
Telemarketer:	You need not have to send a check. This amount will be charged to you in the next 5 days.
Victim:	hum, hum,...you know... I don't know you... I've never seen you, I'm not looking at you. In other words,...I just don't pass out my check number ... you know what I'm talking about.
Telemarketer:	Yeah sir... I know that, I'm having the information in front of me... I'm just need to check it out. Right.
Victim:	Right.
Telemarketer:	...so just...yeah... I'm having in front of me...
Victim:	...but I'll send you a money order back or a check.
Telemarketer:	...you need not have to send...we do not accept any money orders or check by mail...this is the only payment which we are accepting toward check by phone, ok. ... *[not audible]* this is for verification...right. *[not audible]* ...correct information.
Victim:	Dangerous game...very dangerous game....
Telemarketer:	I'm sorry?
Victim:	Very dangerous game...giving out your check number. You know, hum, private number, what have you.

Telemarketer:	Sir, I'm having in front of me...you have to read me this for the verification, right.
Victim:	I'm saying that....but if them groups of sole check numbers ...check information to other people then they will hit that bank tonight.
Telemarketer:	Listen, nobody...nobody will withdraw any money without authorization right? It needs authorization of you...so you need not have to be skeptical about it. Just read me the numbers for the one last time.
Victim:	David
	(peep)
Automated Call Verifier:	*Are you over the age of 18 and an authorized user of this account?*
	(peep)
Victim:	*[not audible]* ...play again.
Automated Call Verifier:	*Are you over the age of 18 and an authorized user of this account?*
	(peep)
Victim:	*[not audible]*
Telemarketer:	Is that a yes?
Victim:	I'm gonna send it to you at *[not audible]*.
Telemarketer:	and your...and this is your account right?
Victim:	*[not audible]*
Telemarketer:	I'm sorry?
Victim:	Yes... *[not audible]*live out of town and wife is deceased.
Telemarketer:	Uhn,uhn...and this your account?
Victim:	*[not audible]*
Telemarketer:	Yes or No?
Victim:	Yes.
Automated Call Verifier:	*After the tone please state the name and phone number of the bank where your checking account is located.*
	(peep)

Telemarketer:	Sir the name of your Bank.
Victim:	Wachovia Bank.
	(peep)
Automated Call Verifier:	*There is a onetime introductory fee of $4.95. Did you authorize that debit or check [not audible]to your checking account? Correct?*
Victim:	*[not audible]h*um, $4.95 for what? $4.99?
Telemarketer:	Sir you do authorize for $4.95 correct?
Victim:	One time?
Telemarketer:	Yes – one time. $4.95 correct?
Victim:	One time.
Telemarketer:	Is that a Yes?
Victim:	Yes…that's a yes.
	(peep)
Automated Call Verifier:	*For your convenience the checks for any of the deposits being accepted of [not audible]termed unpaid you do authorize us to create and submit additional [not audible] components too, ok?*
Victim:	What am I gonna do?
Telemarketer:	Sir, this is for your on convenience. They say the charges that you are acquire today does not clear your bank for any reason we will send a reprint of the same check to your bank. OK? That's ok?
Victim:	Yeah.
Automated Call Verifier:	*After the tone, please confirm your acceptance by stating today's date.*
	(peep)
Victim:	ahhh, really. (laughs)
Telemarketer:	You have to state today's date.
Victim:	I hadn't gotten my newspaper yet…That's where I get my dates from.
Telemarketer:	OK... so I will tell you, yesterday I believe it was November 29, 2005. So today…
Victim:	Right, ok.
Telemarketer:	Sir you have to state today's date.

Victim:	...ahh, November...oh, its December 1st... no, November 29th?
Telemarketer:	Yesterday. It was yesterdays. You have to state today's date.
Victim:	...ahh, November 31st, that's it if we got a 31st.
Telemarketer:	I'm sorry?
Victim:	Its the 31st month... of the 30th or what.
Telemarketer:	Sir yesterday I believe it was November 29, 2005, so today is...
Victim:	Ok...November 20th... November 30th, ahh (laughs)
Telemarketer:	Wait...sir, just stay on line go the *[not audible]*read about the packet, I will be right back. Do not hang up, you got to have your striking number at the end of the verification. Stay on line.
Automated Call Verifier:	*800 xxx xxxx is the customer ...*

.....

CALL ENDS HERE

United States of America
v.
Payment Processing Center

A Case Study of Remotely Created Check Abuse and Payment System Vulnerabilities

Joel M. Sweet, AUSA
United States Attorney's Office for the Eastern District of Pennsylvania

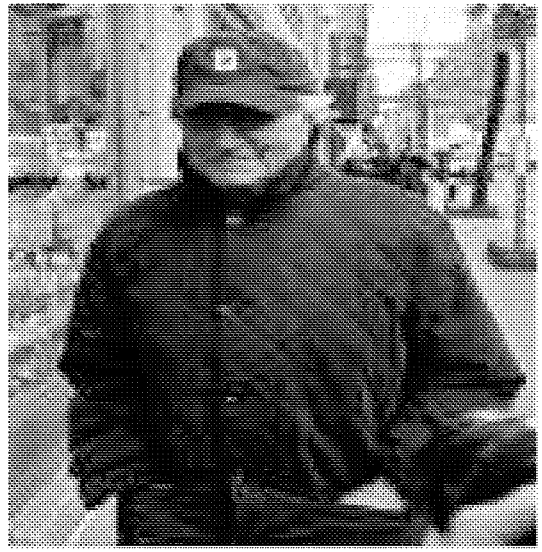
Disclaimer

Any opinions reflected in this presentation are those of the presenter and are not necessarily those of the Department of Justice, or any government official, agency, department, or branch.

The information in this presentation is from public sources.

Consumer Fraud – a National Scourge

Bernie Madoff swindled more than $40Billion.



Imagine another Bernie Madoff EVERY YEAR!

Congress has estimated that consumer fraud costs the public $40 billion every year.

Which is likely to receive more attention: a single theft of $100 million, or one million thefts of $100?

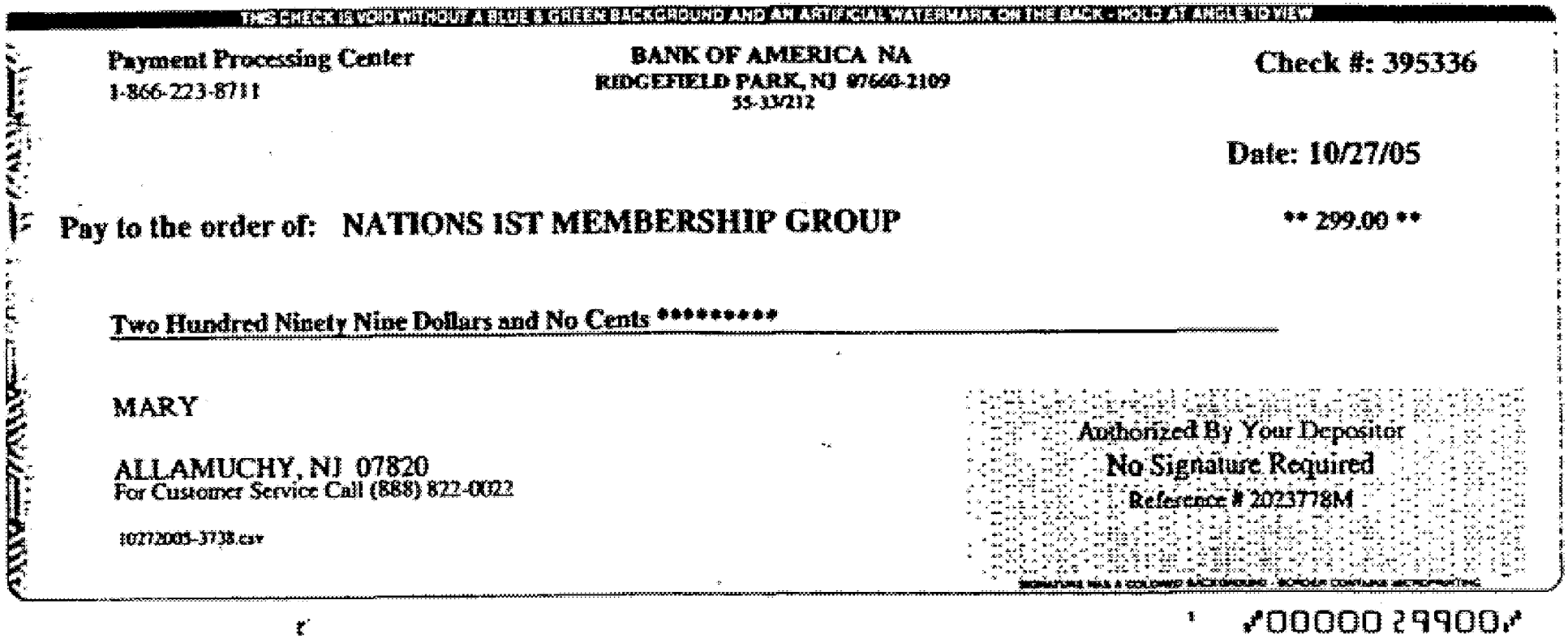
Common Methods of Payment System Abuse

- Remotely Created Checks processed by telemarketers and payment processors without consumer authorization
- Phone bills used to deduct unauthorized charges (often initiated by text message)
- Mortgage payment mechanisms used to deduct unauthorized charges

Law Enforcement Challenges to Prosecuting Telemarketing/Internet Fraud

- Jurisdictional limitations (state and international)
- Fraudsters easily relocate and change corporate identities leading to "whack-a-mole" results
- Victims are dispersed geographically
- Victims cannot identify fraudsters – no face-to-face contact
- Plausible deniability (call centers, mail houses, payment processors, "fulfillment centers")
- Limited investigative and prosecutorial resources
- State Attorneys General and FTC have limited reach

A Remotely Created Check ("RCC")



THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK - HOLD AT ANGLE TO VIEW

Payment Processing Center
1-866-223-8711

BANK OF AMERICA NA
RIDGEFIELD PARK, NJ 07660-2109
55-33/212

Check #: 395336

Date: 10/27/05

Pay to the order of: NATIONS 1ST MEMBERSHIP GROUP

** 299.00 **

Two Hundred Ninety Nine Dollars and No Cents *********

MARY

ALLAMUCHY, NJ 07820
For Customer Service Call (888) 822-0022

10272005-3738.csv

Authorized By Your Depositor
No Signature Required
Reference # 2023778M

⑈00000 29900⑈

RCC Fraud: Well-Known to Banks

"Demand drafts can be misused to commit check fraud. This practice involves the misuse of account information to obtain funds from a person's bank account without that person's signature on a negotiable instrument. . . **demand drafts have been used by deceptive telemarketers who obtain bank account information and withdraw unauthorized funds from consumers' bank accounts,** without their realizing that such withdrawals are occurring. . . ."

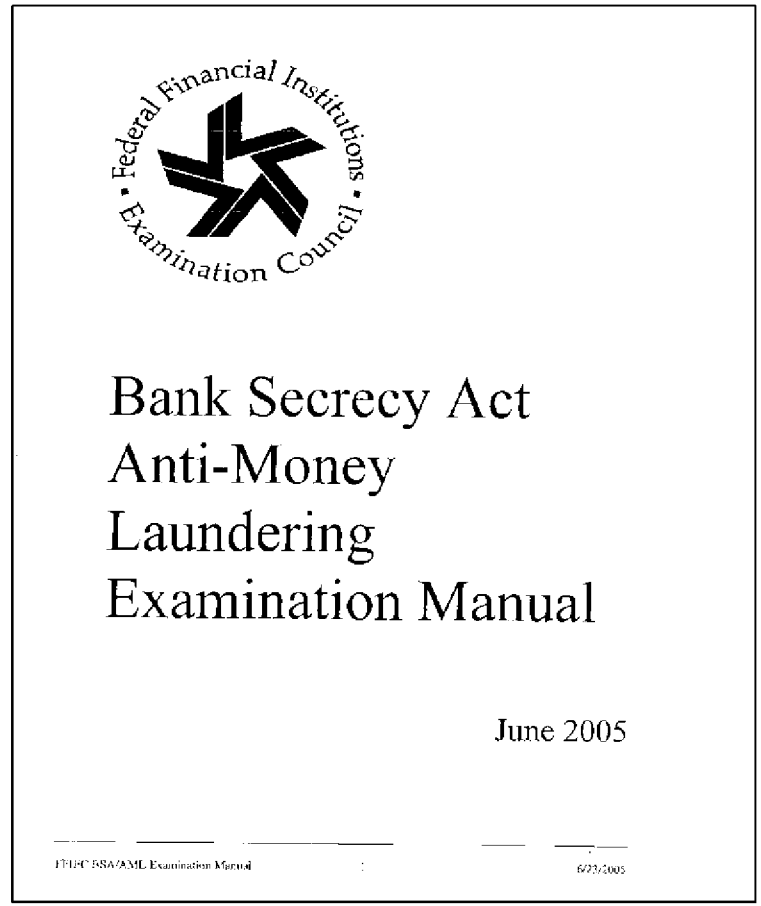
A Guide to Checks and Check Fraud, published by **Wachovia,** 2003

RCC Fraud: Well-Known to State Law Enforcement and FRB

- In 2005, 35 state attorneys general jointly request that the Federal Reserve ban RCCs from the payments system:
  - "demand drafts are frequently used to perpetrate fraud on consumers"
  - "such drafts should be eliminated" in favor of other forms of payment
  - If not eliminated, mandatory marking of RCCs and other measures to protect consumers

RCC Fraud: Well-Known to Bank Regulators

BSA/AML Examination Manual (FRB, FDIC, NCUA, OCC, and OTS)



Expanded Overview – Third-Party Payment Processors

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with its relationships with third-party payment processors, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Non-bank, or third-party, payment processors (processors) are bank customers that provide payment-processing services to merchants and other business entities.

Traditionally, processors contracted primarily with retailers that had physical locations in order to process the retailers' transactions. These merchant transactions primarily included credit card payments but also covered automated clearing house demand drafts[118] (also known as e-checks), and debit and stored value cards transactions. With the expansion of the Internet, retail borders have been eliminated. Processors may now service a variety of merchant accounts, including conventional retail and Internet-based establishments, prepaid travel, and Internet gaming enterprises.

RISK FACTORS

Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, and fraud schemes.

The bank's BSA/AML risks when dealing with a processor account are similar to risks from other activities in which the bank's customer conducts transactions through the bank on behalf of the customer's clients. When the bank is unable to identify and understand the nature and source of the transactions processed through an account, the risks to the bank and the likelihood of suspicious activity can increase. If a bank has not implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or sanctioned transactions.

[118] A demand draft is a substitute for a preprinted paper check. The draft is produced without a consumer signature but presumably with the consumer's authorization.

RISK MITIGATION

Banks offering account services to processors should develop and maintain adequate policies, procedures, and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. Verification and assessment of a processor can be completed by performing the following procedures:

- Reviewing the processor's promotional materials, including its web site, to determine the target clientele. (Businesses with elevated risk may include: offshore companies, online gambling-related operations, and online payday lenders). For example, a processor whose customers are primarily offshore would be inherently riskier than a processor whose customers are primarily restaurants.
- Determining whether the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization (ISO) opportunities" or "gateway" arrangements.[119]
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.
- Identifying the processor's major customers.
- Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.

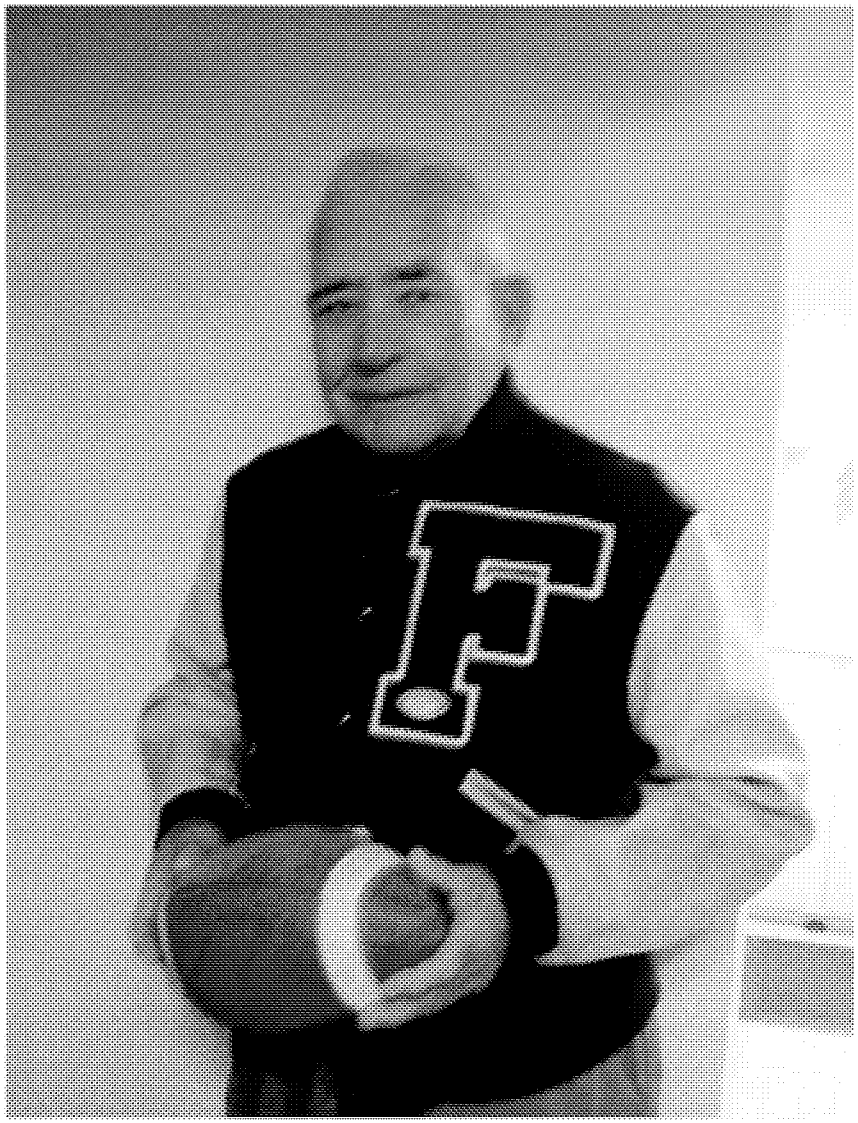
Banks that provide account services should monitor their processor relationships for any significant changes in the processors' business strategies that may affect their risk profile. Banks should periodically re-verify and update the businesses' profiles to ensure the risk assessment is appropriate.

In addition to adequate and effective account opening and due diligence procedures for processor accounts, management should monitor these relationships for unusual and suspicious activities. To effectively monitor these accounts, the bank should have an understanding of the following processor information:

- Merchant base.
- Merchant activities.
- Average number of dollar volume and number of transactions.
- "Swiping" versus "keying" volume for credit card transactions.
- Charge-back history.

[119] Gateway arrangements are similar to an Internet service provider with excess computer storage capacity who sells its capacity to a third party, who would then distribute computer service to various other individuals unknown to the provider. The third party would be making decisions about who would be receiving the service, although the provider would be providing the ultimate storage capacity. Thus, the provider bears all of the risks while receiving a smaller profit.

Purported Authorization Obtained By Telemarketer



David XXX, Sr.

1933-2006

University Football Coach

Little League Coach

Sunday School Teacher

Husband, Father, Grandfather, Brother

Incentives to Induce Authorization

Commerce Bank, NA
3-180/360

PharmAssist
45 E City Line Avenue PMB 463
Bala Cynwyd, PA 19004

No. 501586

Date: September 15, 2005

Pay to the Order of: [redacted]

$ 15.00
VOID AFTER 60 DAYS

Fifteen Dollars and 00 cents ** **Dollars**

[redacted]

MEMO:

Cashing or Depositing this check activates your membership in Family Health Solutions.

⑈501586⑈ ⑆036001808⑆ 36 652225 8⑈ ⑈0000001500⑈

Save 10% to 60% on Your Medications!

Save money on Dental Work, Doctor Visits, Extended Care, Chiropractic, Podiatry, Vision & Hearing Care... The list goes on and on!

Save at Pharmacies such as:

ACME
COSTCO
CVS/pharmacy
ECKERD
Kroger
Kmart
The Medicine Shoppe
Pathmark
Publix
RITE AID
SAFEWAY
TARGET

Plus 48,000 Others Including Independent Pharmacies Nationwide

Dear Roy [redacted]:

Are the high costs of Prescription drugs getting to you? Are you tired of all the politicians talking about Prescription Drug savings but doing nothing? Are you tired of having to dig down deep into your wallet to pay for your families' prescription medicines?

Roy, we would like to let you in on a little secret that will allow you to save up to 60 percent on all your prescription drug needs. **That's right, up to 60 percent!**

Pharm Assist has the answer and would like you to cash the above check and activate the membership that has been reserved in your name. You've read the newspaper articles and seen the news stories on local and national television. Now it's time for you to start taking advantage of the low, low prices Pharm Assist has negotiated with National Pharmacy chains, your local pharmacy, and mail order pharmacies as well.

You'll receive the medications that your Doctor prescribes at your local Pharmacy and Pharm Assist's mail order division will provide you with even BIGGER discounts. Isn't it time you started saving money and stopped listening to the empty promises of politicians? Just present your FHS card at your Pharmacy when you drop off your prescriptions. It's that easy!... Not convinced?

As an extra incentive, **we'll provide you with a $500.00 Emergency Cash Certificate*** that you never need to pay back! See the back of this form for details.

IMPORTANT: BY CASHING OR DEPOSITING THIS CHECK I AGREE THAT I UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED A ONE TIME SET UP FEE OF $79.95 WHICH WILL INCLUDE THE FIRST MONTHS SERVICE. I ALSO UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED $19.95 PER MONTH COMMENCING APPROXIMATELY 30 DAYS AFTER FULFILLMENT AND EVERY 30 DAYS THEREAFTER ON AN ONGOING BASIS FOR MY MONTHLY MEMBERSHIP FEES. I UNDERSTAND THAT I MAY CANCEL THE FAMILY HEALTH SOLUTIONS MEMBERSHIP AT ANY TIME AND BE ENTITLED TO A REFUND OF THE CURRENT MONTH'S MEMBERSHIP FEE BY CALLING CUSTOMER SERVICE AT 1-800-755-0070. BY DEPOSITING OR CASHING THIS CHECK I AUTHORIZE THESE FEES TO BE DEBITED FROM MY CHECKING ACCOUNT AS OUTLINED ABOVE.

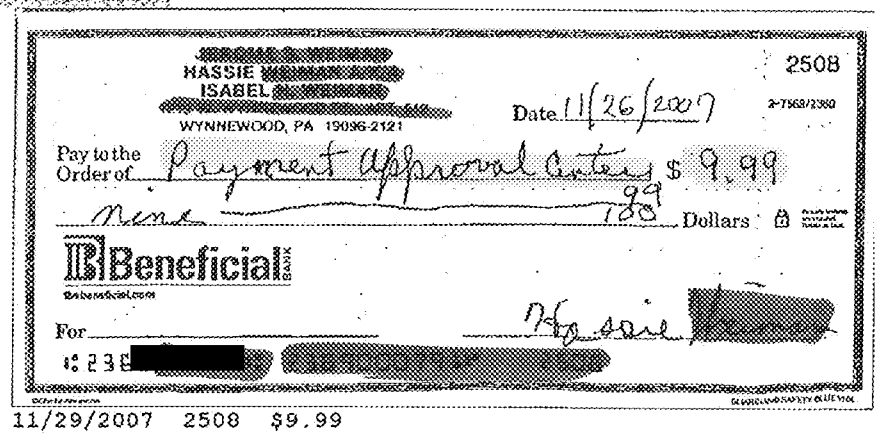
Sincerely yours,

Carol Soble
Director Membership Services

P.S. A limited number of participants have been chosen to receive this offer and you're one of the lucky ones. Cash or deposit your check... NOW!

Incentives for Purported Authorization

Beneficial SAVINGS BANK


HASSIE [redacted]
ISABEL [redacted]
WYNNEWOOD, PA 19096-2121

2508

Date 11/26/2007

Pay to the Order of Payment Approval Entry $ 9.99

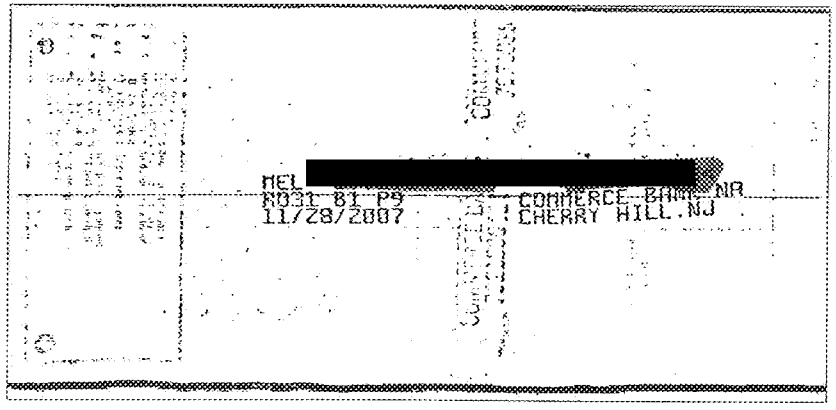
nine 99/100 Dollars

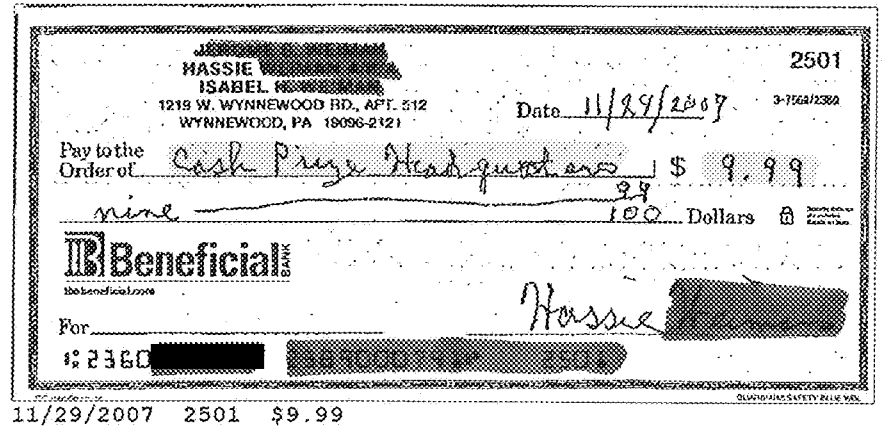
Beneficial

For [redacted]

Hassie [redacted]

11/29/2007 2508 $9.99


MEL [redacted]
RO31 81 P9
11/28/2007
COMMERCE BANK NA
CHERRY HILL,NJ


HASSIE [redacted]
ISABEL [redacted]
1219 W. WYNNEWOOD RD., APT. 512
WYNNEWOOD, PA 19096-2121

2501

Date 11/29/2007

Pay to the Order of Cash Prize Headquarters $ 9.99

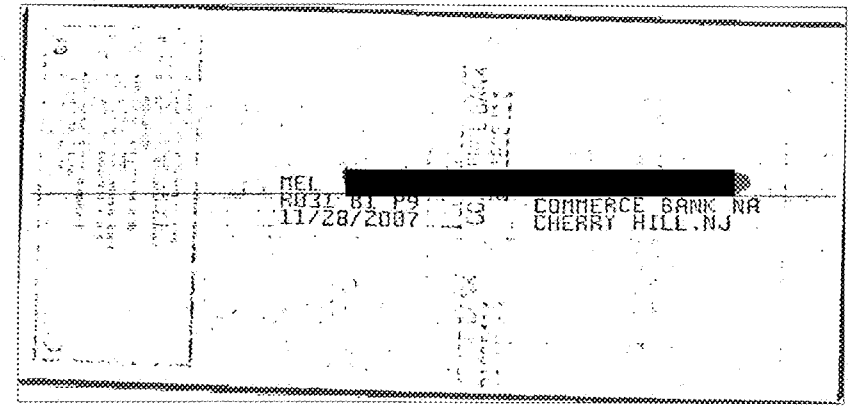
nine 99/100 Dollars

Beneficial

For [redacted]

Hassie [redacted]

11/29/2007 2501 $9.99


MEL [redacted]
RO31 81 P9
11/28/2007
COMMERCE BANK NA
CHERRY HILL,NJ

[redacted]

Prime Time Checking

Account Number: [redacted]
Statement Date: October 31, 2007
Page 1 of 3

- For Customer Service during business hours call 215.864.6730 or e-mail us at info@BeneficialSavingsBank.com
- For 24-hour account information call DirectLink at 215.864.1793 or 1.800.784.8490
- For other information visit us at www.BeneficialSavings.com

[redacted]
HASSE[redacted]
ISABEL[redacted]
[redacted]
WYNNEWOOD PA 19096

Account Summary

Previous Statement Balance As Of 09/30/07	1,444.48
Total Withdrawals/Charges	2,625.50
Total Deposits/Credits	2,968.02
Ending Balance	1,798.99

Annual Percentage Yield Earned: 0.50%

Check Summary

Checks Enclosed: 7

Date	Chk No.	Amount	Date	Chk No.	Amount	Date	Chk No.	Amount
10/01	2459	40.00	10/18	2462	438.50	10/18	2466	337.00
10/19	2460	33.86	10/19	2464	159.46	10/26	2470	5.99
10/24	2468*	10.00						

* Denotes Gap in Check Number Sequence

Other Transactions

Date	Description	Deposit(+) Withdrawal(-)
10/02	Ac-Us Treasury 303 -Soc Sec	595.00+
10/02	Ac-Us Treasury 303 -Soc Sec	1,193.00+
10/02	Ac-Car -Convcheck Ck-00000000002444	33.99-
10/03	Ac-Pcd -Convcheck Ck-00000000002446	37.99-
10/03	Ac-Pcd -Convcheck Ck-00000000002447	37.99-
10/03	Ac-App -Convcheck Ck-00000000002448	34.99-
10/05	Ac-Fin -Convcheck Ck-00000000002445	[illegible]
10/05	Ac-Sdd -Convcheck Ck-00000000002450	21.99-
10/05	Ac-Dcd Main Office -Convcheck Ck-00000000002449	24.99-
10/05	Ac-Met Life Ins. Co-Aarpfood	212.00-
10/05	Ac-Aarp Health Care-Premium	135.52-
10/09	Ac-Chase -Check Pymt Ck-00002458	322.75-
10/10	Ac-Pcd -Convcheck Ck-00000000002451	35.99-
10/10	Ac-Cppd Main Office-Convcheck Ck-00000000002452	31.99-
10/12	Deposit	800.00+
[illegible]	Ac-Reporting Data C-Convcheck Ck-00000000002454	24.99-
[illegible]	Ac-For -Convcheck Ck-00000000002455	27.99-
[illegible]	Ac-Aim -Convcheck Ck-00000000002453	[illegible]
[illegible]	Ac-Fpn -Convcheck Ck-00000000002457	[illegible]
10/17	Ac-Son -Convcheck Ck-00000000002456	[illegible]
10/19	Ac-At&T Consumer -Checkpaymt Ck-00002461	77.66-
[illegible]	Ac-Ron -Convcheck Ck-00000000002467	33.99-
[illegible]	Ac-Adm -Convcheck Ck-00000000002469	[illegible]
[illegible]	Ac-Se -Convcheck Ck-00000000002465	[illegible]
[illegible]	Ac-Cppd Main Office-Convcheck Ck-00000000002463	[illegible]
[illegible]	Ac-Reporting Data C-Convcheck Ck-00000000002473	[illegible]

From Target Gift Card to Automated Electronic Mortgage Payment

WACHOVIA

P.O. Box 900001
Raleigh, NC 27675-9001

MORTGAGE STATEMENT

ACCOUNT INFORMATION:

Statement Date:	10/05/06
Loan Number:	
Interest Rate:	5.9900
NEXT PAYMENT DUE DATE:	11/01/06
Current Payment:	$949.28
Past Due Payment(s):	
Unpaid Late Charges:	
Other Charges:	
TOTAL AMOUNT DUE:	$949.28
Home Phone #:	(215)

Customer Service Fax: 1-866-260-3962
Customer Service Dept.: 1-866-642-9405

Philadelphia PA 19144-3725

Property Address:

PHILADELPHIA PA 19144

Activity Since Your Last Statement:

Date	Description	Principal	Interest	Escrow	Late Charge	Other	Total
08/01	Payment	$175.59	$764.69			$9.00	$949.28
09/01	Payment	$176.46	$763.82			$9.00	$949.28
10/02	Payment	$177.35	$762.93			$9.00	$949.28

Account Summary:

Loan Balance* As of 10/05/06	Interest Paid Year to Date	Escrow Balance As of 10/05/06	Taxes Paid Year to Date

Incentives to Induce Authorization

HOMEQ SERVICING

$20.00 Target® GiftCard

Expiration Date
01/26/2005

Exclusively For

PHILADELPHIA PA 19144 3725

Please sign and return this reply form with your mortgage payment to get your $20.00 Target GiftCard and to activate your Great Fun privileges [illegible] HomEq Servicing Corporation Loan [illegible] for as long as I wish [illegible] Great Fun toll-free, 800-290-8609, to cancel. [illegible] After the free trial period, I may cancel at any time, for any reason [illegible] HomEq loan [illegible] By signing below I authorize HomEq to provide Great Fun [illegible] number, name, address, and any other information [illegible] benefits. Additionally I authorize [illegible]

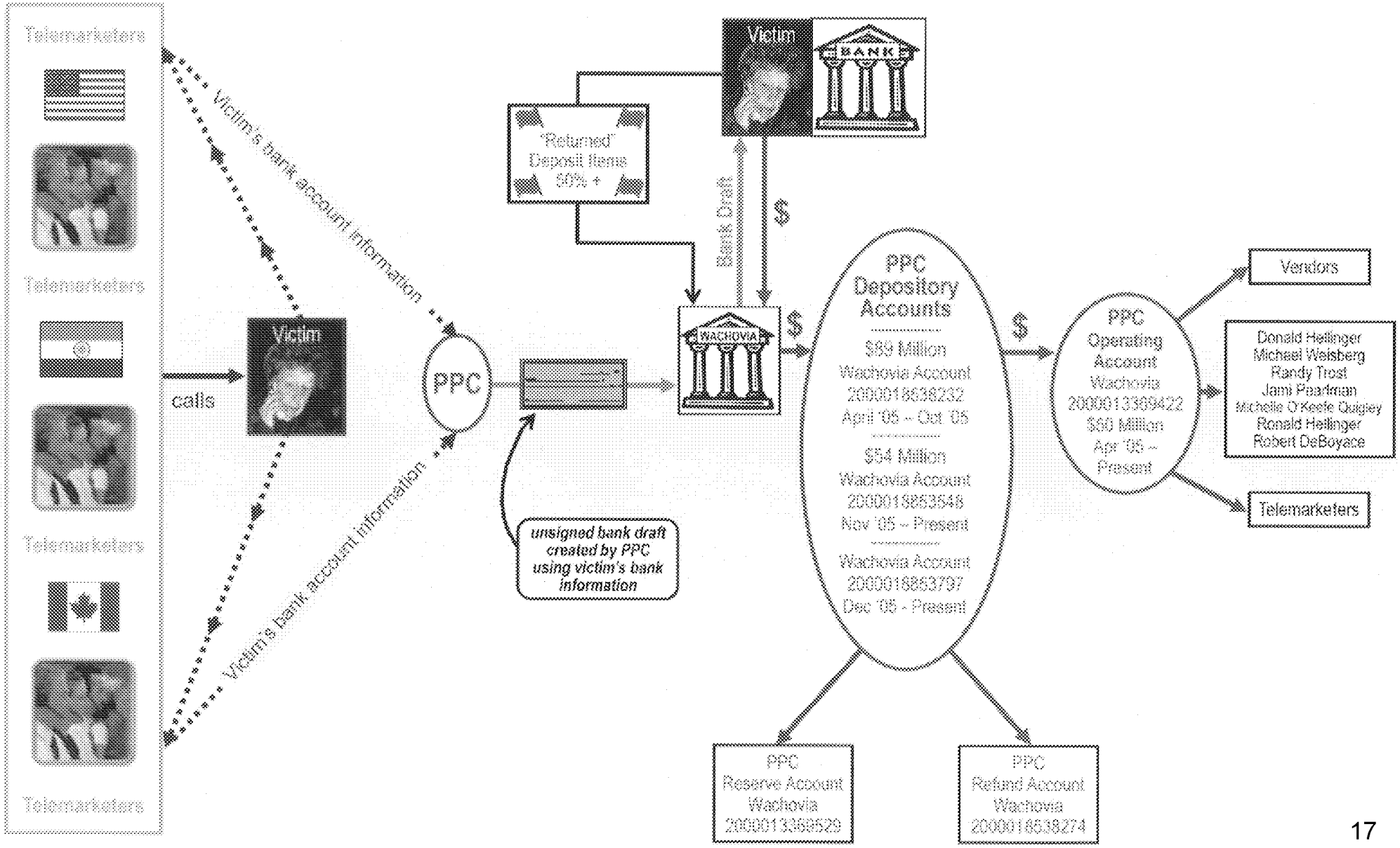
X ______________________
SIGNATURE REQUIRED FOR PROCESSING

Sign and return this form to claim the $20.00 Target GiftCard reserved for you
THIS FORM IS NOT REDEEMABLE AT ANY TARGET LOCATION

Z07615 Z7434[illegible]021[illegible] HCB 0303297089

HOGR-3PPP000133

The Payment Process



Payment Processing Center, LLC

- Provides "end-to-end solutions" for telemarketing merchants
- Specializes in "Bank Draft origination for telephone **transactions that may be prohibited**" by NACHA rules

Failure in Due Diligence
Know Your Customer's Customers

- PPC's Management Team
  - tax fraud conviction; subject of FTC consent decree arising out of coupon scam
  - "Madame Arielle DuPont"

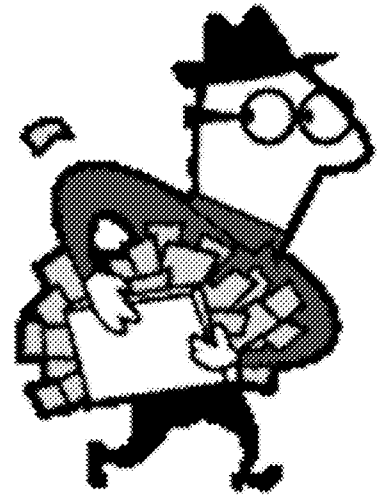
A Profitable Enterprise!

Dollar amount of PPC drafts deposited with Bank in 12 month period: **$162,000,000**

Income from RCC fees:

PPC -- **approx. $8,000,000**

Bank – **approx. $1,900,000**



PPC's Bank: Victim or Participant?

- Knew or had reason to know that PPC and other third-party payment processors serviced fraudsters
- Ignored red flags
- Suppressed internal concerns and dissent
- Entered agreements to protect banks interests over those of own customers, other banks, other banks' customers

Failure in Due Diligence
PPC's Telemarketing Merchants

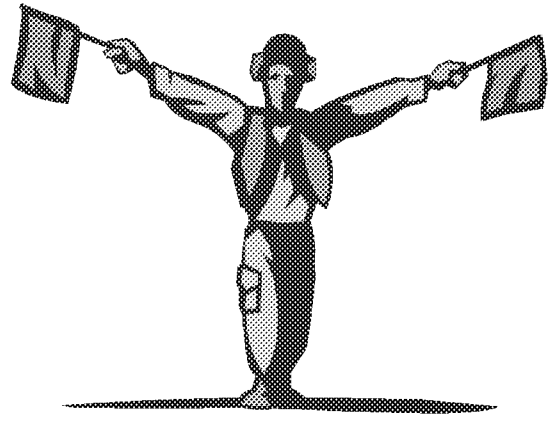
- Facially suspicious product offers and marketing scripts
  - Grant offers
  - Prescription discount cards
  - Travel Programs
  - Free Gift Cards
  - Free Computers
- Merchants mostly based overseas and/or using foreign banks
- Exploited names of legitimate companies, such as Wal-Mart, K-Mart, Home Depot, Carnival Cruises, AIG

Eyes Wide Shut

- PPC merchants were fraudsters well-known to Better Business Bureaus, state Attorneys General, and consumer protection websites
  - Star Communications
  - Advantage America
  - Suntasia
- Bank continued to process RCCs for same fraudsters as successive payment processers shut down by law enforcement

Returns – Charge Backs

- At inception, Bank **anticipated returns exceeding 35 percent** (compared to approximately 1/2 of 1 percent for all checks)
- Actual returned items exceeded **50 percent**
- Bank charged PPC substantial fee for returns
- Bank offered PPC volume discount on fees for returns



Return Reasons

- More than 50 percent of PPC's "with entry" returns identified on their face as:
  - UNAUTHORIZED
  - FRAUD
  - REFER TO MAKER
- In addition, Bank received thousands of "without entry" returns from other banks – **each including a sworn affidavit from a consumer alleging that the transaction was not authorized**

Banknorth, N.A.

AFFIDAVIT OF UNAUTHORIZED CONSUMER DRAFT

(Type or Print Neatly)

Bank: Banknorth Massachusetts
Banking Center: SW Commons/39
RC: 3390
Telephone #: (508) 754 - 6745

Use this form for drafts with the following tran codes only:
184 POD Check
187 Check

[redacted] Customer's Name
[redacted] Account Number
[redacted] Street
Apt. #
P.O. Box
Worcester City MA State 01604 Zip
[redacted] Daytime Telephone
Home Telephone

I declare, swearing under oath, that a draft charged to my account and appearing on my account statement is UNAUTHORIZED.

Call One Communications Name of Company
$149.90 Debit Amount
05/09/05 Date of Debit*

* If you are reporting this debit to the Bank more than sixty (60) days after the date of the statement on which it appears, the Bank will not re-credit your account and you should not complete this form.

Check appropriate Section I OR Section II:

I. Draft Never Authorized:

☒ I have never authorized the company named above to debit my account

II. Draft Authorization Has Been Revoked:

☐ I authorized the company named above to debit my account, but I revoked ** the authorization on _____ Date of Revocation in the manner specified in said authorization.

** Customer must provide Bank with a copy of the written revocation

I further declare that the above transaction was not initiated by me or by any person acting on my behalf. In signing this form, I understand that the Bank will reverse any credit(s) to my account if it receives proof from the payee of the draft that I, in fact, authorized this draft.

[redacted] Customer Signature (required)
5-17-05 Date
Banking Center Representative

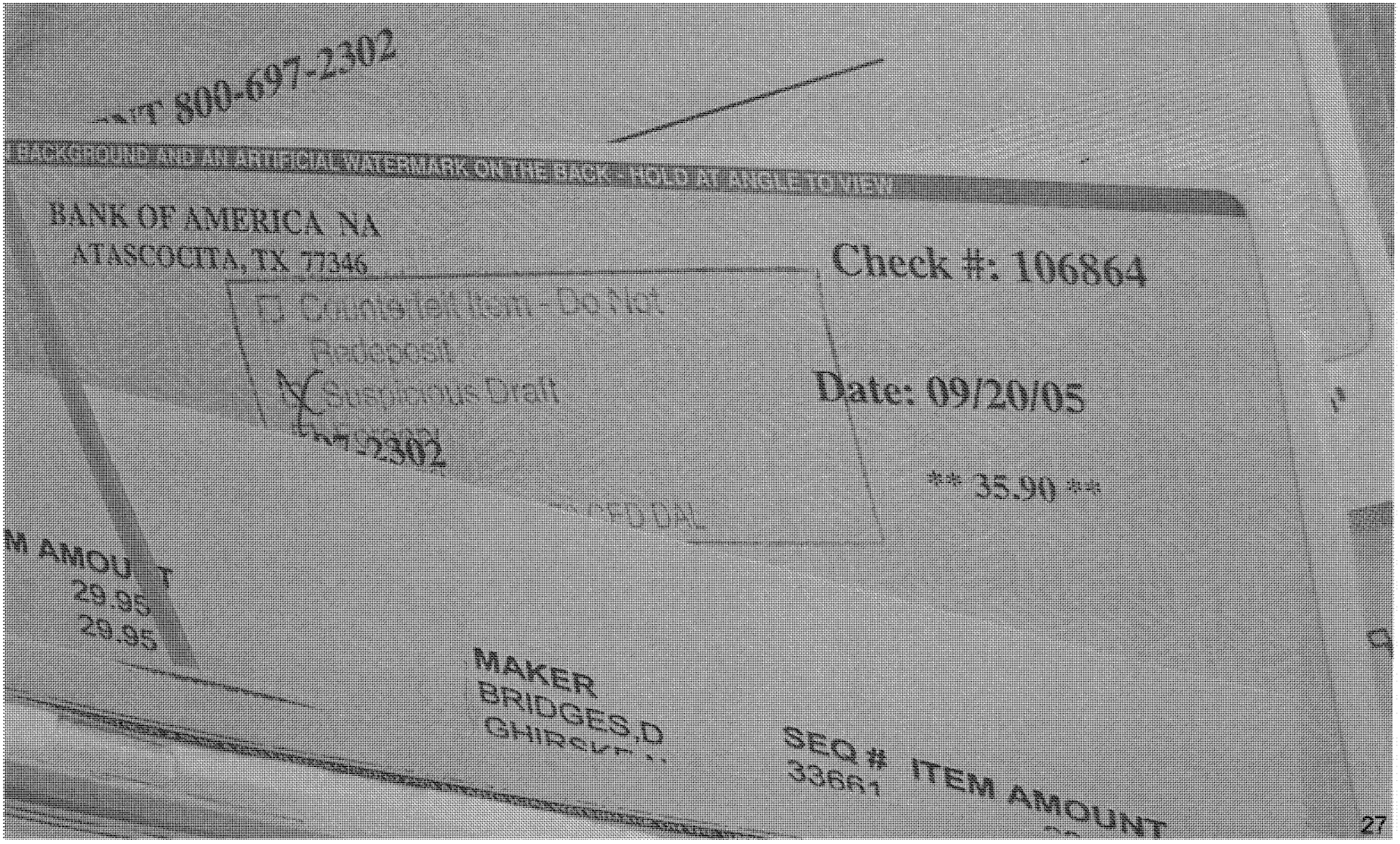
FOR USE ON PERSONAL ACCOUNTS ONLY

nstructions:

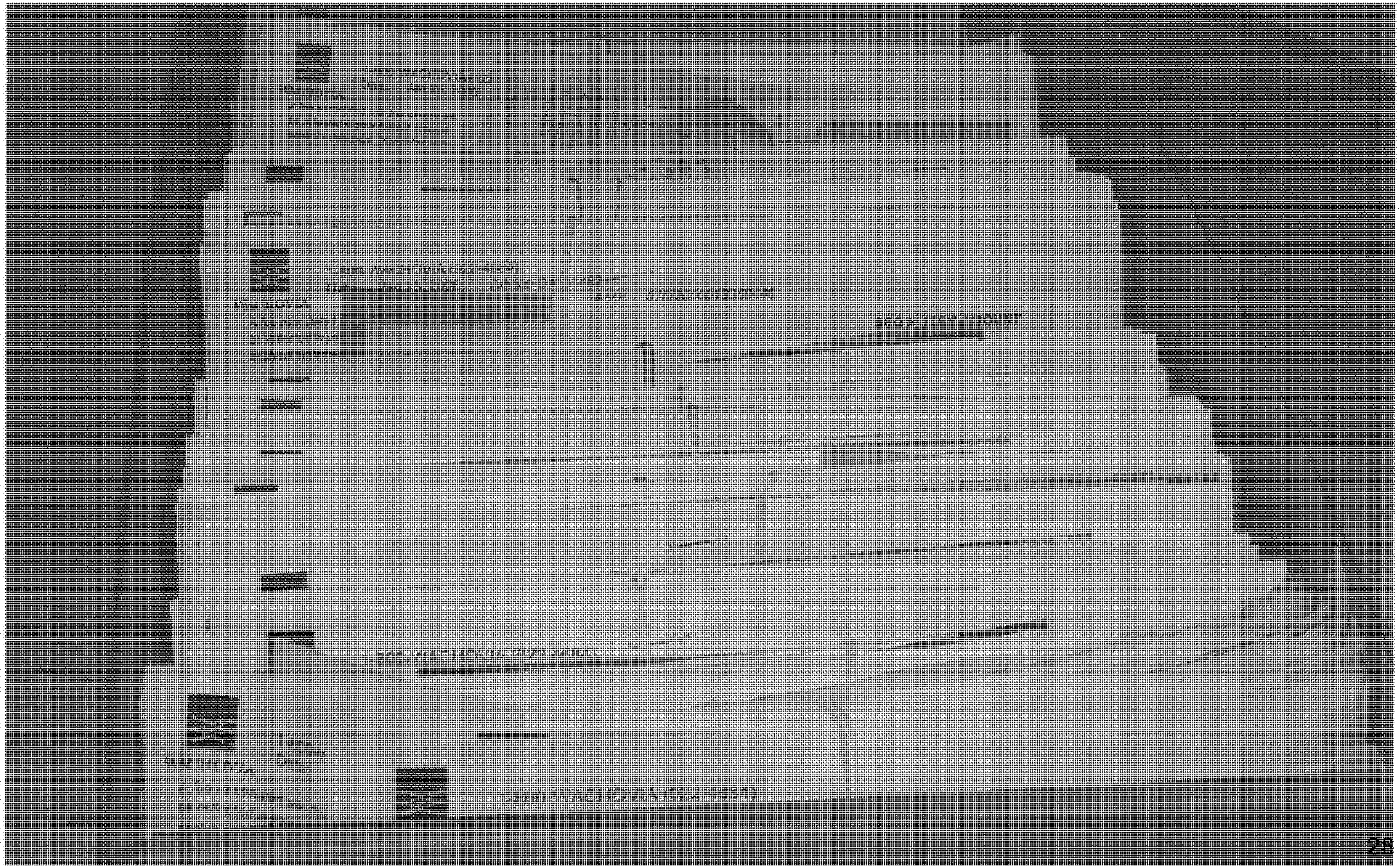
1. Fax to Adjustment Department 207-755-6315 OR Send a copy of the returned item (if available) and the signed affidavit through interoffice mail to: *Adjustment Department ME091-31*
2. Place a stop payment for the amount of the draft on the customer's account to prevent any future drafts from processing to the account. Have customer sign Stop Payment Order and remit form as usual.
3. Advise customer that provisional credit will NOT be granted on this transaction. Customer account will only be credited upon Bank receiving credit back from draft originator.

fidavit of Unauthorized Consumer Draft Rev. 03/2004

A Returned Item

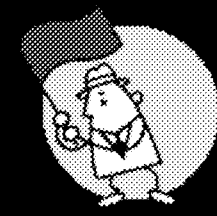


A Box of Returned Items



A Room of Boxes of Returned Items

Outlier Business Practices

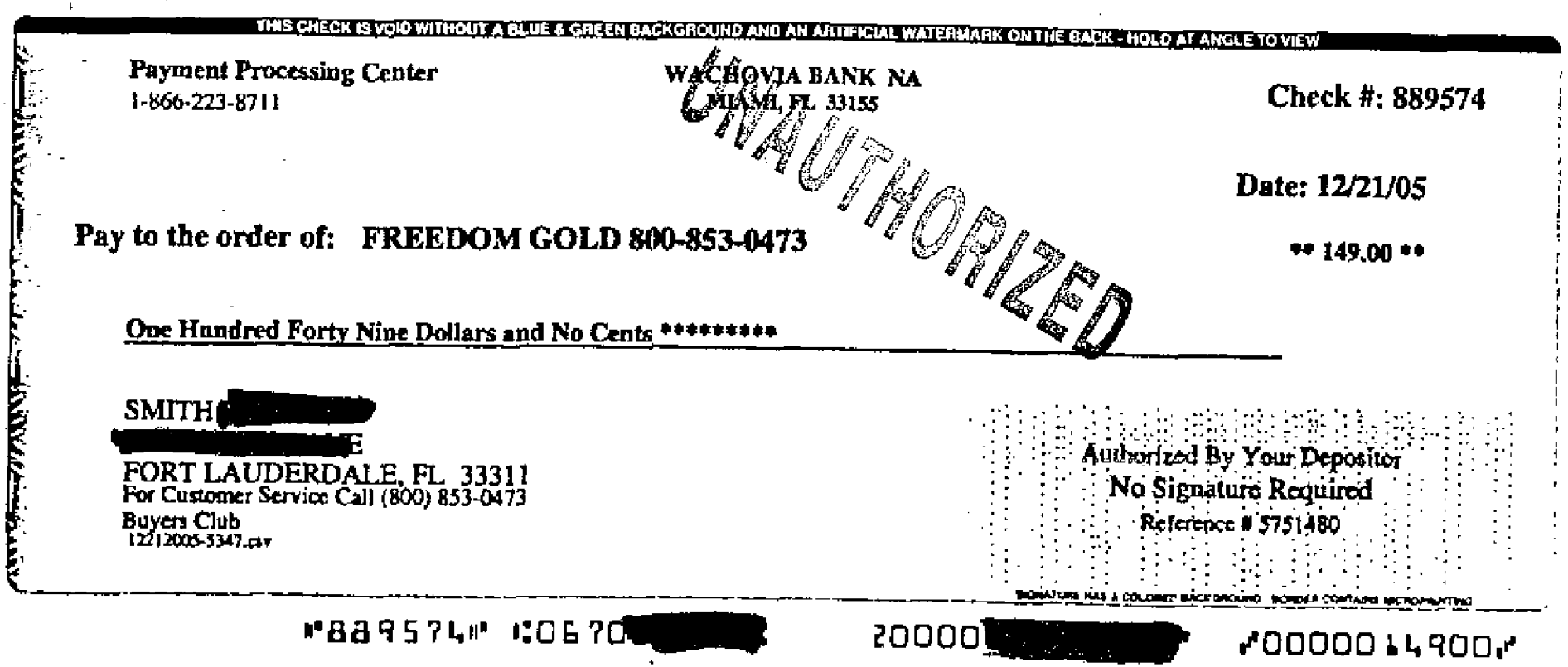


- PPC transferred overseas large amounts of money to numbered accounts and accounts in countries known to host fraudsters.
- Bank did not require agency agreements to permit PPC to deposit into its own accounts checks payable to PPC's merchant-clients (the telemarketers).
- Business model based on large volume activity for returns -- what is ordinarily suspect and undesired.
- Bank's own customers often treated differently than other banks' customers.

Justifications Offered for Continuing to Bank Suspected Fraudsters

- Customer has liberal return policy
- Consumer complaints reflect "buyers remorse"
- Rogue telemarketer has been fired
- Return reasons other than "unauthorized"

"On the House" Returns



THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK - HOLD AT ANGLE TO VIEW

Payment Processing Center
1-866-223-8711

WACHOVIA BANK NA
MIAMI, FL 33155

UNAUTHORIZED

Check #: 889574

Date: 12/21/05

Pay to the order of: FREEDOM GOLD 800-853-0473

** 149.00 **

One Hundred Forty Nine Dollars and No Cents *********

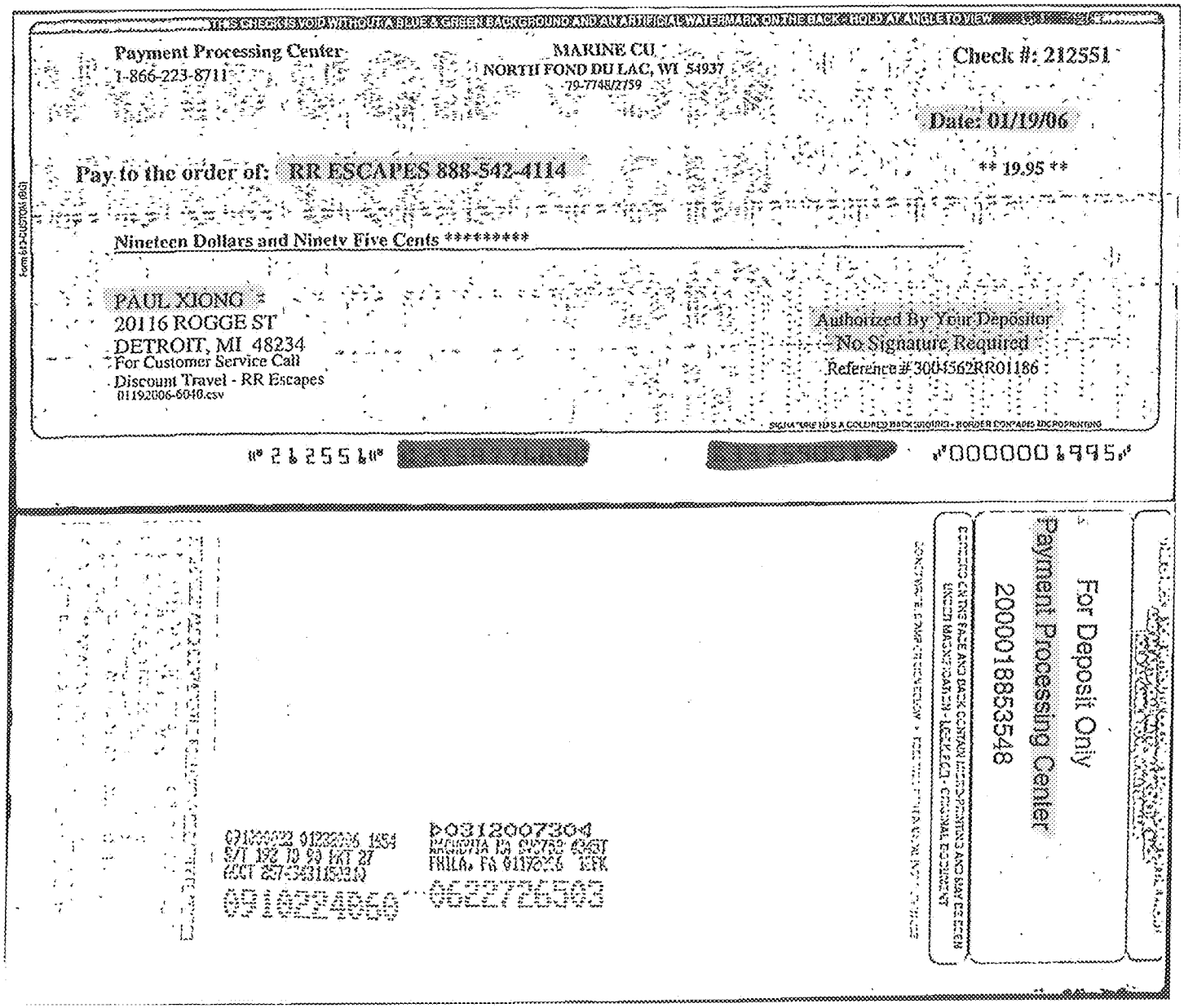
SMITH [redacted]
[redacted]E
FORT LAUDERDALE, FL 33311
For Customer Service Call (800) 853-0473
Buyers Club
12212005-5347.csv

Authorized By Your Depositor
No Signature Required
Reference # 5751480

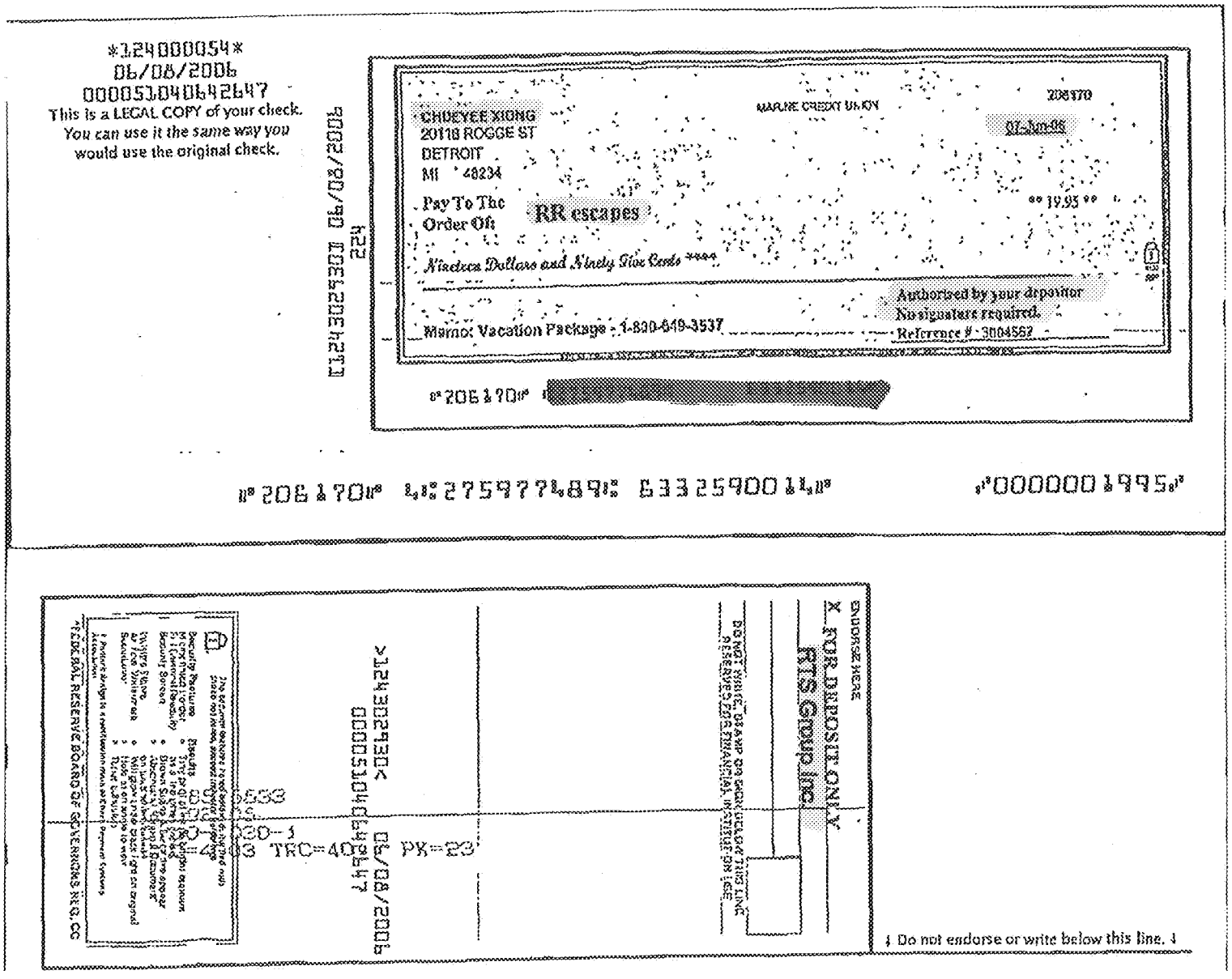
SIGNATURE HAS A COLORED BACKGROUND BORDER CONTAINS MICROPRINTING

⑈889574⑈ ⑆0670[redacted] 20000[redacted] ⑈000001 4900⑈

"Whack-a-Mole"


Payment Processing Center
1-866-223-8711
MARINE CU
NORTH FOND DU LAC, WI 54937
Check #: 212551
Date: 01/19/06
Pay to the order of: RR ESCAPES 888-542-4114
** 19.95 **
Nineteen Dollars and Ninety Five Cents **********
PAUL XIONG
20116 ROGGE ST
DETROIT, MI 48234
For Customer Service Call
Discount Travel - RR Escapes
01192006-6040.csv
Authorized By Your Depositor
No Signature Required
Reference#3004562RR01186
"212551"
"0000001995"
For Deposit Only
Payment Processing Center
200001885348

Migration from National Bank to Community Bank



Bank Ignored Explicit Warnings By Its Own Personnel

Return "volumes are tremendous" and "payment of these items is not our normal process"

Returns Operations Supervisor to VP of Loss Management

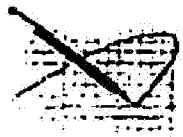
"Nothing [PPC] could ever do would make me comfortable . . ."

Bank Loss Management Official after learning about Bank relationship with PPC

After Loss Management official recommended closing PPC accounts, wrote "business line has assumed risk for the customer and decided to keep their accounts open"

Communication between Bank Loss Management Officials

DOUBLE YIKES!!!!



08/23/2005 06:35 PM

To

cc

Subject Guardian Marketing # 2000027007068

Tom,
Bob, Tim & I need to huddle with you on this account relationship. It is a Business Banking account. it has been actively making deposits since 6/23/05 and there is a current balance of $743,000+ in the account. The account came to us from B of A (so we are advised by : :n Bus. Bnkg.) and she is monitoring the account. The rub is there has already been 3,430 chargebacks this month and 4,579 since the account "got rolling". 4,579 chargebacks in 2 months. YIKES!!!! Now, the crux of the problem (in case you haven't already guessed) is that ALL their deposits are THIRD PARTY DRAFTS!!! DOUBLE YIKES!!!! Moreover, the drafts that are being deposited and are charging back, are not $99.99; these items are all over the place in terms of their amount. Moreover, there is another account, Suntasia, #2000027027721. Same address, same principals. $ from the Guardian acct is transferred to Suntasia and then the $ is wired out to Bank of America (funny, I thought I said they were leaving B of A at the beginning of this note, didn't I??). And, there is more, but nothing more that I want to put into a note. Bob and I really need to talk o you on tomorrow, 8/24/05. My number is below and Bob's number is

Thanks,

Loss Management
954-788-'

Bank Ignored Explicit Fraud Warnings From Other Banks

"The purpose of this message is to **put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam . . .** instigate an investigation into whether [PPC is] conducting legitimate business and whether [Bank is] getting **a high volume of return items on those accounts (that should place your bank on notice of potential fraud).**"

E-Mail from Citizens Bank

Bank's In-House Counsel's Warning

"Please consider the regulatory and reputational risks involved here. **We have now been put on notice that accounts at [Bank] are being used . . . to further these schemes.**

"If PPC has in place 'a standing agreement with [Bank] to pay all claims without dispute,' then they know they have rogue telemarketers in their customer base."

Internal E-mail from Bank's In-house Counsel after receiving fraud warning from another bank

Bank's "Oral Agreement" With PPC To Pay All Returns

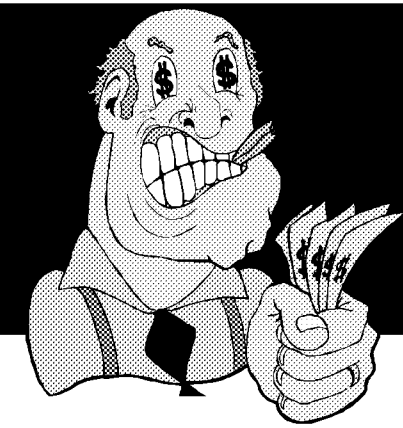
- Intended to protect Bank's reputation rather than consumers

"[I]f we can find a way to pay the returns . . . without sending them back to other banks, I think that will go a long way to preserve our reputation. **The sooner the complaint gets paid the quicker it goes away."**

Internal Bank e-mail

- Demonstrates that UCC warranty rule is not an effective anti-fraud tool

Money Motivates



"[P]lease mark your calendar – we will take them somewhere nice for lunch. We are making a ton of money from them."

Bank Relationship Manager to Senior Business Development Officer

"[T]his is our most profitable account. $1mm per year in profit. They have asked for Eagle tickets. What can we do?? They deserve them with all we make from them."

Bank Relationship Manager to Senior Business Development Officer

Reasons Banks Should Act Vigorously to Prevent Participation in Consumer Fraud

- Criminal prosecution risk (banks and bank employees)
- Regulatory enforcement risk
- Class action litigation risk
- Banks are uniquely situated to identify and prevent consumer fraud
- ***It's the right thing to do – even by banker standards!***

What's a reputation worth?

CNNMoney.com News | Markets | Technology | Personal Finance | Small Business | CNN.com

FORTUNE

Yikes: Wachovia and the telemarketers

April 25, 2008

Wachovia Million

to Pay as Much as $144
arketing Case

Business Day

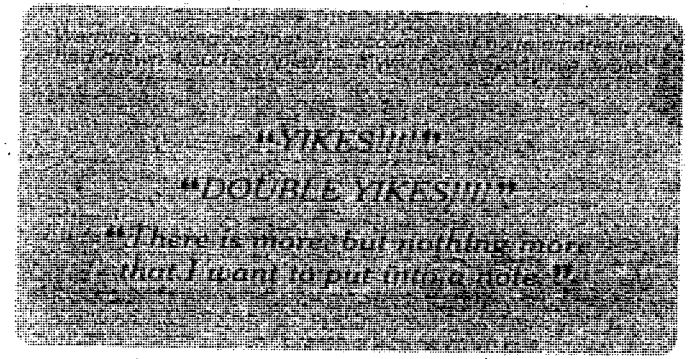
The New York Times

Papers Show Wachovia Knew of Thefts

By CHARLES DUHIGG

Last spring, **Wachovia** bank was accused in a lawsuit of allowing fraudulent telemarketers to use the bank's accounts to steal millions of dollars from unsuspecting victims. When asked about the suit, bank executives said they had been unaware of the thefts.

But newly released documents from that lawsuit now show that Wachovia had long known about allegations of fraud and that the bank, in fact, solicited business from companies it knew had been accused of telemarketing crimes.



e banking giant, has agreed to pay as
investigation accusing the bank of
ccounts to steal millions of dollars

HOGR-3PPP000159

Yes – it *is* a crime.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 10-20165 CR - LENARD
31 U.S.C. § 5318(h)
31 U.S.C. § 5322(a)

MAGISTRATE JUDGE
BRANNON

UNITED STATES OF AMERICA

v.

WACHOVIA BANK, N.A.,

Defendant.

FILED by D.C.
MAR 12 2010
STEVEN M. LARIMORE
CLERK U. S. DIST. CT.
S. D. of FLA. – MIAMI

INFORMATION

The United States Attorney charges that:

GENERAL ALLEGATIONS

At all times material to this Information

1. Defendant **WACHOVIA BANK, N.A.** was a national banking association based in Charlotte, North Carolina.

It's not over until it's over.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	CRIMINAL NO. 11-
	:	DATE FILED: February 10, 2011
v.		
	:	VIOLATIONS:
DONALD HELLINGER		18 U.S.C. § 371 (conspiracy – 1 count)
RONALD HELLINGER	:	18 U.S.C. § 1960 (operating an illegal money
MICHAEL WEISBERG		transmission business – 1 count)
RANDY TROST	:	18 U.S.C. § 1955 (operating an illegal gambling
JAMI PEARLMAN		business – 1 count)
MICHELE QUIGLEY	:	18 U.S.C. § 1084 (transmission of wagers and
		wagering information – 8 counts)
	:	18 U.S.C. § 1956(a)(2)(A) (international money
		laundering – 3 counts)
	:	Notice of forfeiture

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES THAT:

At all times relevant to this indictment:

BACKGROUND

1. Defendants DONALD HELLINGER, RONALD HELLINGER, MICHAEL WEISBERG, RANDY TROST, JAMI PEARLMAN, and MICHELE QUIGLEY

Financial accountability -- thanks to federal agents, prosecutors, and bank regulators, class action attorneys, local and state law enforcement, *The New York Times*, and many determined victims of consumer fraud !

Thanks for your time and interest!

Questions?

Joel M. Sweet, AUSA

[redacted]

From: Olin, Jonathan F. (CIV)
Sent: Monday, June 10, 2013 6:41 PM
To: Blume, Michael S.; Bresnick, Michael J (ODAG)
Cc: Frimpong, Maame Ewusi-Mensah (CIV)
Subject: FW: FYI on NYT story to include CIV

Nice work.

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Monday, June 10, 2013 6:37 PM
To: Martinez, Brian (OAAG); Taylor, Elizabeth G. (OAAG); Chilakamarri, Varudhini (OASG); Thompson, Karl (OAG); Jacobsohn, Robin (ODAG); Starks, Geoffrey (ODAG)
Cc: Olin, Jonathan F. (CIV); Blume, Michael S.; Bresnick, Michael J (ODAG)
Subject: RE: FYI on NYT story to include CIV

Hi –

The story is online now, and is supposed to run in tomorrow's paper: http://www.nytimes.com/2013/06/11/business/fraud-against-seniors-often-is-routed-through-banks.html?src=busln&_r=0 Great quotes by Mike Blume and Mike Bresnick. Kudos to them and OPA for making this happen.

Regards,
Maame

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Friday, June 07, 2013 2:19 PM
To: Martinez, Brian (OAAG); Taylor, Elizabeth G. (OAAG); Chilakamarri, Varudhini (OASG); Thompson, Karl (OAG); Jacobsohn, Robin (ODAG); Starks, Geoffrey (ODAG)
Cc: Olin, Jonathan F. (CIV)
Subject: FYI on NYT story to include CIV

Hi –

You may have already heard about this from OPA, but just in case, we wanted to let you know that there will likely be a story in the NYT this weekend about third-party payment processors that we anticipate will favorably discuss the work that CIV is doing in this area. Mike Bresnick and Mike Blume did an interview with the NYT on this issue generally and our work. Apparently, it went very well, and we are hoping that the story will highlight the proactive approach we have taken on this issue. Let us know if you have any questions or need more information on the initiative. I include a bit of background and context below.

What are Third-Party Payment Processors?
Since very few of the fraudulent schemes we are looking at involve cash transactions, fraudulent merchants need access to victims' bank accounts in order to get money from them. And they are only able to take money from their victims' bank accounts if they have a relationship with a bank, and thus access to the nation's banking system. Banks are reluctant to establish direct relationships with such merchants due to significant legal, financial, and reputational risks. To overcome this obstacle, fraudulent merchants create indirect relationships with banks through third-party payment processors. In many cases, these processors are unlicensed, unregulated, and owned or controlled by the fraudulent

merchants. By using processors as conduits to gain access to the banking system, fraudulent merchants can evade and frustrate statutes and regulations designed to require banks to know their clients, and to prevent their clients from using the banking system to further criminal activity.

What is the Consumer Protection Branch Doing?
The Consumer Protection Branch has increasingly been trying to identify the "choke points" in fraudulent schemes so as to make our enforcement efforts more effective since the number of fraudulent schemes and perpetrators of those schemes is so large. Third-party payment processors represent one such choke point. Our initiative focuses on banks and third-party payment processors and seeks to get both to comply with their "know your customer" obligations; the authorities we are using are civil and criminal (FIRREA, Bank Secrecy Act, wire fraud). In addition to our attorneys who are working on this, we also have an AUSA on detail, an individual from Treasury on detail, and two USPIS agents working on this.

Note that FINCEN circulated an advisory on this issue last year, and we participated in an interagency webinar with over 1000 financial institutions to help them understand what the law requires. Third-party payment processors is also the focus of one of the three subgroups of the FFETF Consumer Protection Working Group, where we are working with a number of other agencies.

Thanks!

Regards,
Maame

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

FILE

U.S. Department of Justice

Civil Division

Washington, D.C. 20530 July 8, 2013

TO: Stuart F. Delery
Acting Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

MB 7/8/13

SUBJECT: Operation Choke Point: Four-Month Status Report

This memo addresses our efforts during the past four months to combat mass-market consumer fraud by focusing on payment systems vulnerabilities. Our goal is to block fraudsters' access to consumers' funds by targeting the banks and payment processors that facilitate scams. The scams we expect to affect – and believe we already have affected – include telemarketing and internet scams, and internet payday lending. Many of these scams are directed at the elderly and economically vulnerable consumers.

I. Bank and Payment Processor Investigations

In February 2013, we served subpoenas on [redacted] banks requesting documents sufficient to identify third-party payment processors and merchants with high transaction return rates. In May 2013, we served subpoenas on [redacted] additional banks requesting similar information. The banks served with subpoenas were identified as having originated transactions on behalf of suspected consumer frauds, having outlier return rates indicative of potential fraud, or having been the target of suspicious third-party payment processors seeking to establish bank relationships. The subpoenas were narrow in scope and designed to elicit information to decide whether further investigation was warranted.

The subpoena returns we have received indicate that we are on the right path. Even before our first enforcement action, our activity has helped stem the tide of consumer fraud. As we expected, the mere receipt of a subpoena has caused many financial institutions to reconsider the wisdom and risks of processing payments for suspect processors and merchants. We have substantial anecdotal evidence that our efforts are causing banks to scrutinize potential third-party processor relationships more closely. For example, counsel for a [redacted] bank informed us that, following receipt of our subpoena, the bank terminated a merchant that processed approximately 20,000 debit transactions against consumer accounts each month with

U.S. Department of Justice

Civil Division

Washington, D.C. 20530 July 8, 2013

TO: Stuart F. Delery
Acting Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: Operation Choke Point: Four-Month Status Report

This memo addresses our efforts during the past four months to combat mass-market consumer fraud by focusing on payment systems vulnerabilities. Our goal is to block fraudsters' access to consumers' funds by targeting the banks and payment processors that facilitate scams. The scams we expect to affect – and believe we already have affected – include telemarketing and internet scams, and internet payday lending. Many of these scams are directed at the elderly and economically vulnerable consumers.

I. Bank and Payment Processor Investigations

In February 2013, we served subpoenas on [redacted] banks requesting documents sufficient to identify third-party payment processors and merchants with high transaction return rates. In May 2013, we served subpoenas on [redacted] additional banks requesting similar information. The banks served with subpoenas were identified as having originated transactions on behalf of suspected consumer frauds, having outlier return rates indicative of potential fraud, or having been the target of suspicious third-party payment processors seeking to establish bank relationships. The subpoenas were narrow in scope and designed to elicit information to decide whether further investigation was warranted.

The subpoena returns we have received indicate that we are on the right path. Even before our first enforcement action, our activity has helped stem the tide of consumer fraud. As we expected, the mere receipt of a subpoena has caused many financial institutions to reconsider the wisdom and risks of processing payments for suspect processors and merchants. We have substantial anecdotal evidence that our efforts are causing banks to scrutinize potential third-party processor relationships more closely. For example, counsel for a [redacted] bank informed us that, following receipt of our subpoena, the bank terminated a merchant that processed approximately 20,000 debit transactions against consumer accounts each month with

payment processors servicing mostly high-risk merchants, including a considerable number of Internet payday lenders, after receiving our subpoena. Two banks have self-disclosed that they had relationships with payment processors servicing suspected fraudsters. Other banks have notified us preliminarily that they have identified processor relationships that raise concerns. We learned that a large Internet payday lender decided recently to exit the business due to difficulties securing a bank or payment processor relationship. Counsel for third-party payment processors have intimated that banks are requiring more information about merchants before accepting their business. Counsel for banks have complimented our investigatory approach. And our regulatory partners are benefiting from our initiative as well; an FTC attorney recently informed us that banks now are taking more seriously the FTC's fraud investigations.

We have designed a process to review the banks' document productions and to distill information that will assist us in deciding whether further investigation or action is appropriate. For each bank, we prepare a summary of the bank's processor relationships, return rate history, merchant identification and consumer history (based on the FTC's Sentinel database), and other pertinent information. When completed, our DOJ team considers alternative courses of action for each bank, including criminal prosecution, FIRREA civil actions, and referral to an appropriate regulator. The FDIC has volunteered two attorneys from its Depositor and Consumer Protection Branch to assist with this review.

Based on this initial analysis, the Consumer Protection Branch has formed investigative teams to delve deeper into specific banks and payment processors that produced troubling return-rate information and other evidence of potential fraud. The following sections briefly describe some of the information we have collected on these entities.[1]

[1] We anticipate several additional investigations will be justified after analysis of documents received from various banks.

[redacted]

II. Merchant Investigations and Internet Payday Lending

Given the breadth and complexity of the bank and processor investigations and resource constraints, we must forgo in-depth investigations into many of the fraudulent merchants that are using the banks and processors to steal consumers' funds. Nevertheless, we have our eyes open for merchant targets that fall within such high priority areas as service member fraud and pay-day lending.

We have been engaged in an ongoing discussion with CFPB concerning the Internet payday lending industry. Internet payday lending is challenging from a law enforcement perspective. Lending generally is governed by state law. State authorities, however, are stymied in their efforts to combat unlawful lending, in part due to a lack of jurisdiction over Internet payday lenders. We have tentatively agreed with CFPB to determine whether there are payday lenders that would make good targets of federal investigation, and a structure for joint analysis of evidence. Despite past inconsistency with respect to CFPB's offers to work with us on this effort, CFPB's Director of Enforcement has approved our proposal for a joint approach. We are working out details and hope to begin in the coming weeks.

In the course of our investigations, we have learned of U.S. Military Lending Corp., an Internet payday lending company targeting military families. During a five-month period, U.S. Military Lending originated 87 debit transactions against consumer accounts with an average monthly return rate of 61 percent. Although the number of transactions is low, the high return rate justifies further scrutiny. We are preparing a request for authority to serve a FIRREA subpoena on U.S. Military Lenders to determine whether the company's activities violate any FIRREA predicate crimes.

We also have served subpoenas on banks and payment processors that are facilitating the Internet payday loan industry, in an attempt to learn more about their practices. We believe that Internet payday lending as it is practiced violates a variety of state lending laws, as well as arguably the Electronic Funds Transfer Act and its implementing regulations (Regulation E). Ultimately, if we can induce banks and payment processors to stop facilitating transactions by

Internet payday lenders that make unlawful loans, we will be attacking the problem at a much broader level.

III. Engagement with Other Agencies

A. Treasury Department

The Treasury Department's Office of Terrorist Finance and Financial Crimes ("OTFFC") has an interest in the roles of payment processors and banks in the facilitation of fraud. They have asked us to participate in two projects. First, OTFFC is drafting a National Money Laundering Threat Assessment, an effort to document major money laundering risks and threats. The threat assessment will serve as the basis for future policy and legislative proposals. OTFFC would like to include our input and data in the threat assessment. Second, OTFFC has asked that we provide information to the Money Laundering Task Force, a multi-agency effort to review and prioritize the government's efforts to combat money laundering.

We are apprehensive about diverting resources from our investigations toward these efforts. We recognize, however, that deeper cooperation with Treasury will increase the financial regulatory community's focus on consumer protection. Moreover, some at Treasury agree with us that recently created regulatory gaps that exclude third-party payment processors from the registration and oversight regime constitute a significant risk to consumers, and also seriously hamper DOJ's ability to effectively use criminal statutes, such as 18 U.S.C. § 1960 – Operating an Illegal Money Transmitting Business, to prosecute illicit payment processors. Our participation in Treasury's Threat Assessment and Task Force will support those efforts.

B. The Federal Reserve Bank – Atlanta

The Federal Reserve Bank – Atlanta ("FRB-A") is one of the nation's primary clearing houses for ACH transactions, and also is a major clearing house for checks. FRB-A also acts as a primary or secondary regulator for many of the nation's banks. In its role as an ACH clearinghouse, FRB-A monitors banks with high return volume. FRB-A communicates with banks experiencing abnormal ACH activity.

On May 28, 2013, we held a three-hour meeting with the FRB-A in Atlanta. The meeting, which included the FRB-A's General Counsel and other senior officials, focused on the operation of the payment systems, information available from that system, processes for obtaining information, abilities to surveil high return rates, and specific case-related matters. In addition to Joel Sweet and two USPIS Inspectors who travelled to Atlanta, participants included approximately 20 Trial Attorneys, AUSAs, FTC counsel, and investigators who participated by telephone. We have cemented a good working relationship with Richard M. Fraher, Vice President and Counsel to the Retail Payments Office, and his staff. FRB-A has requested that we participate in upcoming risk forums on critical issues such as the quality of authorizations that the payment system should rely upon.

FRB-A has reports, data, communications with and among banks, and other information that would assist our efforts to combat consumer fraud. FRB-A has expressed its desire that we obtained this information through subpoenas. We are discussing with the FRB-A whether it could share information based upon formal letter requests, as is the practice at the FDIC and the OCC. If that is not possible, we will draft subpoenas requesting the information on the possession of the FRB-A.

C. NACHA – Electronic Payment Association

NACHA is the association that governs the ACH payment system. On July 2, 2013, CPB and FTC hosted Jane Larimer, Executive Vice President and General Counsel of NACHA. Participants included (in person and by telephone conference) more than 100 law enforcement agents and investigators, government attorneys, and regulators from DOJ, FTC, CFPB, FDIC, OCC, USPIS, FBI, SIGTARP, Treasury, various USAOs, and other agencies. Larimer provided a tutorial on the ACH payment system, including its operating rules, the roles of the key players (merchants, processors, banks), monitoring of the ACH system, fraud trends and detection, special considerations for third-party payment processors, and information available to investigators and the process for obtaining such information.

D. FDIC – Office of Inspector General

We met with officials of FDIC's Office of Inspector General to discuss our initiative and investigative resources needs. FDIC-OIG supports of our work and has established a liaison to work with us. Agent support may be available on a case-by-case basis. We are actively considering which part of our initiative would benefit most from their resources.

E. SIGTARP

Following a recent presentation about Operation Choke Point at Payments Fraud Working Group meeting hosted by DOJ's Criminal Frauds Section, the Office of the Special Inspector General for the Troubled Asset Relief Program ("SIGTARP") requested an opportunity to meet with us to discuss its support of our investigations. Following an initial meeting, SIGTARP informed us that it has received all necessary approvals and that its leadership is fully supportive of SIGTARP agents supporting our cases. SIGTARP has more than 70 agents dedicated to illegal activity relating to banks that received TARP funding. We are actively considering which part of our initiative would benefit most from their resources. At least [redacted] of the banks we have subpoenaed also received TARP funds, and therefore are within SIGTARP's jurisdiction.

F. State Banking Regulators/LE

We have received calls of interest from the attorneys general of several states, including North Carolina, Texas, New York, and Illinois. State banking officials in [redacted] have offered assistance in our investigations against banks in their states. On July 1, 2013, we met with a senior official of the [redacted]

[redacted] to explore opportunities for collaboration. Based on our discussions, [redacted] instructed the head of the Consumer Protection office of the Attorney General to develop strategies and resources to address banks that provide services to scammers, and an enforcement plan relating to Internet-based payday lending.

G. Internal DOJ Training

Travel funding and time permitting, we intend to offer U.S. Attorney Office's training in payment systems/mass market fraud prosecution under FIRREA. Such training will institutionalize the knowledge we have learned and expand the team of federal attorneys that can target banks and processors that facilitate fraud.

H. FTC's Proposed Change to the Telemarketing Sales Rule

The FTC has proposed an amendment to the Telemarketing Sales Rule that would prohibit use of Remotely Created Checks ("RCCs") for use in telemarketing transactions. We have seen numerous instances in which fraudsters have used RCCs to illegally debit consumers' bank accounts without their authorization. We intend to draft a comment to the FTC's proposed rule by the July 29, 2013, deadline for submitting comments.

IV. Related Area of Inquiry – Emerging Payment Systems

Third party payment processors make up a major channel through which fraudsters take money from consumers, but there are others. We are attempting to develop a better understanding of consumer fraud risk posed by emerging payment systems. We also are attempting to establish relationships with payment-related businesses so that we can benefit from their first-line experience with consumer fraud, and to strengthen potential cooperation in investigations. We have met with Green Dot, E-Bay, PayPal, and Netspend. A meeting is being scheduled to meet with AMEX, which recently has launched a pre-paid card with Wal-Mart.

V. Next steps

As described in this memo, we have formulated a successful plan for the initiative and have made significant progress in its implementation. The plan entails:

1) Continuing to identify banks and payment processors that engage in questionable conduct to determine whether a subpoena is warranted;

2) Reviewing subpoena returns to find the most egregious conduct by banks and payment processors and initiating investigations where appropriate;

3) Recruiting the investigatory and prosecutorial resources needed to pursue the specific cases;

4) Bringing civil and criminal enforcement actions to stem the tide of consumer loss and further deter the banking industry from providing fraudsters access to consumers' bank accounts;

5) Learning from those knowledgeable about the payment processing systems, implementing that knowledge in our investigations, and teaching regulators and law enforcement to enable them to join the fight; and

6) Formulating legislative and/or regulatory means for fixing the unregulated world of third-party payment processors.

In sum, we have made real, tangible progress in our initiative to date. More time is necessary to move all of these plans forward.

(Goldberg, Sweet, [redacted]

UNITED STATES DEPARTMENT OF JUSTICE - CIVIL DIVISION
CORRESPONDENCE TRACKING SYSTEM

ID: 67533 Executive Sec #:
Document Type: Litigation
File Code: Deputy for Consumer Protection Branch
Responding Unit:
Reviewer: Richard Goldberg
Drafter: Joel Sweet [redacted]
To: Stuart F. Delery, A/AAG, Civil Division
From: Michael S. Blume, Director, Consumer Protection Branch, thru: Maame Ewusi-Mensah Frimpong, DAAG, Civil Division

Cover Sheet Date: 07/09/2013
Document Date: 07/08/2013
Date Received: 07/09/2013
Response Due: 07/12/2013
EXPEDITE
Date Closed:
SG Due: at your earliest convenience

Subject: Payment Processor Investigation - Request for Issuance of Subpoena to Internet Website Registrar

Comments: Maame Ewusi-Mensah Frimpong: Review and comment
Stuart F. Delery: Sign subpoena [redacted]
Time Frame: "We request your approval by July 12, 2013. There are no external deadlines. However, we believe the information received in response to this subpoena may support an Anti-Fraud Injunction Act action to prevent a large ongoing fraud. Prompt service also is necessary to avoid the risk of information loss."

Actions: Assigned To	Initials	Date Assigned	Finished
Maame Ewusi-Mensah Frimpong		07/09/2013	9 July 2013
Stuart F. Delery	SFD	JUL - 9 2013	7/13/13
[redacted]		JUL 15 2013	JUL 15 2013
Michael S. Blume		JUL 15 2013	

Notes: Stuart – I recommend that you approve this subpoena to an internet website registrar which will permit us to confirm that one of our 3PPP targets owns certain fraudulent websites. As noted, CCIPS has confirmed that this complies w/ ECPA.

U.S. Department of Justice

Civil Division

Washington, D.C. 20530

July 8, 2013

TO: Stuart F. Delery
Principal Deputy Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong MEM
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: Payment Processor Investigation – Request for Issuance of Subpoena to Internet Website Registrar

Time Frame

We request your approval by July 12, 2013. There are no external deadlines. However, we believe the information received in response to this subpoena may support an Anti-Fraud Injunction Act action to prevent a large ongoing fraud. Prompt service also is necessary to avoid the risk of information loss.

Recommendation

We seek authorization to issue a subpoena under the Financial Institutions Reform, Recovery and Enforcement Act of 1989, 12 U.S.C. § 1833a(g)(1)(C) ("FIRREA"). The subpoena would be directed to the entity described below.

Case Summary

In February 2013, we served subpoenas upon several banks and third-party payment processors in furtherance of Operation Choke Point, a multi-agency task force combating mass-market consumer fraud through a focus on payment systems. One of the subpoenas issued was to [redacted]

[redacted]

The subpoena was reviewed and approved by CCIPS to assure compliance with the Electronic Communications Privacy Act.

Discussion

Fraudulent Internet businesses frequently hide their identities by employing a variety of short-lived websites and by incorporating through various shell entities. These techniques impose investigative obstacles for law enforcement through concealment of the identities of the individuals engaged in what appears to be fraudulent activity, and through the ephemeral nature of electronic evidence, which can be rapidly changed and destroyed. The requested subpoena is designed to overcome these obstacles by providing information about the individual who has created and used these Internet websites, and preserving the evidence in an appropriate form.

Typically, an Internet website is created through hiring a "domain name registrar," an entity that manages the reservation and registration of Internet domain names. Numerous domain name registrars operate throughout the world, but all do so under the auspices of the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit entity with headquarters in Los Angeles, California. Domain name registrars must be accredited by ICANN in order to register domain names. Typically, an individual or business wishing to create a website will hire a registrar, thus designating that registrar for the Internet domain name that the individual wishes to operate, normally on the World Wide Web.

Many domain name registrars also provide hosting services, meaning that they will store an end-user's website pages on Internet-connected computers owned by the registrar. Thus, instead of having to purchase and maintain suitable equipment to establish an Internet presence, a customer of a registrar providing these hosting services can merely "rent" space for their website.

[redacted]

[redacted]

Conclusion

We request that you sign the attached FIRREA subpoena intended to obtain information about the individuals and entities responsible for each of the above websites.

(Goldberg/Sweet/[redacted])

UNITED STATES DEPARTMENT OF JUSTICE - CIVIL DIVISION
CORRESPONDENCE TRACKING SYSTEM

ID: 67536 Executive Sec #: Cover Sheet Date: 07/10/2013
Document Type: Litigation Document Date: 07/08/2013
File Code: Deputy for Consumer Protection Branch Date Received: 07/09/2013
Responding Unit: Consumer Protection Branch Response Due: 07/12/2013
Reviewer: Richard Goldberg As soon as practical
Drafter: Joel Sweet [redacted] Date Closed:
To: Stuart F. Delery, A/AAG, Civil Division SG Due:
From: Michael S. Blume, Director, Consumer Protection Branch

Subject: Payment Processor Investigation - Request for Issuance of Subpoena to Banks Identified as Originating Debits on Behalf of Fraudulent Merchant
[redacted]

Comments: Maame Ewusi-Mensah Frimpong: Review and comment
Stuart F. Delery: Sign [redacted] subpoenas
Time Frame: "We request your approval by July 12, 2013. There are no external deadlines. However, we believe the information received in response to this subpoena may support an Anti-Fraud Injunction Act case to prevent a large ongoing fraud. Prompt service also is necessary to avoid the risk of information loss."

Actions: Assigned To	Initials	Date Assigned	Finished
Maame Ewusi-Mensah Frimpong		07/10/2013	10 July 2012
Stuart F. Delery	SFD	JUL 10 2013	7/13/13
[redacted]		JUL 15 2013	JUL 15 2013
Michael S. Blume		JUL 15 2013	

Notes: Stuart – I recommend you authorize these subpoenas of banks that have been identified as working with one of our targets. We are seeking information on their dealings with the target processor as well as with other processors to determine if they may have worked with other entities processing transactions for fraudulent merchants. [redacted]

U.S. Department of Justice

Civil Division

Washington, D.C. 20530

July 8, 2013

TO: Stuart F. Delery
Acting Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: Payment Processor Investigation – Request for Issuance of Subpoena to Banks Identified as Originating Debits on Behalf of Fraudulent Merchant

Time Frame

We request your approval by July 12, 2013. There are no external deadlines. However, we believe the information received in response to this subpoena may support an Anti-Fraud Injunction Act case to prevent a large ongoing fraud. Prompt service also is necessary to avoid the risk of information loss.

Recommendation

We seek authorization to issue subpoenas under the Financial Institutions Reform, Recovery and Enforcement Act of 1989, 12 U.S.C. § 1833a(g)(1)(C) ("FIRREA"). The subpoenas would be directed to the entities described below.

Case Summary

These subpoenas are requested in furtherance of Operation Choke Point, a multi-agency task force combating mass-market consumer fraud through a focus on payment systems.

[redacted]

We intend to request that the banks comply promptly with Part A of the subpoena, which calls for information that would further our potential injunction action, and offer an extension to the banks to comply with the Part B requests.

Conclusion

We request that you sign the attached FIRREA subpoenas.

(Goldberg/Sweet/[redacted]

Operation Choke Point:

a multi-agency effort to combat mass-marketing fraud by focusing on payment systems used to take consumers' money without authorization.

Joel M. Sweet, Trial Attorney, Consumer Protection Branch, DOJ
(detailee from United States Attorney's Office for the Eastern District of Pennsylvania)

Incentives to Induce Authorization

PharmAssist
45 E City Line Avenue PMB 463
Bala Cynwyd, PA 19004

Commerce Bank, NA
3-180/360

No. 501586

Date: September 15, 2005

Pay to the Order of: [redacted] *$ 15.00*

VOID AFTER 90 DAYS

Fifteen Dollars and 00 cents ** Dollars

[redacted]

MEMO

Cashing or Depositing this check activates your membership in Family Health Solutions.

⑈501586⑈ ⑆036001808⑆ 36 652225 8⑈ ⑈0000001500⑈

Save at Pharmacies such as:

ACME
COSTCO
CVS/pharmacy
ECKERD
Kroger
Kmart
The Medicine Shoppe
Pathmark
Publix
RITE AID
SAFEWAY
TARGET

Plus 48,000 Others Including Independent Pharmacies Nationwide

Save 10% to 60% on Your Medications!

Save money on Dental Work, Doctor Visits, Extended Care, Chiropractic, Podiatry, Vision & Hearing Care... The list goes on and on!

Dear Roy [redacted]:

Are the high costs of Prescription drugs getting to you? Are you tired of all the politicians talking about Prescription Drug savings but doing nothing? Are you tired of having to dig down deep into your wallet to pay for your families' prescription medicines?

Roy, we would like to let you in on a little secret that will allow you to save up to 60 percent on all your prescription drug needs. **That's right, up to 60 percent!**

Pharm Assist has the answer and would like you to cash the above check and activate the membership that has been reserved in your name. You've read the newspaper articles and seen the news stories on local and national television. Now it's time for you to start taking advantage of the low, low prices Pharm Assist has negotiated with National Pharmacy chains, your local pharmacy, and mail order pharmacies as well.

You'll receive the medications that your Doctor prescribes at your local Pharmacy and Pharm Assist's mail order division will provide you with even BIGGER discounts. Isn't it time you started saving money and stopped listening to the empty promises of politicians? Just present your FHS card at your Pharmacy when you drop off your prescriptions. It's that easy!... Not convinced?

As an extra incentive, we'll provide you with a $500.00 Emergency Cash Certificate* that you never need to pay back! See the back of this form for details.

IMPORTANT: BY CASHING OR DEPOSITING THIS CHECK I AGREE THAT I UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED A ONE TIME SET UP FEE OF $79.95 WHICH WILL INCLUDE THE FIRST MONTHS SERVICE. I ALSO UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED $19.95 PER MONTH COMMENCING APPROXIMATELY 30 DAYS AFTER FULFILLMENT AND EVERY 30 DAYS THEREAFTER ON AN ONGOING BASIS FOR MY MONTHLY MEMBERSHIP FEES. I UNDERSTAND THAT I MAY CANCEL THE FAMILY HEALTH SOLUTIONS MEMBERSHIP AT ANY TIME AND BE ENTITLED TO A REFUND OF THE CURRENT MONTH'S MEMBERSHIP FEE BY CALLING CUSTOMER SERVICE AT 1-800-755-0070. BY DEPOSITING OR CASHING THIS CHECK I AUTHORIZE THESE FEES TO BE DEBITED FROM MY CHECKING ACCOUNT AS OUTLINED ABOVE.

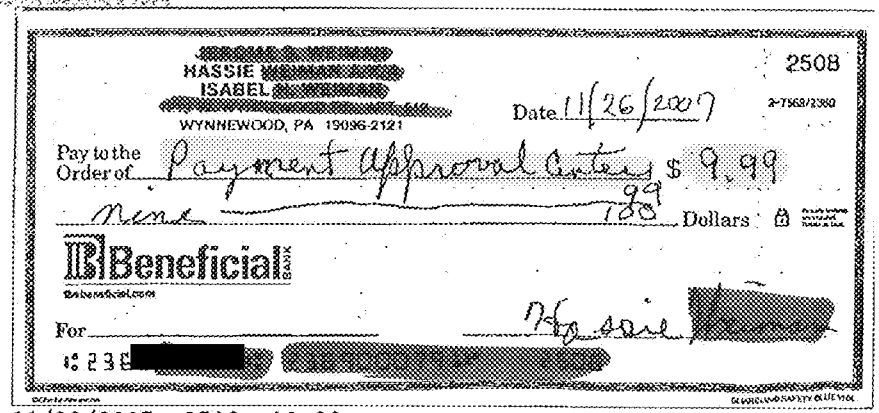
Sincerely yours,

Carol Soble
Carol Soble
Director Membership Services

P.S. A limited number of participants have been chosen to receive this offer and you're one of the lucky ones. Cash or deposit your check... NOW!

Incentives for Purported Authorization

Beneficial SAVINGS BANK


HASSIE [redacted]
ISABEL [redacted]
WYNNEWOOD, PA 19096-2121

2508

Date 11/26/2007

Pay to the Order of Payment Approval Center $ 9.99

Nine 99/100 Dollars

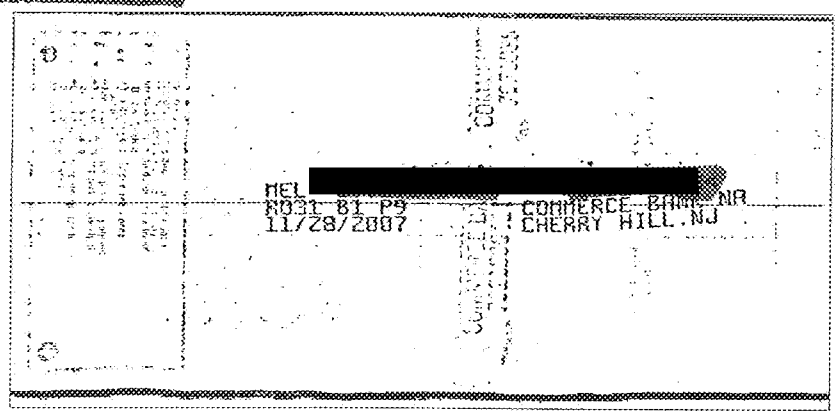
Beneficial

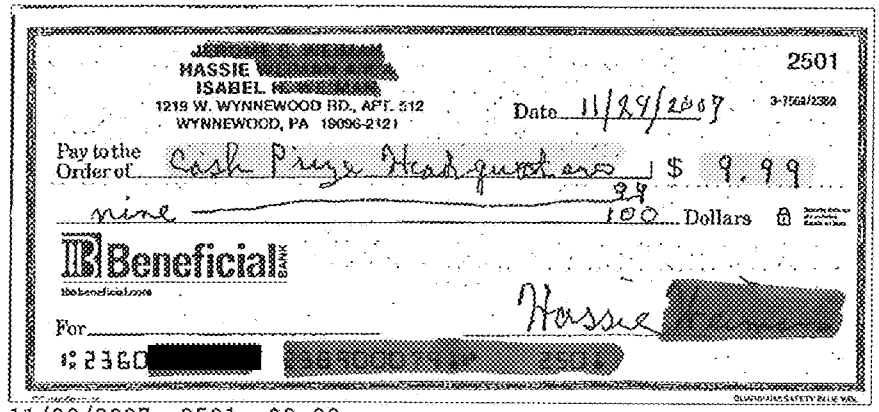
For

Hassie [redacted]

⑆ 23[redacted]

11/29/2007 2508 $9.99


MEL [redacted]
R031 B1 P9 COMMERCE BANK NA
11/28/2007 CHERRY HILL,NJ


HASSIE [redacted]
ISABEL [redacted]
1219 W. WYNNEWOOD RD., APT. 512
WYNNEWOOD, PA 19096-2121

2501

Date 11/29/2007

Pay to the Order of Cash Prize Headquarters $ 9.99

nine 99/100 Dollars

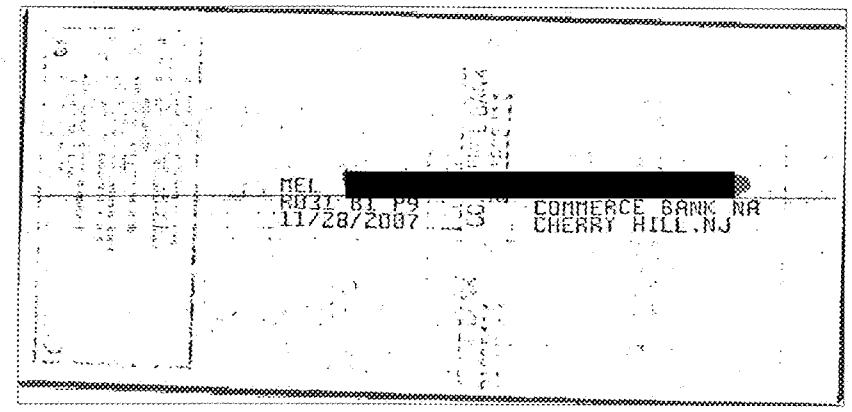
Beneficial

For

Hassie [redacted]

⑆ 2360[redacted]

11/29/2007 2501 $9.99


MEL [redacted]
R031 B1 P9 COMMERCE BANK NA
11/28/2007 CHERRY HILL,NJ

Prime Time Checking

Account Number: [redacted]
Statement Date: October 31, 2007
Page 1 of 3

- For Customer Service during business hours call **215.864.6730** or e-mail us at **info@BeneficialSavingsBank.com**
- For 24-hour account information call DirectLink at **215.864.1799** or **1.800.784.8490**
- For other information visit us at **www.BeneficialSavings.com**

[redacted]
WYNNEWOOD PA 19096

Account Summary

Previous Statement Balance As Of 09/30/07	1,864.08
Total Withdrawals/Charges	2,625.50
Total Deposits/Credits	2,560.02
Ending Balance	1,798.60

Annual Percentage Yield Earned: 0.50%

Check Summary

Checks Enclosed: 7

Date	Chk No.	Amount	Date	Chk No.	Amount	Date	Chk No.	Amount
10/01	2439	40.00	10/18	2462	438.50	10/18	2466	237.00
10/10	2463	13.86	10/19	2464	159.46	10/26	2470	9.95
10/24	2460*	10.00						

* Denotes Gap in Check Number Sequence

Other Transactions

Date	Description	Deposit(+) Withdrawal(-)
10/02	Ac-Us Treasury 303 -Soc Sec	565.00+
10/02	Ac-Us Treasury 303 -Soc Sec	1,194.00+
10/02	Ac-Car -Convcheck Ck-000000000002444	24.99-
10/02	Ac-Ppd -Convcheck Ck-000000000002446	27.99-
10/02	Ac-Pnd -Convcheck Ck-000000000002447	27.99-
10/02	Ac-App -Convcheck Ck-000000000002448	34.99-
10/03	Ac-Pm -Convcheck Ck-000000000002445	25.99-
10/05	Ac-Sdrd -Convcheck Ck-000000000002450	23.99-
10/05	Ac-Dcd Main Office -Convcheck Ck-000000000002449	24.99-
10/17	Ac-Ppa -Convcheck Ck-000000000002457	27.99-
10/17	Ac-Sbn -Convcheck Ck-000000000002458	39.99-
10/19	Ac-At&T Consumer -Checkpaymt Ck-00002461	77.46-
10/23	Ac-Rda -Convcheck Ck-000000000002467	31.99-
10/24	Ac-Adrd -Convcheck Ck-000000000002468	19.99-
10/24	Ac-Sr -Convcheck Ck-000000000002465	29.00-
10/25	Ac-Dpd Main Office -Convcheck Ck-000000000002469	31.99-
10/25	Ac-Reporting Data D-Convcheck Ck-000000000002471	24.99-

From Target Gift Card to Automated Electronic Mortgage Payment

WACHOVIA

P.O. Box 900001
Raleigh, NC 27675-9001

MORTGAGE STATEMENT

ACCOUNT INFORMATION:
Statement Date: 10/05/06
Loan Number:
Interest Rate: 5.9900
NEXT PAYMENT DUE DATE: 11/01/06
Current Payment: $949.28
Pa
Ur
Ot
TC 949.28
Hc
Cu
Cu

Philadelphia PA 19144-3725

Property Address:

PHILADELPHIA PA 19144

Other
$9.00
$9.00
$9.00

Activity Since Your Last Statement:

Date	Description	Principal	Interest	Escrow		tal
08/01	Payment	$175.59	$764.69			$949.28
09/01	Payment	$176.46	$763.82			$949.28
10/02	Payment	$177.35	$762.93			$949.28

Account Summary:

Loan Balance* As of 10/05/06	Interest Paid Year to Date	Escrow Balance As of 10/05/06	Taxes Paid Year to Date

Incentives to Induce Authorization

HOMEQ SERVICING **$20.00 Target® GiftCard**

Expiration Date
01/26/2005

Exclusively For

PHILADELPHIA PA 19144 3725

Please sign and return this reply form with your mortgage payment to get your $20.00 Target GiftCard and to activate your Good Neighbor Privileges!

Check this box, sign and return this reply form with your payment to get your $20.00 Target GiftCard and to activate your Good Neighbor Privileges!

I Did to my HomEq Servicing Corporation loan, for as long as I wish to [illegible] payment at all times. If I decide to [illegible] Good Fun to Give, 800-290-8600, to cancel. I [illegible] Over the "life of loan" period, I may cancel at any time, by [illegible] additional. By signing below I authorize HomEq to provide [illegible] number name, address, and any other [illegible] benefits. Additionally I authorize [illegible]

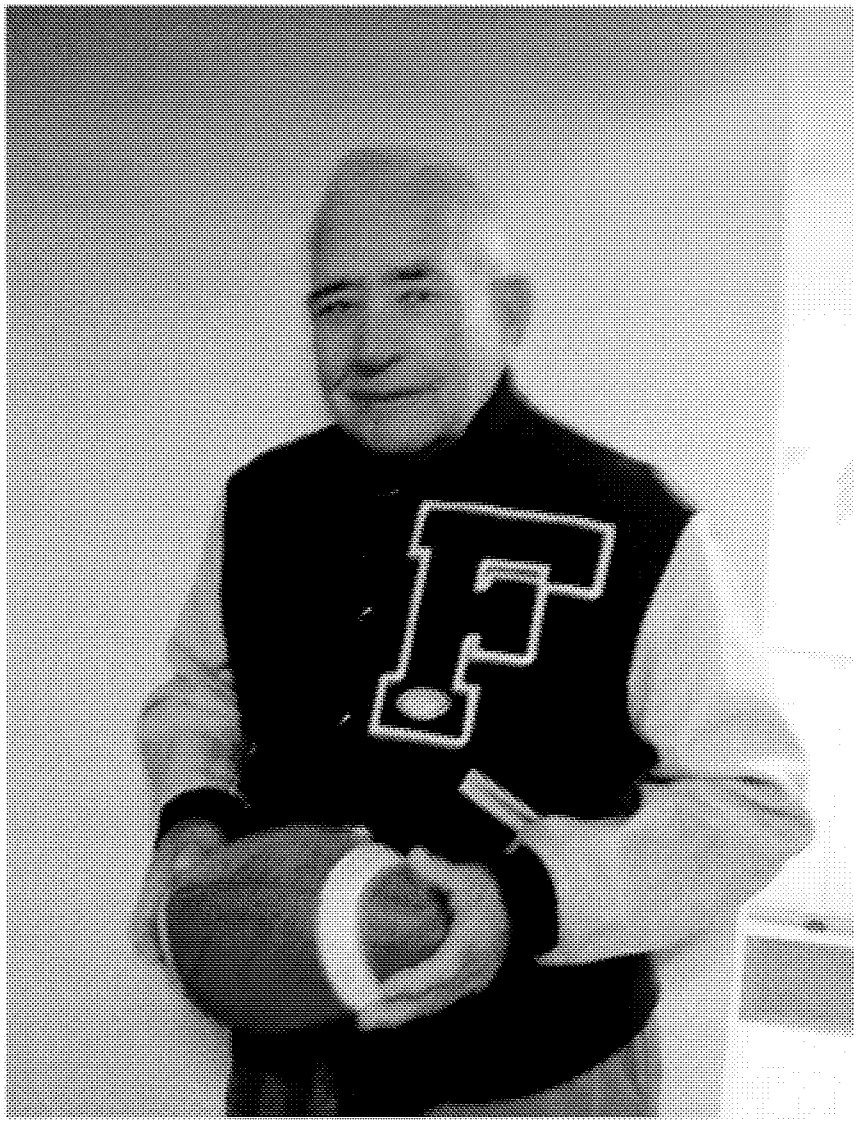
X _____

SIGNATURE REQUIRED FOR PROCESSING

Sign and return this form to claim the $20.00 Target GiftCard reserved for you
THIS FORM IS NOT REDEEMABLE AT ANY TARGET LOCATION

Z07635 Z7434[illegible]02[illegible]3 HCB 0303297089

Purported Authorization Obtained By Telemarketer



David XXX, Sr.

1933-2006

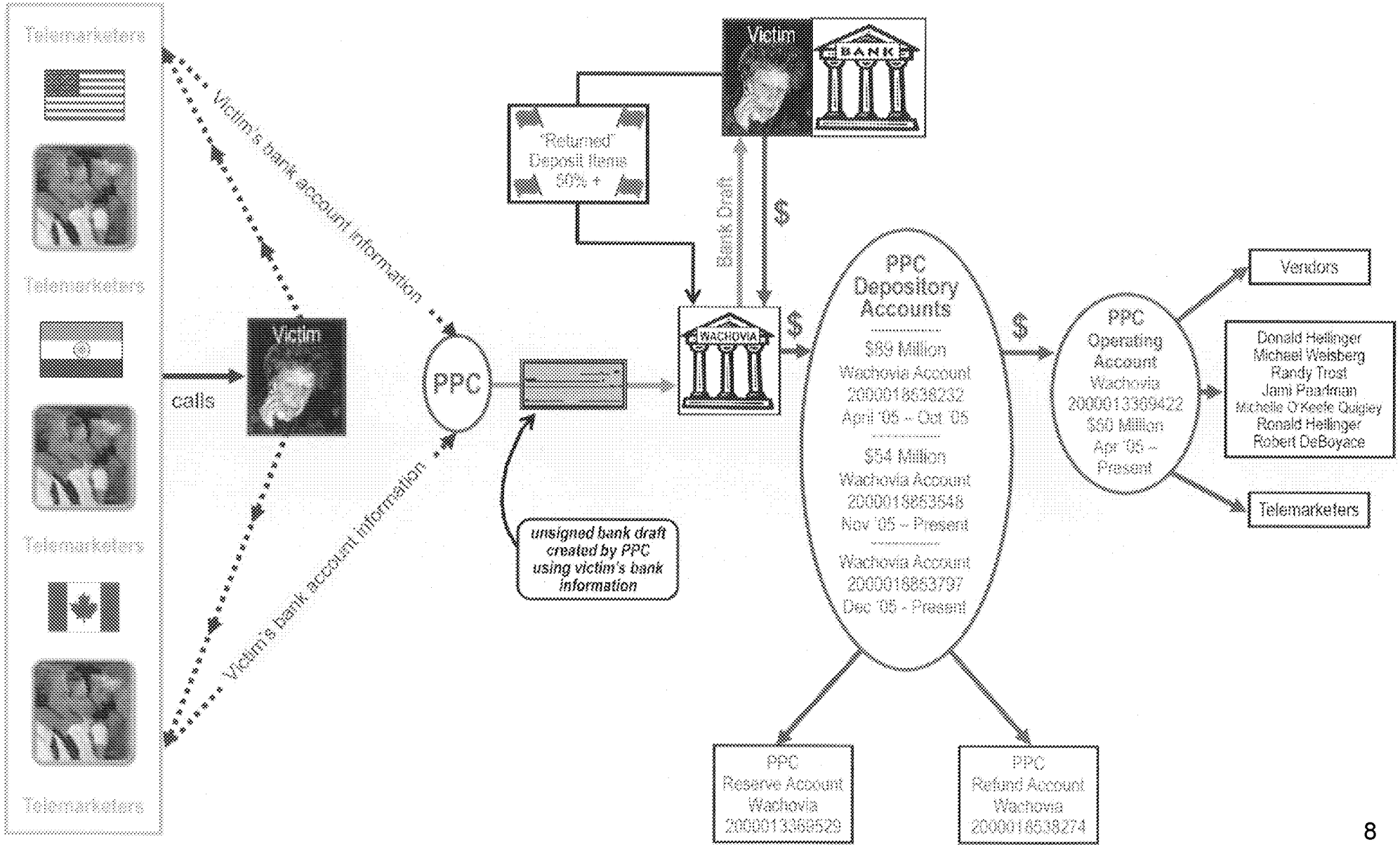
University Football Coach

Little League Coach

Sunday School Teacher

Husband, Father, Grandfather, Brother

The Payment Process



: lmeojhlihcbbcapbcmliiebhcaaa.justin@paymentprocessingcenter.com
= 0000000353
: 00000000D8B3FD5A785EC54E87ADC17FEBD9131424232100
: To the fine people that made hellish phone abuse a little more bearable,
Thank you for making my summer a little less tedious and a little more

, I am glad to have shared the daily death-threats, hate-filled rants, and ignorance with all of you. I think sometime in the next couple weeks I may almost (in some kind of sick way) miss the sound of shit-kickers screamed obsenities over the verification playback.

bacon-speckled tomato soup, dealt with a phonebook's worth of customer callbacks, and a lot of soggy bread from the sandwich club.
When you come into work on Monday don't be sad that my cute little ass isn't around, be happy... because finally one of us will get to know what daylight looks like during a weekday. Just remember my smiling face and boyish good

I know the customer service number and I'm not afraid to call with my bank rep on the line)

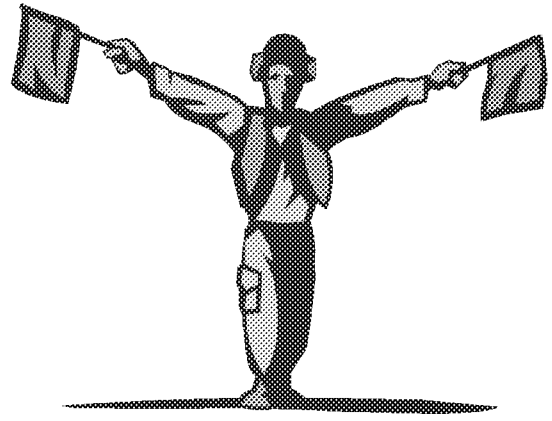
Now, as I hang up my Steno Pad and descend back in to a world of relative normality I would like to say THANK YOU to everyone.

Side note to Michael: How much exactly do I owe you for the knowledge that it takes a total of 16 combined brain cells and teeth to provide your bank account information to a stranger on the phone to order something with as stupid a name as Washballs? or; the knowledge that old people are just plain easy to trick?

stay in touch,
Justin

Returns – Charge Backs

- At inception, Wachovia **anticipated returns exceeding 35 percent** (compared to approximately 1/2 of 1 percent for all checks)
- Actual returns exceeded **50 percent**
- Wachovia charged PPC substantial fee for returns
- Wachovia offered PPC volume discounts on return fees



Banknorth, N.A.

AFFIDAVIT OF UNAUTHORIZED CONSUMER DRAFT

(Type or Print Neatly)

Bank: Banknorth Massachusetts
Banking Center: SW Commons/39
RC: 3390
Telephone #: (508) 754 - 6745

Use this form for drafts with the following tran codes only:
184 POD Check
187 Check

[redacted] Customer's Name
[redacted] Account Number
[redacted] Street
Apt. #
P.O. Box
Worcester City
MA State
01604 Zip
[redacted] Daytime Telephone
Home Telephone

I declare, swearing under oath, that a draft charged to my account and appearing on my account statement is UNAUTHORIZED.

Check appropriate Section I OR Section II:

I. Draft Never Authorized:

☒ I have never authorized the company named above to debit my account

☐ I authorized the company named above to debit my account, but I revoked ** the authorization on _____ in the manner specified in said authorization.
Date of Revocation

** Customer must provide Bank with a copy of the written revocation

I further declare that the above transaction was not initiated by me or by any person acting on my behalf. In signing this form, I understand that the Bank will reverse any credit(s) to my account if it receives proof from the payee of the draft that I, in fact, authorized this draft.

[redacted] Customer Signature (required)
5-17-05 Date
Banking Center Representative

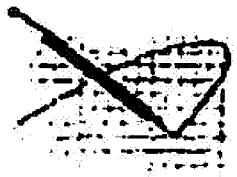
FOR USE ON PERSONAL ACCOUNTS ONLY

Instructions:

1. Fax to Adjustment Department 207-755-6315 OR Send a copy of the returned item (if available) and the signed affidavit through interoffice mail to: *Adjustment Department ME091-31*
2. Place a stop payment for the amount of the draft on the customer's account to prevent any future drafts from processing to the account. Have customer sign Stop Payment Order and remit form as usual.
3. Advise customer that provisional credit will NOT be granted on this transaction. Customer account will only be credited upon Bank receiving credit back from draft originator.

Affidavit of Unauthorized Consumer Draft Rev. 03/2004

DOUBLE YIKES!!!!



08/23/2005 06:35 PM

To

cc

Subject Guardian Marketing # 2000027007068

Tom,
Bob, Tim & I need to huddle with you on this account relationship. It is a Business Banking account, it has been actively making deposits since 6/23/05 and there is a current balance of $743,000+ in the account. The account came to us from B of A (so we are advised by [redacted] in Bus. Bnkg.) and she is [redacted]

ALL their deposits are THIRD PARTY DRAFTS!!! DOUBLE YIKES!!!!

YIKES!!!! Moreover, the drafts that are being deposited and are charging back, are not $99.99; these items are all over the place in terms of their amount. Moreover, there is another account, Suntasia, #2000027027721. Same address, same principals. $ from the Guardian acct is transferred to Suntasia and then the $ is wired out to Bank of America (funny, I thought I said they were leaving B of A at the beginning of this note, didn't I??). And, there is more, but nothing more that I want to put into a note. Bob and I really need to talk o you on tomorrow,

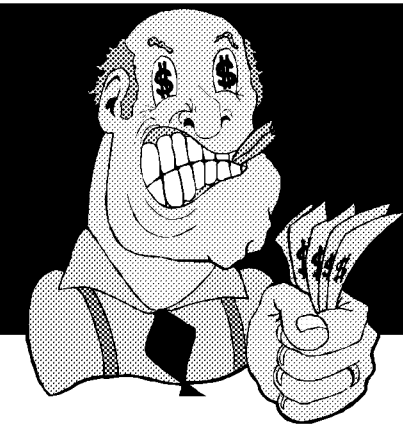
Thanks,

Wachovia Ignored Explicit Fraud Warnings From Other Banks

"The purpose of this message is to **put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam . . .** instigate an investigation into whether [PPC is] conducting legitimate business and whether [Bank is] getting **a high volume of return items on those accounts (that should place your bank on notice of potential fraud).**"

E-Mail from Citizens Bank

Money Motivates



"[P]lease mark your calendar – we will take them somewhere nice for lunch. We are making a ton of money from them."

Bank Relationship Manager to Senior Business Development Officer

"[T]his is our most profitable account. $1mm per year in profit. They have asked for Eagle tickets. What can we do?? They deserve them with all we make from them."

Bank Relationship Manager to Senior Business Development Officer

Internal Bank Communication

In a recent case:

"A request has been placed to [TPPP] to block the attached R/T, hopefully this will help minimize our daily [returns]. Please continue monitoring any suspicious issues **when time allows,** do not spend extra time trying to resolve fraudulent cases, remember that we have to focus on processing first." (emphasis in original)

This bank charged TPPP $11 per returned item. Daily fee income for the bank often exceeded more than $20,000.

Identification of Suspect Banks and TPPPs

- FTC investigations
- Victims/Sentinel
- Bank regulators
- Clearing houses (exception reports)
- Ongoing investigations (cooperators, banks)

A simple proposition.

Mass-market scammers need access to payment systems (RCC's, ACH, CC) to take consumers' money. Without bank access there are no unauthorized withdrawals.

Banks are stationary (no "whack-a-mole"), regulated, and are concerned about reputational risk.

Banks already are required to have systems in place to prevent criminals from accessing the banking system.

Cutting off the scammers' access to the payment systems is relatively efficient and fast, and protects consumers prospectively as we investigate.

18 U.S.C. § 1345 – Anti-Fraud Injunction

- Civil injunction to stop fraud during pendency of criminal investigation
  - Predicates are wire fraud, mail fraud, healthcare fraud, banking violations
- Asset restraints
- Receiver
- Civil discovery – presumptions regarding Fifth Amendment
- Favorable legal standards (harm presumed, probable cause)

FIRREA: 12 U.S.C. § 1833a

- Civil action (standards/discovery/presumptions)
- Fraud affecting a federally-insured FI
- Predicates -- wire fraud, mail fraud, other
- Relief -- penalty equal to amount of defendant's profit or victim's loss (no provision for restitution)
- FIRREA subpoenas (documents and testimony)

18 U.S.C. § 1960 – Illegal Money Transmitting Business

- Criminal statute
- Owners, managers, operators
- Money transmitting affecting interstate commerce
  - Without state license where required
  - Failing to register with Treasury as a "Money Transmitter"
  - Where funds are known to be derived from a criminal offense
- Maximum sentence -- 5 years + fines

Regulatory Loophole

- Treasury Department regulation amended in 2011 arguably excludes third-party payment processors from the definition of "money transmitter" and thus is not a Money Services Business ("MSB").

- **A payment processor that originates tens of millions of dollars of debit transactions against consumers' bank accounts on behalf of Internet and telemarketing merchants may not be an MSB and may not be required to register with FinCEN or comply with the BSA.**

So far . . .

- We've issued more than 50 subpoenas to banks and TPPPs.
- Several active criminal and civil investigations.
- Banks are self-disclosing problematic TPPP relationships.
- Banks are terminating TPPP relationships and scrutinizing scammer relationships.
- Internet Payday lending – collateral benefits.
- Investigative support from USPIS, FBI, SIGTARP, USSS

In any consumer fraud case . . .

- Look to payment system for evidence and potential defendants.
- If there is a bank involved, contact its regulators and ask them to examine possible unsound practices.
- Where possible, share information with other agencies (federal, state, local).
- Consider contacting the bank at the outset of the investigation. Some banks will immediately terminate fraudsters once on notice. Others wont, but they'll be on notice.
- Some bankers are not too smart – you may have to push their noses into the muck before they smell it.

Thanks for listening!

Operation Choke Point contacts at the Consumer Protection Branch

Rich Goldberg

202[redacted]

[redacted]

[redacted]

Joel Sweet

202-[redacted]

CONSUMER PROTECTION BRANCH

July 18, 2013

CPB – FTC Joint Training Event

TOPICS

- CPB Management and Staff
- CPB's Role
- What Types of Cases Do CPB Attorneys Handle?
- Work Associated with the FTC
- Payment Processing – what we have been doing recently, and where we are headed
- Information/Evidence gathered by FTC in Civil Investigations May Lead to Development of Criminal Prosecutions

Consumer Protection Branch

Mike Blume, Director
Jill Furman, Deputy Director
Rich Goldberg, Assistant Director
Jeff Steger, Assistant Director
Andy Clark, Assistant Director

CPB has approximately 40 attorneys who participate in a nationwide practice.

CPB has approximately a dozen paralegal specialists who excel at litigation support and are well versed in modern technologies for efficient and effective courtroom presentations.

202-616-0219

CPB's Role

- The Consumer Protection Branch (CPB), a branch in the Civil Division of the Department of Justice (DOJ), enforces through civil litigation and criminal prosecutions a number of Federal statutes that protect the public health and safety, and protect consumers from unfair practices.

- *See* 28 C.F.R. § 0.45(j) for a list of Federal statutes which the branch has long enforced.

- Other consumer issues are addressed with additional tools such as conspiracy, mail fraud, and wire fraud statutes.

What types of cases do CPB attorneys handle?

Traditional areas of enforcement

- Federal Trade Commission Act and other FTC-related statutes
- Food, Drug, and Cosmetic Act
- Consumer Product Safety Act
- Mail and Wire Fraud violations aimed at defrauding consumers
- National Highway Traffic Safety Administration/odometer fraud
- Defend certain federal agencies against lawsuits

Newer areas of enforcement

- Financial fraud
- Mortgage fraud
- Immigration services fraud

Which agencies do CPB Attorneys work with?

- CPB Attorneys work with various client agencies, including:
  - Federal Trade Commission
  - Consumer Product Safety Commission
  - Food and Drug Administration
  - National Highway Traffic Safety Administration in the U.S. Department of Transportation

CPB's Partnership with FTC

Our mission:

- Partner with FTC to protect consumers from deceptive trade practices.

- To work with FTC in bringing civil enforcement actions for civil penalties and injunctive relief.

- To complement these civil efforts by bringing criminal prosecutions (criminal contempt, conspiracy, mail and wire fraud).

Some Recent FTC matters

- Recent civil referrals
  - Work at home schemes
  - Do Not Call violations
  - Credit repair
  - Recovery schemes

- Recent criminal referrals:
  - Immigration services fraud
  - Debt relief
  - Loan modification
  - Cramming

CPB's Work on FTC-Related Matters

- Conduct witness interviews and proffer sessions with subjects and targets of investigations.
- Appear before Grand Juries to investigate alleged criminal conduct.
- Handle significant document review work through a hands-on approach as well as through directing government agents who work with our office.
- Develop litigation strategies.
- Draft charging documents, and legal filings.
- Handle hearings and conduct trials.

Operation Choke Point

Multi-agency effort to combat mass-marketing fraud by focusing on payment systems used to take consumers' money without authorization.

Simple propositions

Mass-market scammers need access to payment systems (RCC's, ACH, CC) to take consumers' money.

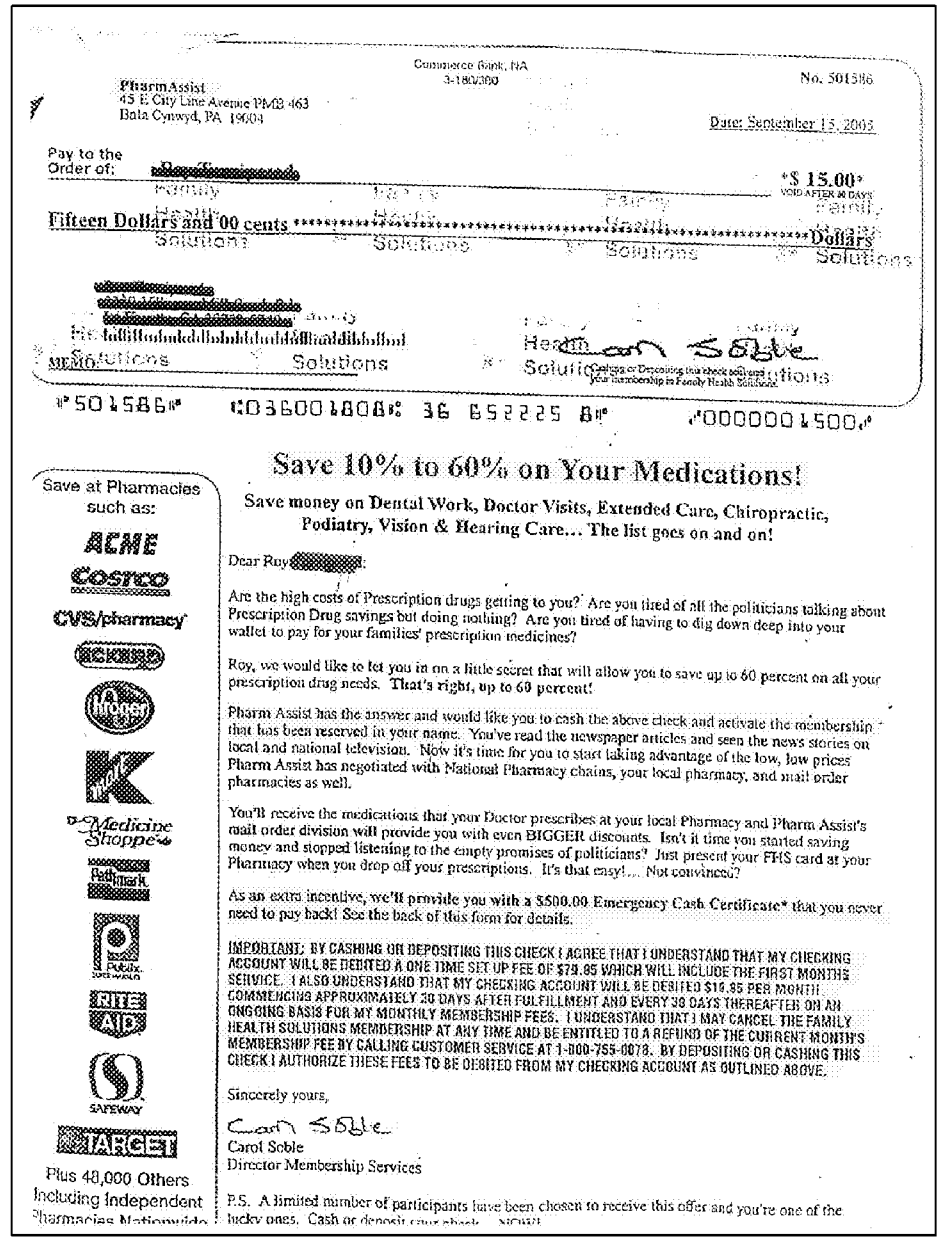
Cutting off the scammers' access to the payment systems is relatively efficient (compared to investigations and litigation against scammers) and protects consumers prospectively as we continue to investigate.

Evidence of "willful blindness" is sufficient to support a criminal fraud convictions.

Banks already are required to have systems in place to prevent criminals from accessing the banking system.

Banks are stationary (no "whack-a-mole"), regulated, and concerned about reputational risk.

Incentives to Induce Authorization



Commerce Bank, NA
3-180/360

No. 501586

PharmAssist
45 E City Line Avenue PMB 463
Bala Cynwyd, PA 19004

Date: September 15, 2003

Pay to the Order of: [redacted]

$ 15.00
VOID AFTER 30 DAYS

Fifteen Dollars and 00 cents ********** Dollars

[redacted]

MEMO

⑈501586⑈ ⑆036001808⑆ 36 652225 8⑈ ⑈000001500⑈

Save at Pharmacies such as:

ACME
Costco
CVS/pharmacy
Kmart
Medicine Shoppe
Rite Aid
SAFEWAY
TARGET

Plus 48,000 Others Including Independent Pharmacies Nationwide

Save 10% to 60% on Your Medications!

Save money on Dental Work, Doctor Visits, Extended Care, Chiropractic, Podiatry, Vision & Hearing Care... The list goes on and on!

Dear Roy [redacted]:

Are the high costs of Prescription drugs getting to you? Are you tired of all the politicians talking about Prescription Drug savings but doing nothing? Are you tired of having to dig down deep into your wallet to pay for your families' prescription medicines?

Roy, we would like to let you in on a little secret that will allow you to save up to 60 percent on all your prescription drug needs. **That's right, up to 60 percent!**

Pharm Assist has the answer and would like you to cash the above check and activate the membership that has been reserved in your name. You've read the newspaper articles and seen the news stories on local and national television. Now it's time for you to start taking advantage of the low, low prices Pharm Assist has negotiated with National Pharmacy chains, your local pharmacy, and mail order pharmacies as well.

You'll receive the medications that your Doctor prescribes at your local Pharmacy and Pharm Assist's mail order division will provide you with even BIGGER discounts. Isn't it time you started saving money and stopped listening to the empty promises of politicians? Just present your FHS card at your Pharmacy when you drop off your prescriptions. It's that easy!... Not convinced?

As an extra incentive, we'll provide you with a $500.00 Emergency Cash Certificate* that you never need to pay back! See the back of this form for details.

IMPORTANT: BY CASHING OR DEPOSITING THIS CHECK I AGREE THAT I UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED A ONE TIME SET UP FEE OF $79.85 WHICH WILL INCLUDE THE FIRST MONTHS SERVICE. I ALSO UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED $19.95 PER MONTH COMMENCING APPROXIMATELY 30 DAYS AFTER FULFILLMENT AND EVERY 30 DAYS THEREAFTER ON AN ONGOING BASIS FOR MY MONTHLY MEMBERSHIP FEES. I UNDERSTAND THAT I MAY CANCEL THE FAMILY HEALTH SOLUTIONS MEMBERSHIP AT ANY TIME AND BE ENTITLED TO A REFUND OF THE CURRENT MONTH'S MEMBERSHIP FEE BY CALLING CUSTOMER SERVICE AT 1-800-765-0078. BY DEPOSITING OR CASHING THIS CHECK I AUTHORIZE THESE FEES TO BE DEBITED FROM MY CHECKING ACCOUNT AS OUTLINED ABOVE.

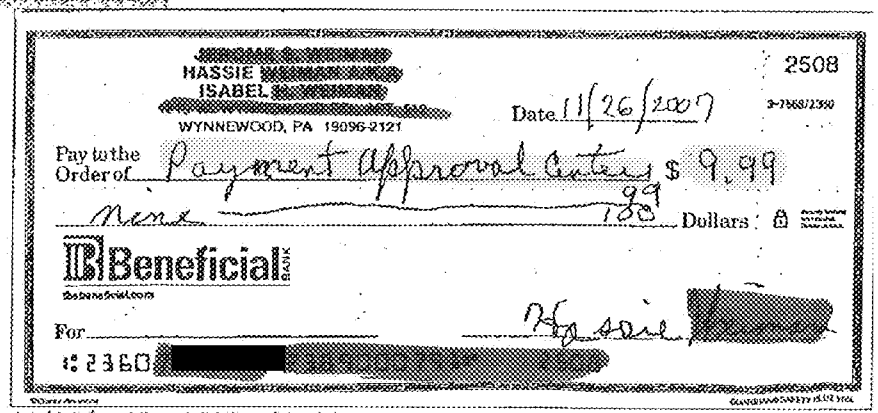
Sincerely yours,

Carol Soble
Director Membership Services

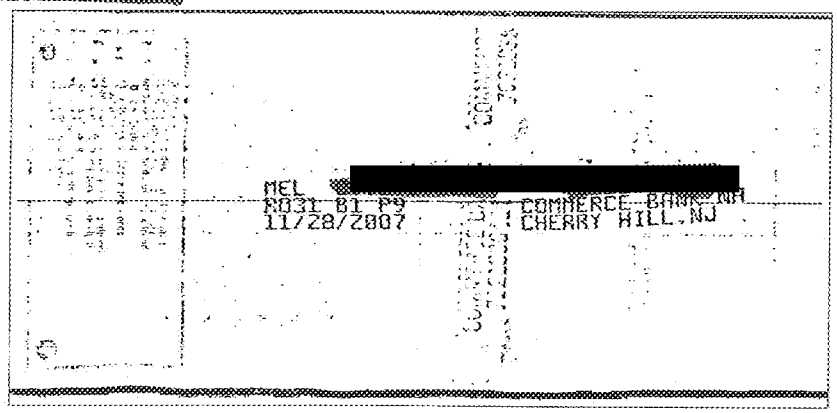
P.S. A limited number of participants have been chosen to receive this offer and you're one of the lucky ones. Cash or deposit your check NOW!

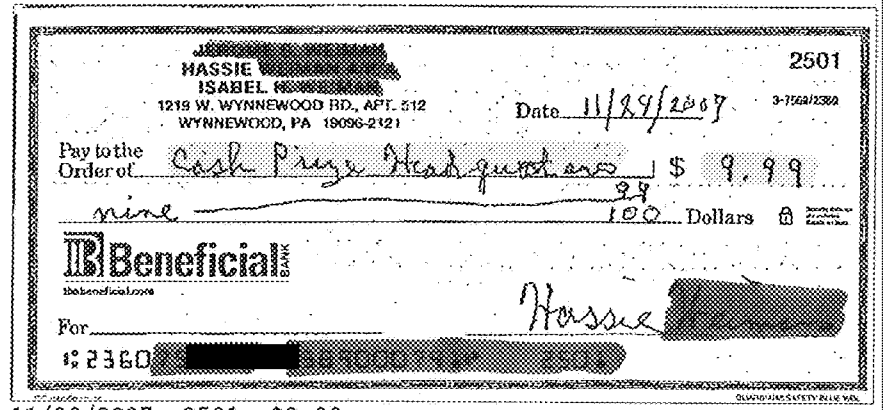
Incentives for Purported Authorization

Beneficial SAVINGS BANK

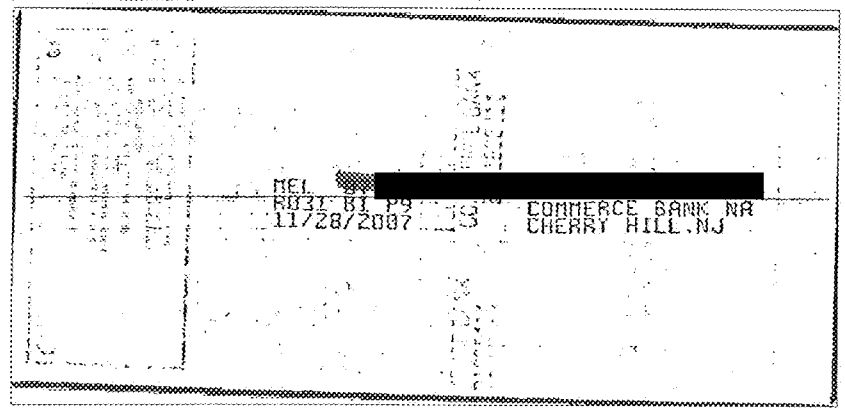

HASSIE [redacted]
ISABEL [redacted]
WYNNEWOOD, PA 19096-2121
2508
Date 11/26/2007
Pay to the Order of Payment Approval Center $ 9.99
Nine 99/100 Dollars
Beneficial
For
Hassie [redacted]
⑆ 2360 [redacted]

11/29/2007 2508 $9.99


MEL [redacted]
R031 B1 P9
11/28/2007
COMMERCE BANK NA
CHERRY HILL,NJ


HASSIE [redacted]
ISABEL [redacted]
1219 W. WYNNEWOOD RD., APT. 512
WYNNEWOOD, PA 19096-2121
2501
Date 11/29/2007
Pay to the Order of Cash Prize Headquarters $ 9.99
nine 99/100 Dollars
Beneficial
For
Hassie [redacted]
⑆ 2360 [redacted]

11/29/2007 2501 $9.99


MEL [redacted]
R031 B1 P9
11/28/2007
COMMERCE BANK NA
CHERRY HILL,NJ

Prime Time Checking

Account Number [redacted]
Statement Date: October 31, 2007
Page 1 of 3

HASSIE [redacted]
ISABEL [redacted]
WYNNEWOOD PA 19096

- For Customer Service during business hours call **215.864.6730** or e-mail us at **info@BeneficialSavingsBank.com**
- For 24-hour account information call DirectLink at **215.864.1799** or **1.800.784.8490**
- For other information visit us at **www.BeneficialSavings.com**

Account Summary

Previous Statement Balance As Of 09/30/07	1,864.08
Total Withdrawals/Charges	2,625.50
Total Deposits/Credits	2,560.02
Ending Balance	1,798.60

Annual Percentage Yield Earned: 0.50%

Check Summary

Checks Enclosed: 7

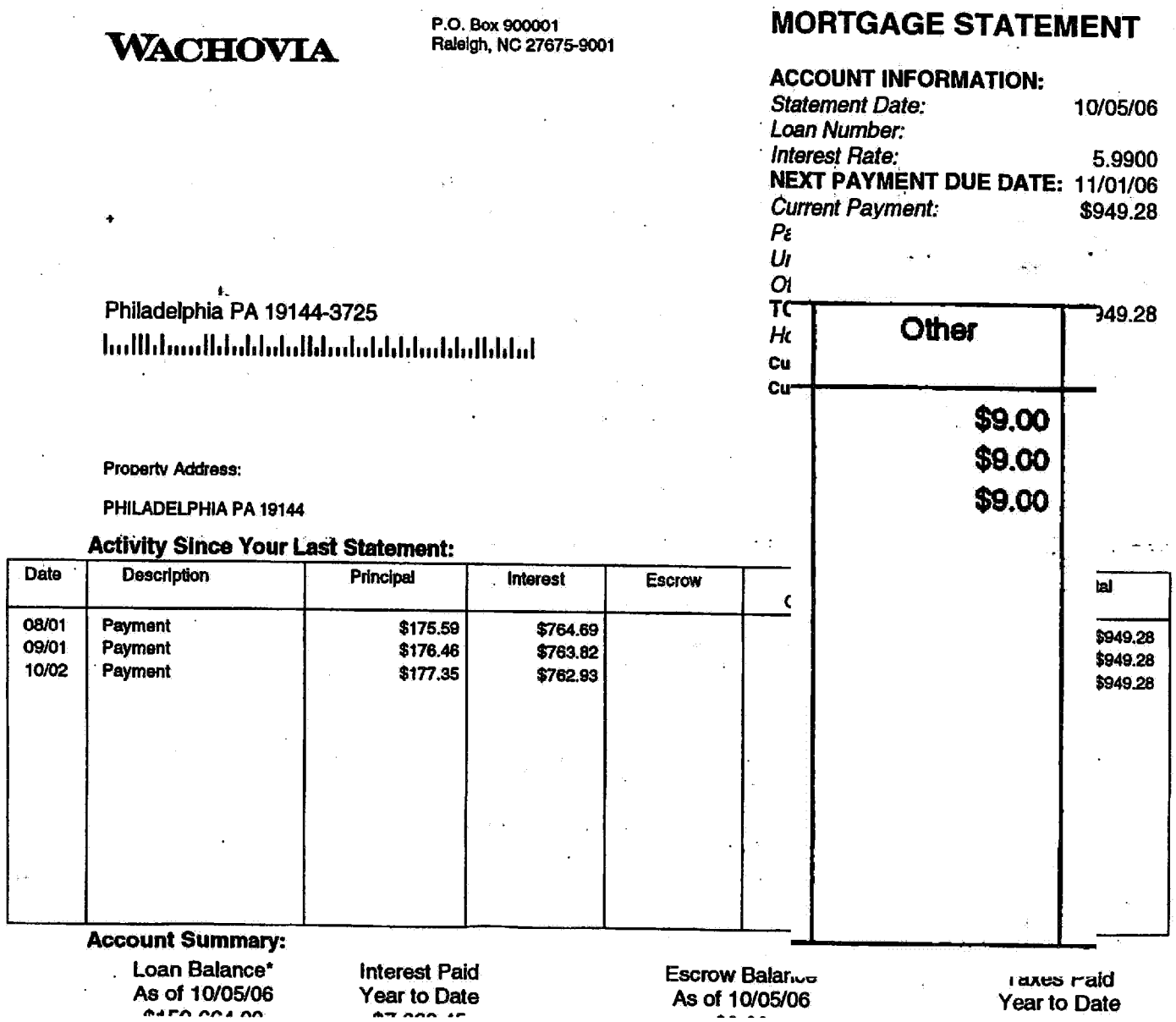
Date	Chk No.	Amount	Date	Chk No.	Amount	Date	Chk No.	Amount
10/01	2439	40.00	10/18	2462	438.50	10/30	2466	237.00
10/10	2463	13.86	10/19	2464	159.46	10/26	2470	9.95
10/24	2460*	10.00						

* Denotes Gap in Check Number Sequence

Other Transactions

Date	Description	Deposit(+) Withdrawal(-)
10/02	Ac-Us Treasury 303 -Soc Sec	565.00+
10/02	Ac-Us Treasury 303 -Soc Sec	1,194.00+
10/02	Ac-Car -Convcheck Ck-000000000002444	24.99-
10/02	Ac-Ppd -Convcheck Ck-000000000002446	27.99-
10/02	Ac-Pnd -Convcheck Ck-000000000002447	27.99-
10/02	Ac-App -Convcheck Ck-000000000002448	34.99-
10/03	Ac-Pm -Convcheck Ck-000000000002445	25.99-
10/05	Ac-Sdrd -Convcheck Ck-000000000002450	23.99-
10/05	Ac-Dcd Main Office -Convcheck Ck-000000000002449	24.99-
10/17	Ac-Ppa -Convcheck Ck-000000000002457	27.99-
10/17	Ac-Sbn -Convcheck Ck-000000000003458	39.99-
10/19	Ac-At&T Consumer -Checkpaymt Ck-00002461	77.46-
10/23	Ac-Rda -Convcheck Ck-000000000002467	31.99-
10/24	Ac-Adrd -Convcheck Ck-000000000002468	19.99-
10/24	Ac-Sr -Convcheck Ck-000000000002465	29.00-
10/25	Ac-Dpd Main Office -Convcheck Ck-000000000002469	31.99-
10/25	Ac-Reporting Data D-Convcheck Ck-000000000002471	24.99-

From Target Gift Card to Automated Electronic Mortgage Payment



WACHOVIA

P.O. Box 900001
Raleigh, NC 27675-9001

MORTGAGE STATEMENT

ACCOUNT INFORMATION:
Statement Date: 10/05/06
Loan Number:
Interest Rate: 5.9900
NEXT PAYMENT DUE DATE: 11/01/06
Current Payment: $949.28
Pa
Ur
Ot
TC 949.28
Hc
Cu
Cu

Philadelphia PA 19144-3725

Other

$9.00
$9.00
$9.00

Property Address:

PHILADELPHIA PA 19144

Activity Since Your Last Statement:

Date	Description	Principal	Interest	Escrow		tal
08/01	Payment	$175.59	$764.69			$949.28
09/01	Payment	$176.46	$763.82			$949.28
10/02	Payment	$177.35	$762.93			$949.28

Account Summary:

Loan Balance*
As of 10/05/06

Interest Paid
Year to Date

Escrow Balance
As of 10/05/06

Taxes Paid
Year to Date

Incentives to Induce Authorization

HOMEQ SERVICING

$20.00 Target' GiftCard

Expiration Date
01/26/2005

Exclusively For

PHILADELPHIA PA 19144 3725

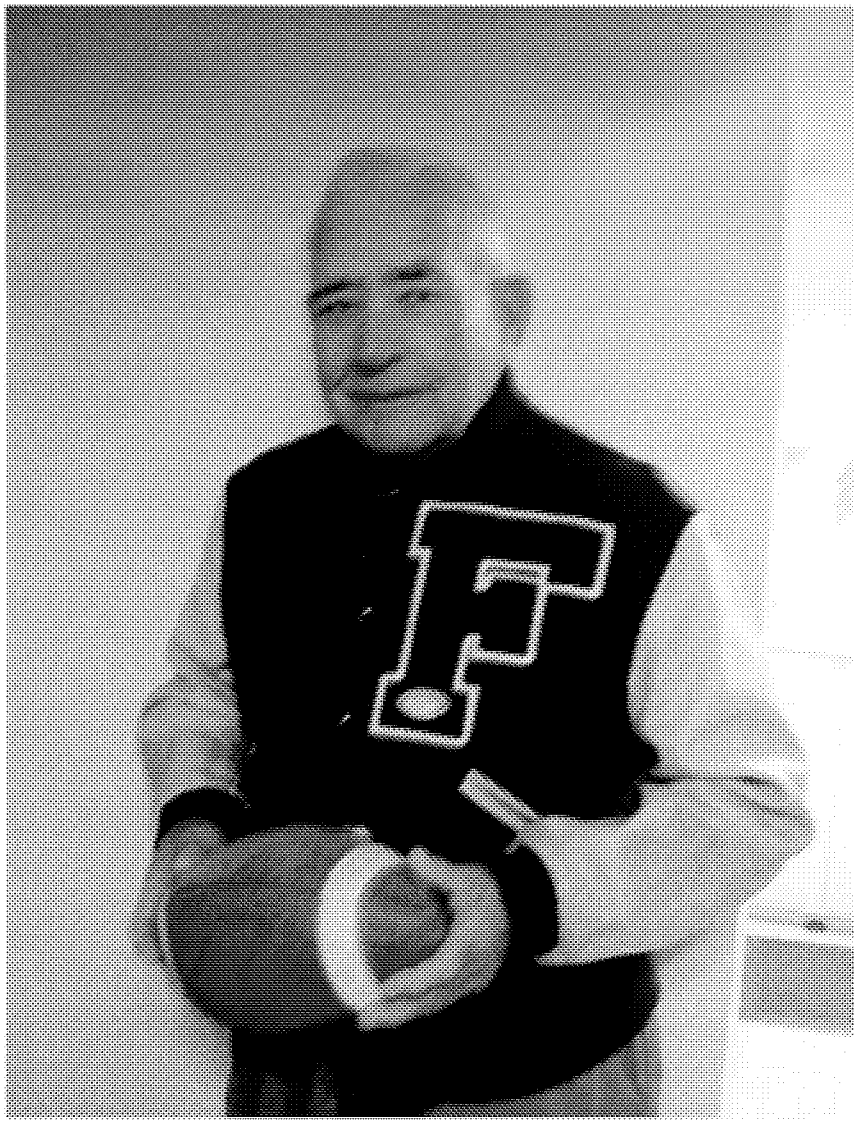
Sign and return this form to claim the $20 00 Target GiftCard reserved for you

THIS FORM IS NOT REDEEMABLE AT ANY TARGET LOCATION

X

ZC7615 Z743475\021000H3 HCB 0303297089

Purported Authorization Obtained By Telemarketer



David XXX, Sr.

1933-2006

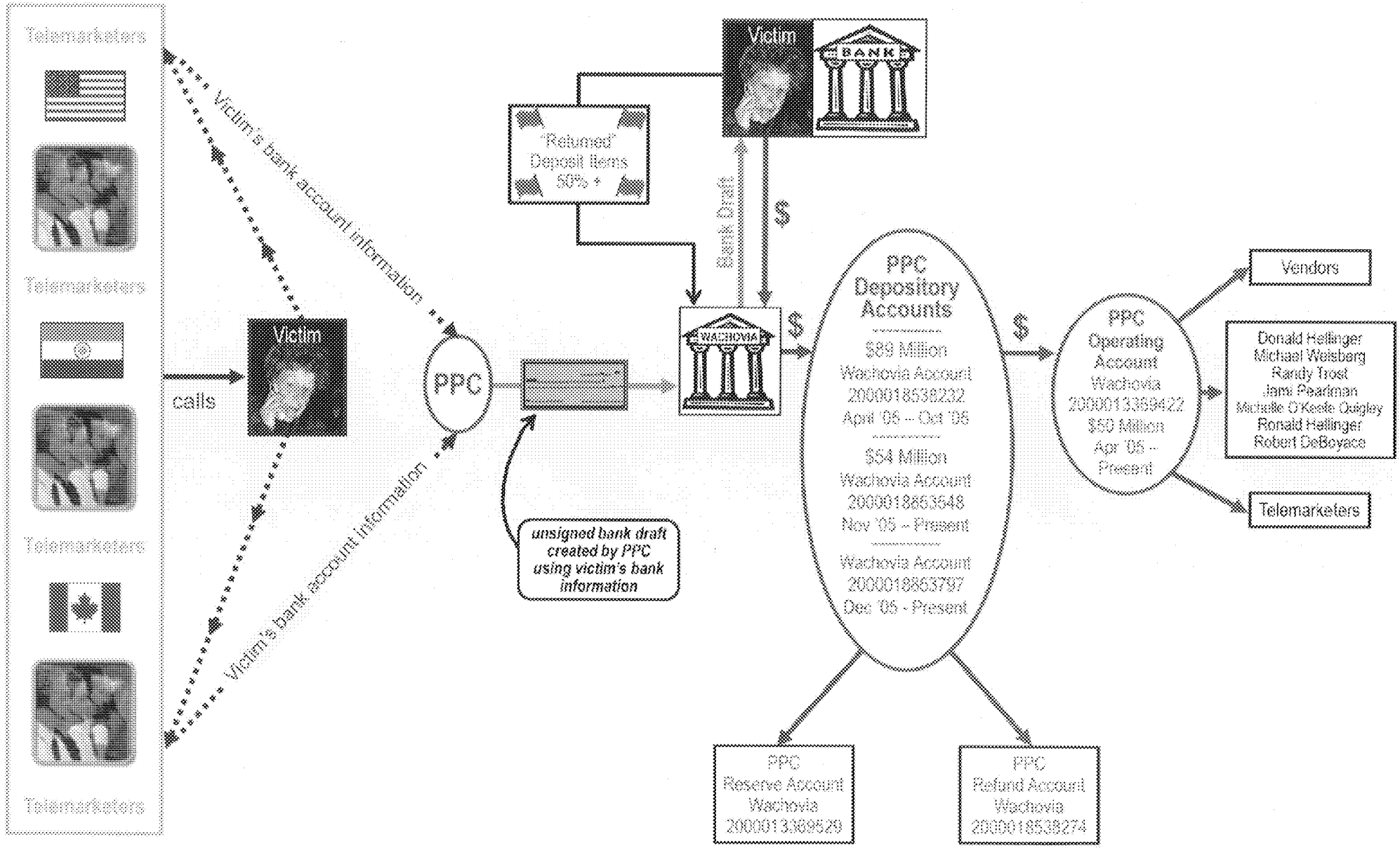
University Football Coach

Little League Coach

Sunday School Teacher

Husband, Father, Grandfather, Brother

The Payment Process



: lmeojhlihcbbcapbcmliiebhcaaa.justin@paymentprocessingcenter.com
= 0000000353
: 00000000D8B3FD5A785EC54E87ADC17FEBD9131424232100
: To the fine people that made hellish phone abuse a little more bearable,
Thank you for making my summer a little less tedious and a little more

, I am glad to have shared the daily death-threats, hate-filled rants, and ignorance with all of you. I think sometime in the next couple weeks I may almost (in some kind of sick way) miss the sound of shit-kickers screamed obsenities over the verification playback.

bacon-speckled tomato soup, dealt with a phonebook's worth of customer callbacks, and a lot of soggy bread from the sandwich club.
When you come into work on Monday don't be sad that my cute little ass isn't around, be happy... because finally one of us will get to know what daylight looks like during a weekday. Just remember my smiling face and boyish good

I know the customer service number and I'm not afraid to call with my bank rep on the line)

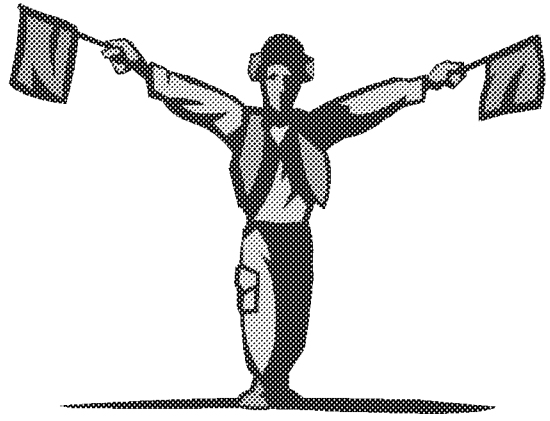
Now, as I hang up my Steno Pad and descend back in to a world of relative normality I would like to say THANK YOU to everyone.

Side note to Michael: How much exactly do I owe you for the knowledge that it takes a total of 16 combined brain cells and teeth to provide your bank account information to a stranger on the phone to order something with as stupid a name as Washballs? or; the knowledge that old people are just plain easy to trick?

stay in touch,
Justin

Returns – the big red flag!

- At inception, Wachovia **anticipated returns exceeding 35 percent** (compared to approximately 1/2 of 1 percent for all checks)
- Actual returns exceeded **50 percent**
- Wachovia charged PPC substantial fee for returns
- Wachovia offered PPC volume discounts on return fees



Banknorth, N.A.

AFFIDAVIT OF UNAUTHORIZED CONSUMER DRAFT

(Type or Print Neatly)

Bank: Banknorth Massachusetts
Banking Center: SW Commons/39
RC: 3390
Telephone #: (508) 754 - 6745

Use this form for drafts with the following tran codes only:
184 POD Check
187 Check

[redacted] Customer's Name
[redacted] Account Number
[redacted] Street
Apt. #
P.O. Box
Worcester City
MA State
01604 Zip
[redacted] Daytime Telephone
Home Telephone

I declare, swearing under oath, that a draft charged to my account and appearing on my account statement is UNAUTHORIZED.

Check appropriate Section I OR Section II:

I. Draft Never Authorized:

☒ I have never authorized the company named above to debit my account

☐ I authorized the company named above to debit my account, but I revoked ** the authorization on _____ in the manner specified in said authorization.
Date of Revocation

** Customer must provide Bank with a copy of the written revocation

I further declare that the above transaction was not initiated by me or by any person acting on my behalf. In signing this form, I understand that the Bank will reverse any credit(s) to my account if it receives proof from the payee of the draft that I, in fact, authorized this draft.

[redacted] Customer Signature (required)
5-17-05 Date
Banking Center Representative

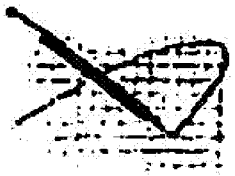
FOR USE ON PERSONAL ACCOUNTS ONLY

nstructions:

1. Fax to Adjustment Department 207-755-6315 OR Send a copy of the returned item (if available) and the signed affidavit through interoffice mail to: *Adjustment Department ME091-31*
2. Place a stop payment for the amount of the draft on the customer's account to prevent any future drafts from processing to the account. Have customer sign Stop Payment Order and remit form as usual.
3. Advise customer that provisional credit will NOT be granted on this transaction. Customer account will only be credited upon Bank receiving credit back from draft originator.

fidavit of Unauthorized Consumer Draft Rev. 03/2004

DOUBLE YIKES!!!!



08/23/2005 06:35 PM

To

cc

Subject Guardian Marketing # 2000027007068

Tom,
Bob, Tim & I need to huddle with you on this account relationship. It is a Business Banking account, it has been actively making deposits since 6/23/05 and there is a current balance of $743,000+ in the account. The account came to us from B of A (so we are advised by : n Bus. Bnkg.) and she is

ALL their deposits are THIRD PARTY DRAFTS!!! DOUBLE YIKES!!!!

YIKES!!!! Moreover, the drafts that are being deposited and are charging back, are not $99.99; these items are all over the place in terms of their amount. Moreover, there is another account, Suntasia, #2000027027721. Same address, same principals. $ from the Guardian acct is transferred to Suntasia and then the $ is wired out to Bank of America (funny, I thought I said they were leaving B of A at the beginning of this note, didn't I??). And, there is more, but nothing more that I want to put into a note. Bob and I really need to talk o you on tomorrow,

Thanks,

Wachovia Ignored Explicit Fraud Warnings From Other Banks

"The purpose of this message is to **put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam . . .** instigate an investigation into whether [PPC is] conducting legitimate business and whether [Bank is] getting **a high volume of return items on those accounts (that should place your bank on notice of potential fraud).**"

E-Mail from Citizens Bank

Money Motivates

"[P]lease mark your calendar – we will take them somewhere nice for lunch. We are making a ton of money from them."

Bank Relationship Manager to Senior Business Development Officer

"[T]his is our most profitable account. $1mm per year in profit. They have asked for Eagle tickets. What can we do?? They deserve them with all we make from them."

Bank Relationship Manager to Senior Business Development Officer

Internal Bank Communication

In a recent case:

"A request has been placed to [TPPP] to block the attached R/T, hopefully this will help minimize our daily [returns]. Please continue monitoring any suspicious issues **when time allows**, do not spend extra time trying to resolve fraudulent cases, remember that we have to focus on processing first." (emphasis in original)

This bank charged TPPP $11 per returned item. Daily fee income for the bank often exceeded more than $20,000.

Anti-Fraud Injunction 18 U.S.C. § 1345

- Civil injunction to stop fraud during pendency of criminal investigation
  - Predicates are wire fraud, mail fraud, healthcare fraud, banking violations
- Asset restraints
- Receiver
- Civil discovery – presumptions regarding Fifth Amendment
- Favorable legal standards (harm presumed, probable cause)

FIRREA
12 U.S.C. § 1833a

- Civil action (standards/discovery/presumptions)
- Fraud affecting a federally-insured FI
- Predicates – wire fraud, mail fraud, other
- Relief – penalty equal to amount of defendant's profit or victim's loss (no provision for restitution)
- FIRREA subpoenas (documents and testimony)

Illegal Money Transmitting Business 18 U.S.C. § 1960

- Criminal statute
- Owners, managers, operators
- Money transmitting affecting interstate commerce
  - Without state license where required
  - Failing to register with Treasury as a "Money Transmitter"
  - Where funds are known to be derived from a criminal offense
- Maximum sentence – 5 years + fines

Regulatory Loophole

- Treasury Department regulation amended in 2011 arguably excludes third-party payment processors from the definition of "money transmitter" and thus is not a Money Services Business ("MSB").

- **A payment processor that originates tens of millions of dollars of debit transactions against consumers' bank accounts on behalf of Internet and telemarketing merchants may not be an MSB and may not be required to register with FinCEN or comply with the BSA.**

Identification of Suspect Banks and TPPPs

- FTC investigations
- Victims/Sentinel
- Bank regulators
- Clearing houses (exception reports)
- Ongoing investigations (cooperators, banks)

Since March. . .

- Issued more than 50 subpoenas to banks and TPPPs.
- Several active criminal and civil investigations.
- Banks are self-disclosing problematic TPPP relationships.
- Banks are terminating TPPP relationships and scrutinizing scammer relationships.
- Internet Payday lending – collateral benefits.
- Investigative support from USPIS, FBI, SIGTARP, USSS, FDIC-OIG

In any consumer fraud case …

- Look to payment system for evidence and potential defendants.
- If there is a bank involved, contact its regulators and ask them to examine possible unsound practices.
- Where possible, share information with other agencies (federal, state, local).
- Consider contacting the bank and its regulator at the outset of the investigation. Some banks will immediately terminate fraudsters once on notice. Others wont, but at least they'll be on notice.
- Some bankers are not too smart – you may have to push their noses into the muck before they smell it.

Operation Choke Point contacts at the CPB

Rich Goldberg

[redacted]

[redacted]

[redacted]

Joel Sweet

[redacted]

Information/Evidence Sharing

1. Most Common Criminal Charges
2. Common Investigative Techniques
3. How we use FTC information
4. [redacted]

Mail and Wire Fraud

- Mail Fraud (18 U.S.C. § 1341)
  - Scheme to defraud
  - Material misrepresentations or omissions
  - Mail (or FedEx/UPS) used
  - 20 years/$250,000 fine
  - Defendant mails bogus promotional materials to victims

- Wire Fraud (18 U.S.C. § 1343)
  - Identical to Mail Fraud, only uses wire transmissions
  - Telemarketer lies to victims about the risk over the telephone

Conspiracy

- 18 U.S.C. § 1349 (Conspiracy to commit Mail/Wire Fraud)
  - Two or more people agree to commit mail or wire fraud
  - 20 year maximum penalty

- 18 U.S.C. § 371 (Conspiracy)
  - Conspiracy to commit offense or defraud the government
  - Includes conspiracy to obstruct lawful functions
    - Thwarting regulatory efforts
  - 5 year maximum penalty

Other Common Crimes

- Criminal Contempt (18 U.S.C. § 401(3))
  - Violations of Judicial Orders
  - Violations of telemarketing bans
- Obstruction (18 U.S.C. § 1512(c)(2))
- False Statements (18 U.S.C. § 1001)

Investigative Techniques

- Grand Jury
  - Secret proceedings
  - Able to compel witnesses
    - Under oath, subject to perjury penalties
    - Hostile witnesses
  - Obtain records from banks, phone companies, internet service providers
  - Obtain indictments

Investigative Techniques

Investigative Techniques

- Search Warrants
  - Probable cause that contraband or evidence will be found in the specific location
  - Physical evidence
    - Photographs, documents
    - Where does the target work? Where does he sleep?
  - Electronic evidence
    - Computers
    - Cell phones
    - Email from providers

Investigative Techniques

- GPS Trackers
- Undercover microphones and cameras
- Pole cameras
- Wiretaps
  - Specific phone
  - Specific email address
  - Target specific (all phones used by target)
  - Room bugs

FTC-CPB Criminal Matters

- Is this a potential criminal case?
  - Do you have specific victims who suffered a loss?
  - Is there any evidence that the target intentionally violated the law?
    - Specific false promises?
    - Did target hide his identity?
    - Did target provide any service to victims?
  - Did the target lie to the government?
    - Hide evidence?
    - Shred documents?
    - Delete computer files?

FTC-CPB Criminal Matters

- Consumer Sentinel
  - Identify specific victims
  - Obtain their communication with targets
  - Obtain their bank records
- FTC Undercover Investigation
  - Recorded investigator calls
  - Promotional material
- Identify specific employees
- This is probable cause for a search warrant


DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR

UNITED STATES DEPARTMENT OF JUSTICE - CIVIL DIVISION
CORRESPONDENCE TRACKING SYSTEM

ID: 67580 Executive Sec #: Cover Sheet Date: 07/18/2013
Document Type: Litigation Document Date: 07/16/2013
File Code: Deputy for Consumer Protection Branch Date Received: 07/18/2013
Responding Unit: Consumer Protection Branch Response Due: 07/26/2013
Reviewer: Richard Goldberg As soon as practical
Drafter: Joel Sweet [redacted] Date Closed:
To: Stuart F. Delery, A/AAG, Civil Division; thru: Maame Ewusi-Mensah Frimpong, DAAG SG Due:
From: Michael S. Blume, Director, Consumer Protection Branch

Subject: Payment Processor Investigation - Request for Issuance of Subpoenas to Banks: [redacted]

Comments: Maame Ewusi-Mensah Frimpong: Review and comment
Stuart F. Delery: Sign subpoenas [redacted]
Time Frame: "We request your approval by July 26, 2013. There are no external deadlines."

Actions: Assigned To	Initials	Date Assigned	Finished
Maame Ewusi-Mensah Frimpong		JUL 18 2013	7/31/13
Stuart F. Delery	SFD	AUG 6 2013	8/8/13
[redacted]		AUG 8 2013	AUG 8 2013
Michael Blume		AUG 8 2013	

Notes: Stuart - I recommend that you approve these subpoenas. As discussed in the memo, they are in furtherance of 3PPP — [redacted] some follow up on prior subpoena returns, as well as information from the FTC.

U.S. Department of Justice

Civil Division

Washington, DC 20530

July 16, 2013

TO: Stuart F. Delery
Acting Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: Payment Processor Investigation – Request for Issuance of Subpoenas to Banks

Time Frame

We request your approval by July 26, 2013. There are no external deadlines.

Recommendation

We seek authorization to issue [redacted] under the Financial Institutions Reform, Recovery and Enforcement Act of 1989, 12 U.S.C. § 1833a(g)(1)(C) ("FIRREA"). The subpoenas would be directed to the entities described below.

Case Summary

These subpoenas are requested in furtherance of Operation Choke Point, a multi-agency task force combating mass-market consumer fraud through a focus on payment systems. Our objective is to identify gateways used by scammers to gain access to the national payment systems. To that end, in February 2013, we served subpoenas upon [redacted] banks and [redacted] third-party payment processors. Based upon information obtained in response to those subpoenas and from other sources, we determined that our process for identifying banks and processors engaged in illicit conduct is accurate. We have opened investigations into several of these entities.

In May 2013, we served [redacted] additional subpoenas on financial institutions that we identified as processing payments on behalf of fraudsters, or that had been identified by suspected fraudulent payment processors as prospects for originating transactions. These subpoenas were narrow in scope and requested documents sufficient for us to identify potentially fraudulent merchant and processors. The documents we have received in response to these subpoenas further confirm that our process for identifying suspect financial institutions is highly accurate. Based on the responses we have received, including self-disclosures by some banks, we have opened several more investigations. We are continuing to evaluate the documents that we receive in response to the subpoenas to determine whether banks knowingly permitted their infrastructure to be used by fraudsters (or remained willfully blind to that conduct), and possibly processors and fraudulent merchants.

Discussion

[redacted]

[redacted]

B. Banks Identified in Our Continuing Investigations.

[redacted]

C. Additional Banks Identified by the Federal Trade Commission.

The FTC continues to provide us with names of banks identified during its investigations of fraudsters and payment processors. In response to Civil Investigative Demands, the FTC received documents that identify the following banks as currently or historically provided banking services to fraudsters, or as having been targeted by fraudsters to be approached for provide ACH and/or check payment services:

[redacted]

[redacted]

[redacted]

D. Banks Previously Misidentified.

[redacted]

[redacted]

As we did in May 2013 with prior subpoenas, we intend to serve the subpoenas upon the respective bank's CEO with a transmittal letter stating that the subpoena has been issued in connection with an investigation of consumer fraud. To assist the bank and its counsel to understand the nature of our investigation, we will include a copy of a recent FinCEN Advisory and bank regulator guidance concerning risks associated with third-party payment processors.

Conclusion

We request that you sign the attached FIRREA subpoenas.

(Goldberg/Sweet/[redacted])

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Monday, July 22, 2013 4:10 PM
To: Blume, Michael S. ([redacted]@CIV.USDOJ.GOV)
Subject: FW: 3PPP Detail

FYI

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Monday, July 22, 2013 4:10 PM
To: Delery, Stuart F. (CIV)
Cc: Olin, Jonathan F. (CIV)
Subject: 3PPP Detail

Hi Stuart –

As we discussed with you, Joel Sweet's detail is set to end on August 24, and we believe it would be highly beneficial to the Third-Party Payment Processor Initiative to extend the detail. Joel has spoken with his supervisors in the USAO, and they are open to extending the detail if they can get approval to extend some term attorneys they have in their office. I have spoken to Ken about whether there is anything we can do to support this request, but apparently there is not (as these attorneys are not working our cases). Ken also indicated that he believes we could continue to fund Joel's detail for another six months if you approved it; he is confirming with his Budget staff. (At your request, we explored with Joel the possibility of moving permanently to the Consumer Protection Branch. Mike would be happy to have him. [redacted] His preference would be to continue the detail for now.)

Given the upcoming vacations, we would like to resolve this by the end of July. Given the situation as described above, my proposal is that you or Jon reach out to U.S. Attorney Memeger to make the request. Please let me know if you would like me to draft an email or talking points for this purpose, or if you would like to discuss further.

Thank you for your continued support of the initiative; we greatly appreciate it.

Regards,
Maame

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

United States of America
v.
Payment Processing Center

A Case Study of Remotely Created Check Abuse and Payment System Vulnerabilities

Joel M. Sweet, Trial Attorney, Consumer Protection Branch, DOJ
(detailee from United States Attorney's Office for the Eastern District of Pennsylvania)

Disclaimer

Any opinions reflected in this presentation are those of the presenter and are not necessarily those of the Department of Justice, or any government official, agency, department, or branch.

The information in this presentation is from public sources.

Mass Market Consumer Fraud – a National Scourge

Bernie Madoff swindled more than $40B from a select group of mostly wealthy investors.

Fraudsters steal more than $40B from consumers – mostly the elderly and those in the lower middle class – every year!

Which is most likely to receive attention from law enforcement, regulators, and the press: a single theft of $100 million, or one million thefts of $100?

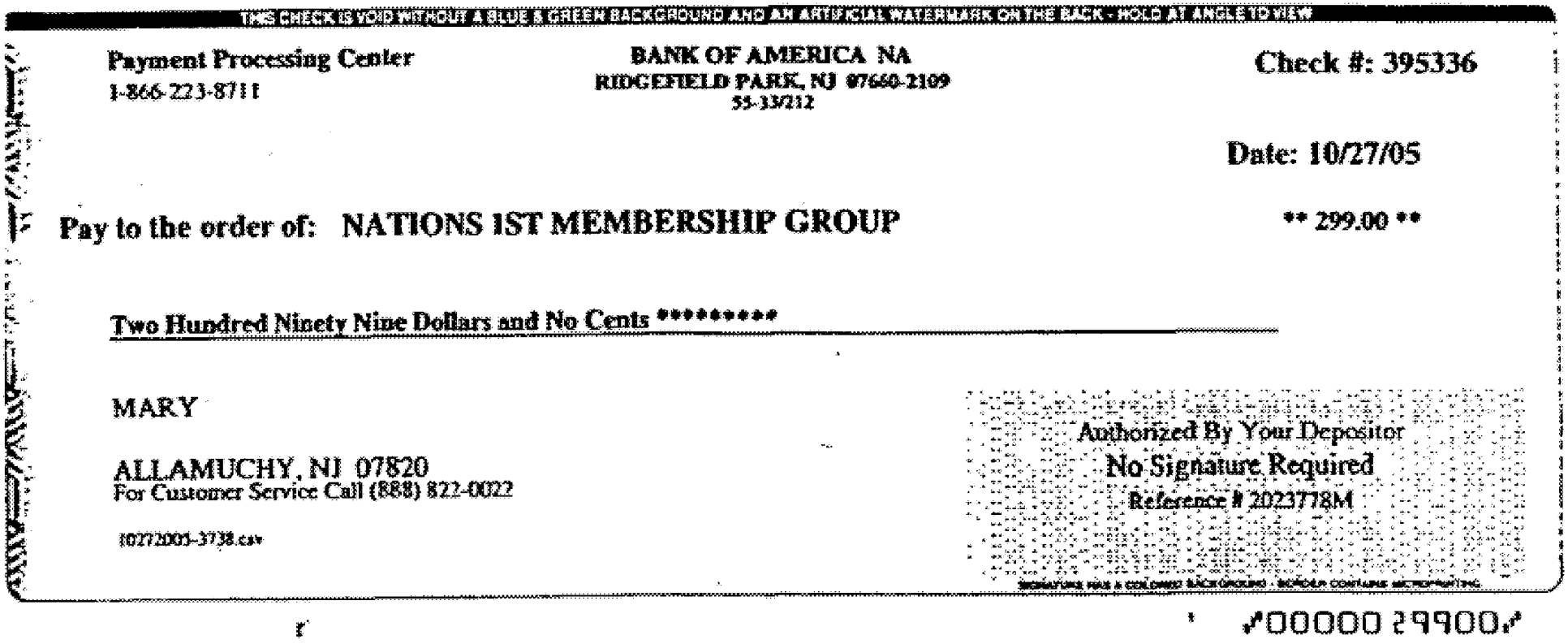
Common Methods of Payment System Abuse

- Debit transactions originated by payment processors and banks on behalf of telemarketing and Internet fraudsters
- Phone company bills used to originate unauthorized charges ("cramming")
- Mortgage payment mechanisms used to originate unauthorized charges

Law Enforcement Challenges to Prosecuting Telemarketing/Internet Fraud

- Jurisdictional limitations (state and international)
- Fraudsters change corporate identities and law enforcement plays "whack-a-mole"
- Victims are dispersed geographically
- Victims cannot identify fraudsters – no face-to-face contact
- Plausible deniability – cross-pointing among call centers, mail houses, fulfillment centers, payment processors, and banks
- Limited investigative and prosecutorial resources
- Limited reach of State Attorneys General and FTC

A Remotely Created Check ("RCC")



THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK. HOLD AT ANGLE TO VIEW

Payment Processing Center
1-866-223-8711

BANK OF AMERICA NA
RIDGEFIELD PARK, NJ 07660-2109
55-13/212

Check #: 395336

Date: 10/27/05

Pay to the order of: NATIONS 1ST MEMBERSHIP GROUP

** 299.00 **

Two Hundred Ninety Nine Dollars and No Cents *********

MARY

ALLAMUCHY, NJ 07820
For Customer Service Call (888) 822-0022

10272005-3738.csv

Authorized By Your Depositor
No Signature Required
Reference # 2023778M

SIGNATURE HAS A COLORED BACKGROUND - BORDER CONTAINS MICROPRINTING

⑈00000 29900⑈

RCC Fraud: Well-Known to Banks

"Demand drafts can be misused to commit check fraud. This practice involves the misuse of account information to obtain funds from a person's bank account without that person's signature on a negotiable instrument. . . **demand drafts have been used by deceptive telemarketers who obtain bank account information and withdraw unauthorized funds from consumers' bank accounts,** without their realizing that such withdrawals are occurring. . . ."

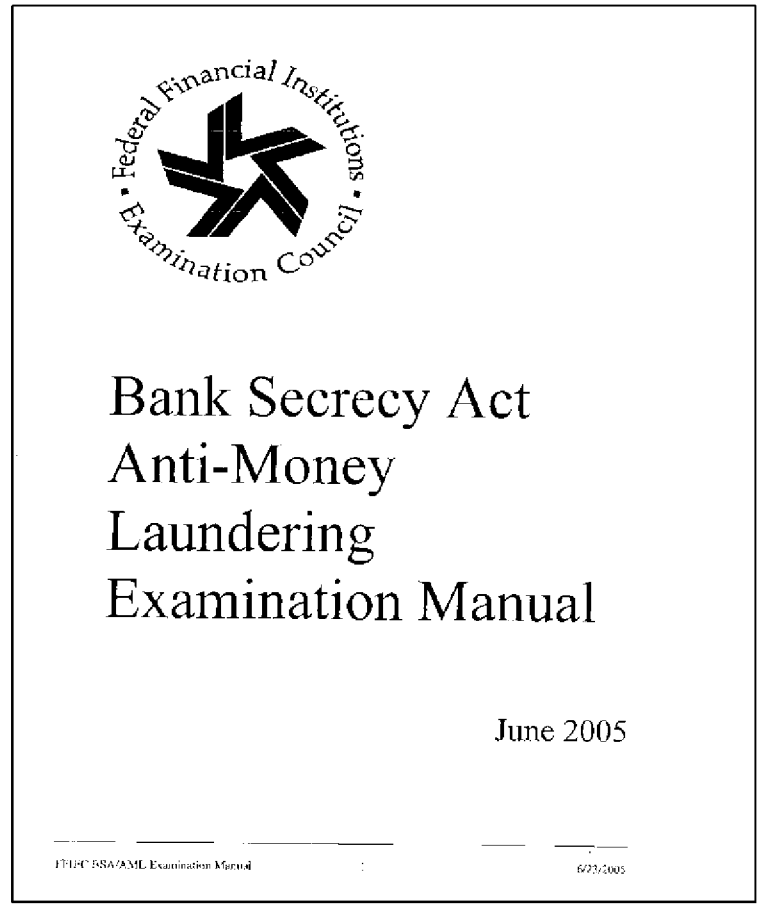
A Guide to Checks and Check Fraud, published by **Wachovia,** 2003

RCC Fraud: Well-Known to State Law Enforcement and FRB

- In 2005, 35 state attorneys general jointly request that the Federal Reserve ban RCCs from the payments system:
  - "demand drafts are frequently used to perpetrate fraud on consumers"
  - "such drafts should be eliminated" in favor of other forms of payment
  - If not eliminated, mandatory marking of RCCs and other measures to protect consumers

RCC Fraud: Well-Known to Bank Regulators

BSA/AML Examination Manual (FRB, FDIC, NCUA, OCC, and OTS)



Expanded Overview – Third-Party Payment Processors

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with its relationships with third-party payment processors, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Non-bank, or third-party, payment processors (processors) are bank customers that provide payment-processing services to merchants and other business entities.

Traditionally, processors contracted primarily with retailers that had physical locations in order to process the retailers' transactions. These merchant transactions primarily included credit card payments but also covered automated clearing house demand drafts[118] (also known as e-checks), and debit and stored value cards transactions. With the expansion of the Internet, retail borders have been eliminated. Processors may now service a variety of merchant accounts, including conventional retail and Internet-based establishments, prepaid travel, and Internet gaming enterprises.

RISK FACTORS

Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, and fraud schemes.

The bank's BSA/AML risks when dealing with a processor account are similar to risks from other activities in which the bank's customer conducts transactions through the bank on behalf of the customer's clients. When the bank is unable to identify and understand the nature and source of the transactions processed through an account, the risks to the bank and the likelihood of suspicious activity can increase. If a bank has not implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or sanctioned transactions.

[118] A demand draft is a substitute for a preprinted paper check. The draft is produced without a consumer signature but presumably with the consumer's authorization.

RISK MITIGATION

Banks offering account services to processors should develop and maintain adequate policies, procedures, and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. Verification and assessment of a processor can be completed by performing the following procedures:

- Reviewing the processor's promotional materials, including its web site, to determine the target clientele. (Businesses with elevated risk may include: offshore companies, online gambling-related operations, and online payday lenders). For example, a processor whose customers are primarily offshore would be inherently riskier than a processor whose customers are primarily restaurants.
- Determining whether the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization (ISO) opportunities" or "gateway" arrangements.[119]
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.
- Identifying the processor's major customers.
- Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.

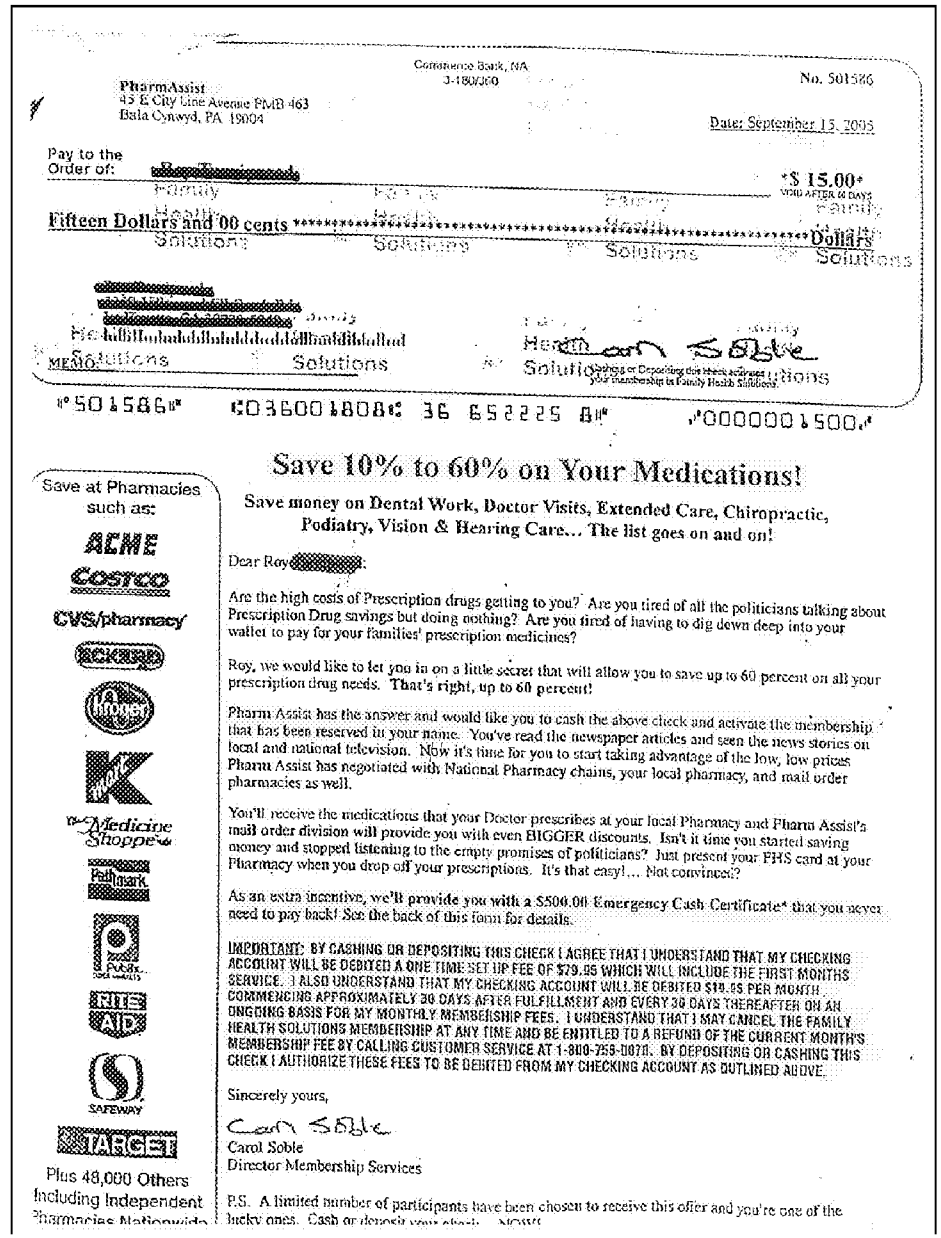
Banks that provide account services should monitor their processor relationships for any significant changes in the processors' business strategies that may affect their risk profile. Banks should periodically re-verify and update the businesses' profiles to ensure the risk assessment is appropriate.

In addition to adequate and effective account opening and due diligence procedures for processor accounts, management should monitor these relationships for unusual and suspicious activities. To effectively monitor these accounts, the bank should have an understanding of the following processor information:

- Merchant base.
- Merchant activities.
- Average number of dollar volume and number of transactions.
- "Swiping" versus "keying" volume for credit card transactions.
- Charge-back history.

[119] Gateway arrangements are similar to an Internet service provider with excess computer storage capacity who sells its capacity to a third party, who would then distribute computer service to various other individuals unknown to the provider. The third party would be making decisions about who would be receiving the service, although the provider would be providing the ultimate storage capacity. Thus, the provider bears all of the risks while receiving a smaller profit.

Incentives to Induce Authorization



Commerce Bank, NA
3-180/360

No. 501586

PharmAssist
45 E City Line Avenue PMB 463
Bala Cynwyd, PA 19004

Date: September 15, 2005

Pay to the Order of: [redacted]

$ 15.00
VOID AFTER 60 DAYS

Fifteen Dollars and 00 cents ********** Dollars

[redacted]

Solutions

⑈501586⑈ ⑆036001808⑆ 36 652225 8⑈ ⑈000001500⑈

Save at Pharmacies such as:

ACME
Costco
CVS/pharmacy
Eckerd
HA-VEE
K mart
Medicine Shoppe
Pathmark
Rite Aid
SAFEWAY
TARGET

Plus 48,000 Others Including Independent Pharmacies Nationwide

Save 10% to 60% on Your Medications!

Save money on Dental Work, Doctor Visits, Extended Care, Chiropractic, Podiatry, Vision & Hearing Care... The list goes on and on!

Dear Roy [redacted]:

Are the high costs of Prescription drugs getting to you? Are you tired of all the politicians talking about Prescription Drug savings but doing nothing? Are you tired of having to dig down deep into your wallet to pay for your families' prescription medicines?

Roy, we would like to let you in on a little secret that will allow you to save up to 60 percent on all your prescription drug needs. **That's right, up to 60 percent!**

Pharm Assist has the answer and would like you to cash the above check and activate the membership that has been reserved in your name. You've read the newspaper articles and seen the news stories on local and national television. Now it's time for you to start taking advantage of the low, low prices Pharm Assist has negotiated with National Pharmacy chains, your local pharmacy, and mail order pharmacies as well.

You'll receive the medications that your Doctor prescribes at your local Pharmacy and Pharm Assist's **mail order division will provide you with even BIGGER discounts.** Isn't it time you started saving money and stopped listening to the empty promises of politicians? Just present your FHS card at your Pharmacy when you drop off your prescriptions. It's that easy!... Not convinced?

As an extra incentive, **we'll provide you with a $500.00 Emergency Cash Certificate*** that you never need to pay back! See the back of this form for details.

IMPORTANT: BY CASHING OR DEPOSITING THIS CHECK I AGREE THAT I UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED A ONE TIME SET UP FEE OF $79.95 WHICH WILL INCLUDE THE FIRST MONTHS SERVICE. I ALSO UNDERSTAND THAT MY CHECKING ACCOUNT WILL BE DEBITED $19.95 PER MONTH COMMENCING APPROXIMATELY 30 DAYS AFTER FULFILLMENT AND EVERY 30 DAYS THEREAFTER ON AN ONGOING BASIS FOR MY MONTHLY MEMBERSHIP FEES. I UNDERSTAND THAT I MAY CANCEL THE FAMILY HEALTH SOLUTIONS MEMBERSHIP AT ANY TIME AND BE ENTITLED TO A REFUND OF THE CURRENT MONTH'S MEMBERSHIP FEE BY CALLING CUSTOMER SERVICE AT 1-800-755-0078. BY DEPOSITING OR CASHING THIS CHECK I AUTHORIZE THESE FEES TO BE DEBITED FROM MY CHECKING ACCOUNT AS OUTLINED ABOVE.

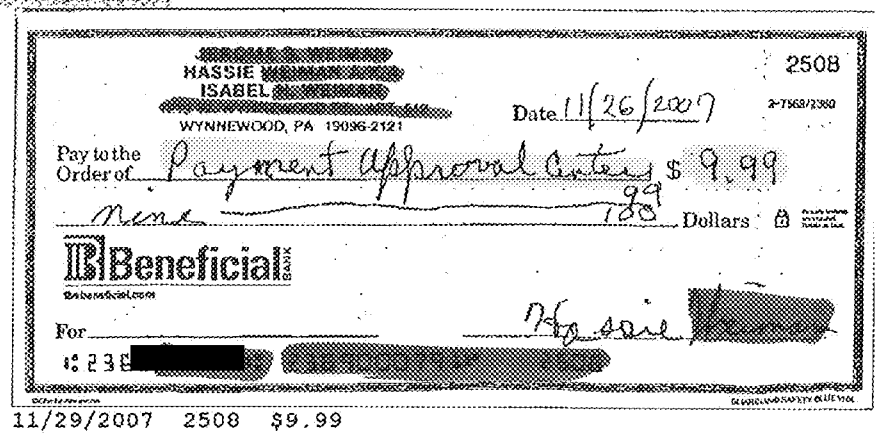
Sincerely yours,

Carol Soble
Director Membership Services

P.S. A limited number of participants have been chosen to receive this offer and you're one of the lucky ones. Cash or deposit your check... NOW!

Incentives for Purported Authorization

Beneficial SAVINGS BANK


HASSIE [redacted]
ISABEL [redacted]
WYNNEWOOD, PA 19096-2121

2508

Date 11/26/2007

Pay to the Order of Payment Approval Entry $ 9.99

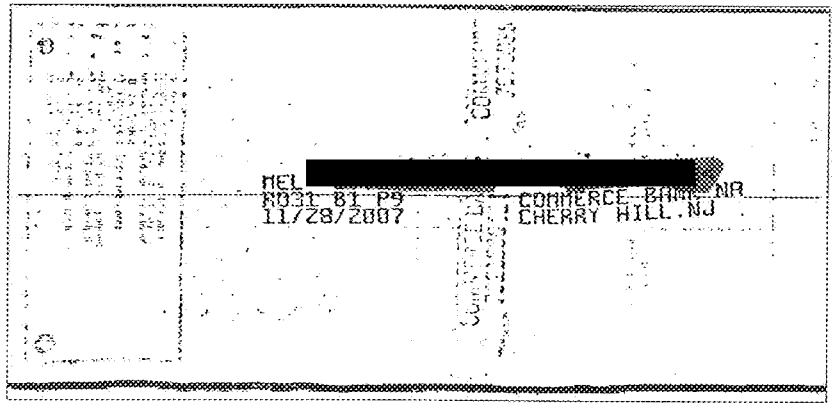
nine 99/100 Dollars

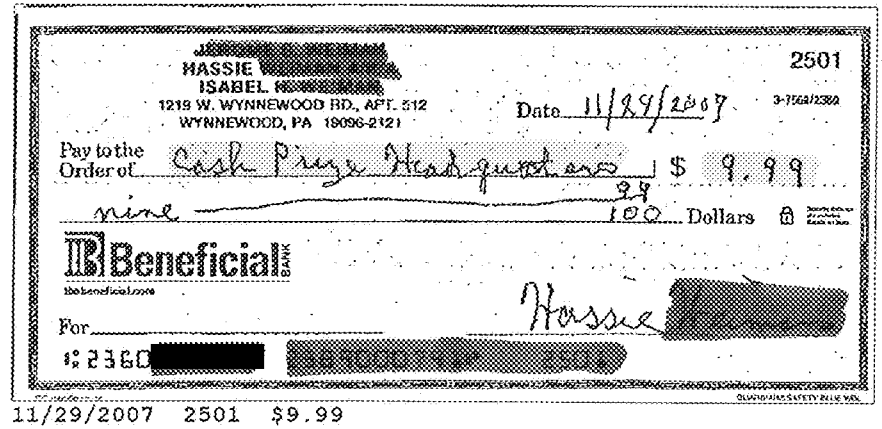
Beneficial

For [redacted]

Hassie [redacted]

11/29/2007 2508 $9.99


MEL [redacted]
R031 81 P9
11/28/2007
COMMERCE BANK NA
CHERRY HILL,NJ


HASSIE [redacted]
ISABEL [redacted]
1219 W. WYNNEWOOD RD., APT. 512
WYNNEWOOD, PA 19096-2121

2501

Date 11/29/2007

Pay to the Order of Cash Prize Headquarters $ 9.99

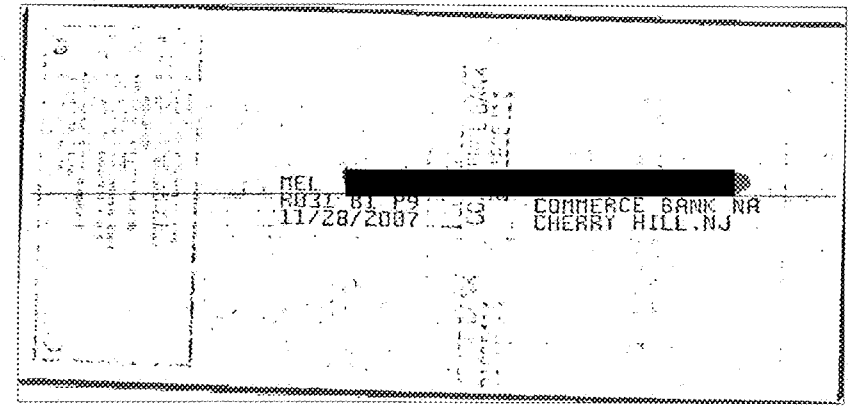
nine 99/100 Dollars

Beneficial

For [redacted]

Hassie [redacted]

11/29/2007 2501 $9.99


MEL [redacted]
R031 81 P9
11/28/2007
COMMERCE BANK NA
CHERRY HILL,NJ

Prime Time Checking

Account Number: [redacted]
Statement Date: October 31, 2007
Page: 1 of 3

- For Customer Service during business hours call **215.864.6730** or e-mail us at **info@BeneficialSavingsBank.com**
- For 24-hour account information call DirectLink at **215.864.1799** or **1.800.784.8490**
- For other information visit us at **www.BeneficialSavings.com**

[redacted]
WYNNEWOOD PA 19096

Account Summary

Previous Statement Balance As Of 09/30/07	1,864.08
Total Withdrawals/Charges	2,625.50
Total Deposits/Credits	2,560.02
Ending Balance	1,798.60

Annual Percentage Yield Earned: 0.50%

Check Summary

Checks Enclosed: 7

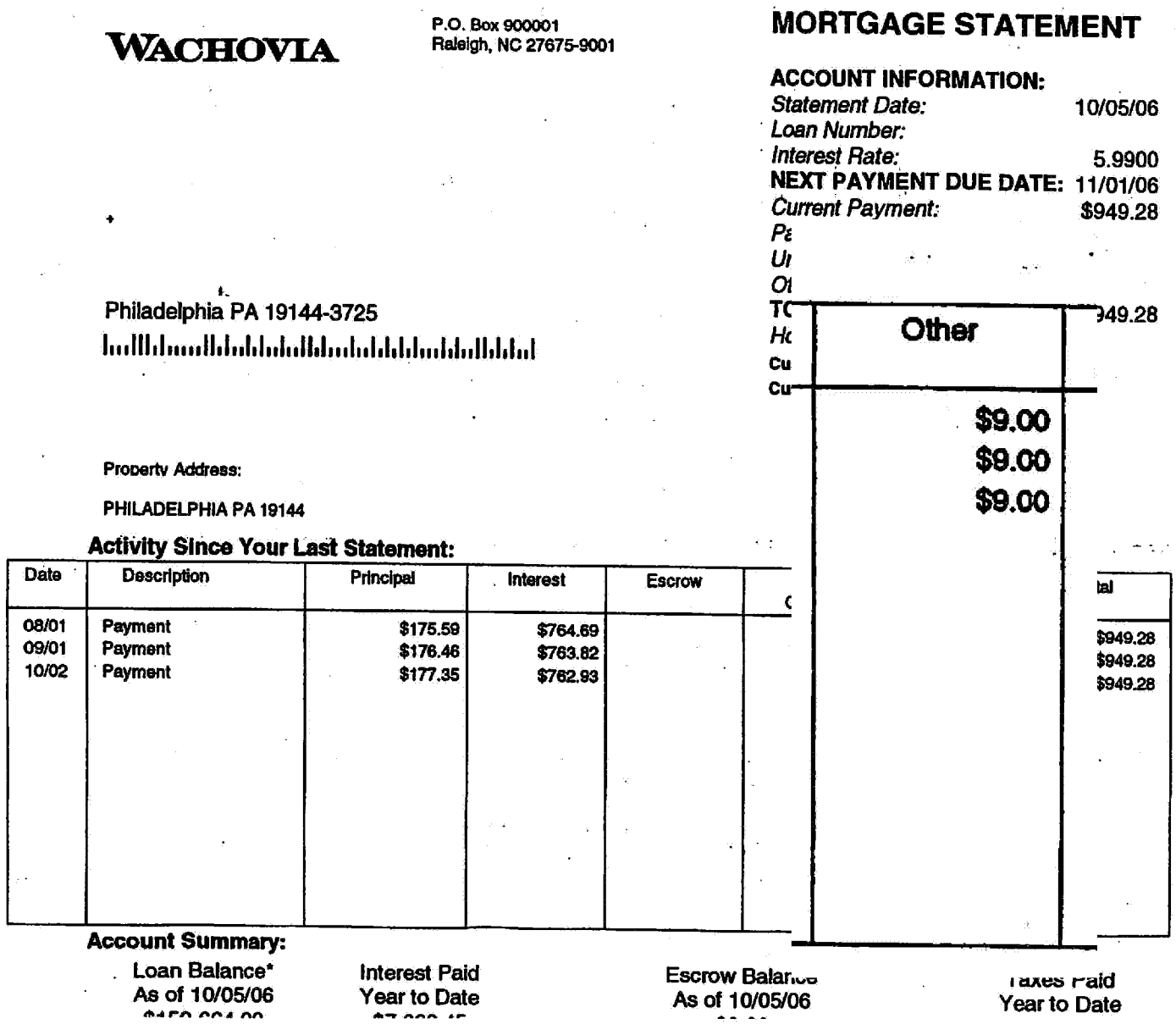
Date	Chk No.	Amount	Date	Chk No.	Amount	Date	Chk No.	Amount
10/01	2439	40.00	10/18	2462	438.50	10/18	2466	237.00
10/10	2463	13.86	10/19	2464	159.46	10/26	2470	9.95
10/24	2460*	10.00						

* Denotes Gap in Check Number Sequence

Other Transactions

Date	Description	Deposit(+) Withdrawal(-)
10/02	Ac-Us Treasury 303 -Soc Sec	565.00+
10/02	Ac-Us Treasury 303 -Soc Sec	1,194.00+
10/02	Ac-Car -Convcheck Ck-000000000002444	24.99-
10/02	Ac-Ppd -Convcheck Ck-000000000002446	27.99-
10/02	Ac-Pnd -Convcheck Ck-000000000002447	27.99-
10/02	Ac-App -Convcheck Ck-000000000002448	34.99-
10/03	Ac-Pm -Convcheck Ck-000000000002445	25.99-
10/05	Ac-Sdrd -Convcheck Ck-000000000002450	23.99-
10/05	Ac-Dcd Main Office -Convcheck Ck-000000000002449	24.99-
10/17	Ac-Ppa -Convcheck Ck-000000000002457	27.99-
10/17	Ac-Sbn -Convcheck Ck-000000000002458	39.99-
10/19	Ac-At&T Consumer -Checkpaymt Ck-00002461	77.46-
10/23	Ac-Rda -Convcheck Ck-000000000002467	31.99-
10/24	Ac-Adrd -Convcheck Ck-000000000002468	19.99-
10/24	Ac-Sr -Convcheck Ck-000000000002465	29.00-
10/25	Ac-Dpd Main Office -Convcheck Ck-000000000002469	31.99-
10/25	Ac-Reporting Data D-Convcheck Ck-000000000002471	24.99-

From Target Gift Card to Automated Electronic Mortgage Payment



WACHOVIA

P.O. Box 900001
Raleigh, NC 27675-9001

MORTGAGE STATEMENT

ACCOUNT INFORMATION:
Statement Date: 10/05/06
Loan Number:
Interest Rate: 5.9900
NEXT PAYMENT DUE DATE: 11/01/06
Current Payment: $949.28
Pa
Ur
Ot
TC 949.28
Hc
Cu
Cu

Philadelphia PA 19144-3725

Other

$9.00
$9.00
$9.00

Property Address:

PHILADELPHIA PA 19144

Activity Since Your Last Statement:

Date	Description	Principal	Interest	Escrow		tal
08/01	Payment	$175.59	$764.69			$949.28
09/01	Payment	$176.46	$763.82			$949.28
10/02	Payment	$177.35	$762.93			$949.28

Account Summary:

Loan Balance*
As of 10/05/06

Interest Paid
Year to Date

Escrow Balance
As of 10/05/06

Taxes Paid
Year to Date

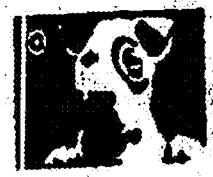
Incentives to Induce Authorization

HOMEQ SERVICING **$20.00 Target® GiftCard**

Expiration Date
01/26/2005

Exclusively For

PHILADELPHIA PA 19144 3725



Please sign and return this reply form with your mortgage payment to get your $20.00 Target GiftCard and to activate your Good Neighbor Privileges!

Add to my HomEq Servicing Corporation loan

for as long as I wish to

payment at all times. If I decide to

Good Fun call me, 800-280-8633, to cancel. I

Use this one last time, I may cancel at any

additional. By signing below I authorize HomEq to

number, name, address, and any other

benefits. Additionally I authorize Target to

X _____

SIGNATURE REQUIRED FOR PROCESSING

Sign and return this form to claim the $20.00 Target GiftCard reserved for you
THIS FORM IS NOT REDEEMABLE AT ANY TARGET LOCATION

Z07635 Z743476A0216[illegible]3 HCB 0303297089

Payment Processing Center, LLC

- Provides "end-to-end solutions" for telemarketing merchants

- Specializes in "Bank Draft origination for telephone **transactions that may be prohibited**" by NACHA rules

: lmeojhlihcbbcapbcmliiebhcaaa.justin@paymentprocessingcenter.com
= 0000000353
: 00000000D8B3FD5A785EC54E87ADC17FEBD9131424232100
: To the fine people that made hellish phone abuse a little more bearable,
Thank you for making my summer a little less tedious and a little more

, I am glad to have shared the daily death-threats, hate-filled rants, and ignorance with all of you. I think sometime in the next couple weeks I may almost (in some kind of sick way) miss the sound of shit-kickers screamed obsenities over the verification playback.

bacon-speckled tomato soup, dealt with a phonebook's worth of customer callbacks, and a lot of soggy bread from the sandwich club.
When you come into work on Monday don't be sad that my cute little ass isn't around, be happy... because finally one of us will get to know what daylight looks like during a weekday. Just remember my smiling face and boyish good

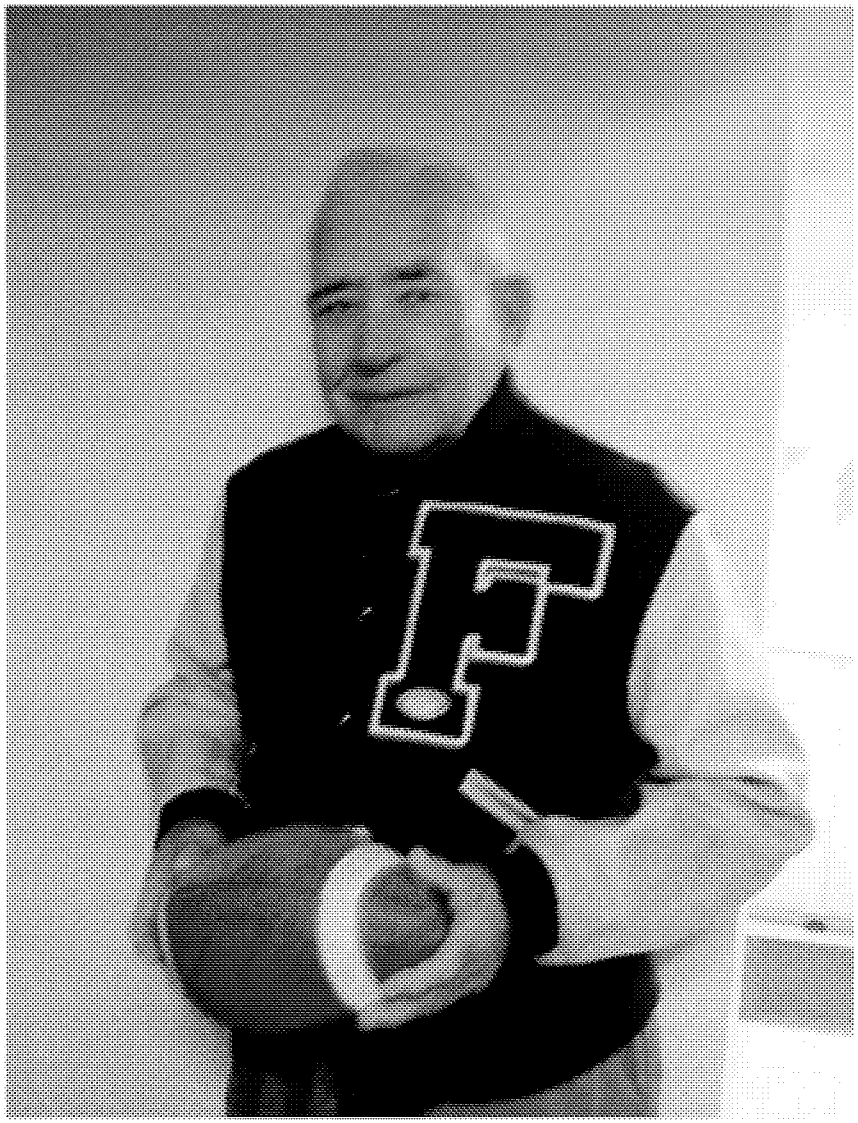
I know the customer service number and I'm not afraid to call with my bank rep on the line)

Now, as I hang up my Steno Pad and descend back in to a world of relative normality I would like to say THANK YOU to everyone.

Side note to Michael: How much exactly do I owe you for the knowledge that it takes a total of 16 combined brain cells and teeth to provide your bank account information to a stranger on the phone to order something with as stupid a name as Washballs? or; the knowledge that old people are just plain easy to trick?

stay in touch,
Justin

Purported Authorization Obtained By Telemarketer



David XXX, Sr.

1933-2006

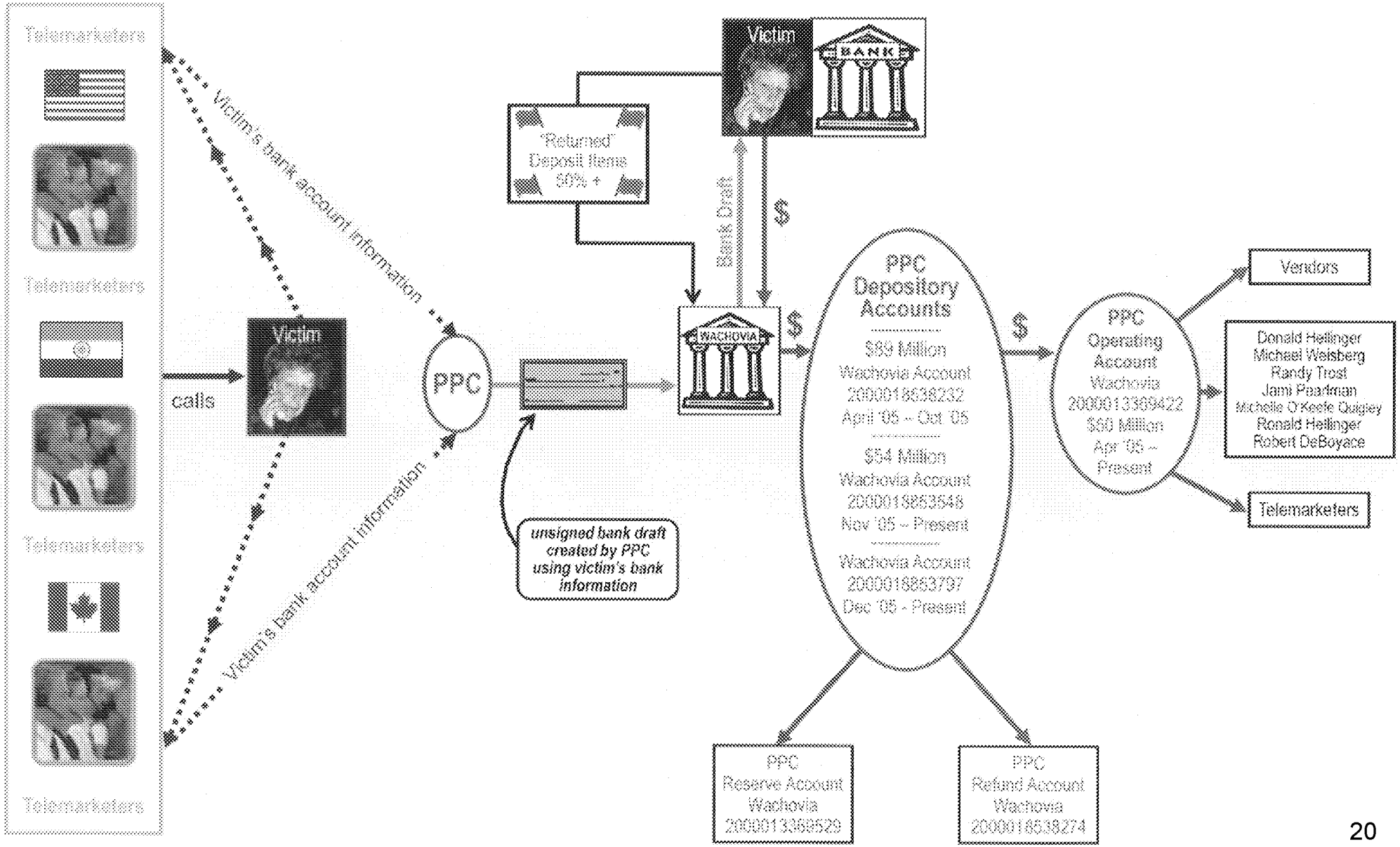
University Football Coach

Little League Coach

Sunday School Teacher

Husband, Father, Grandfather, Brother

The Payment Process

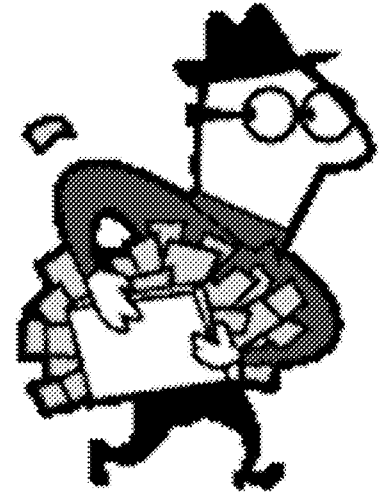


A Mutually Profitable Relationship!

Dollar value of RCCs deposited by PPC with Wachovia in 12-month period: **$162,000,000**

Income from RCC fees:

PPC – **approx. $8,000,000**
Bank – **approx. $1,900,000**



Wachovia: Victim or Participant?

- Knew or remained willfully blind to fact that PPC serviced mass market fraudsters
- Ignored glaring red flags
- Suppressed internal concerns
- Ignored express warnings from other banks
- Entered agreements with PPC to protect its own interests at the expense of the interests of other banks and their customers

Failure in Due Diligence
PPC's Telemarketing Merchants

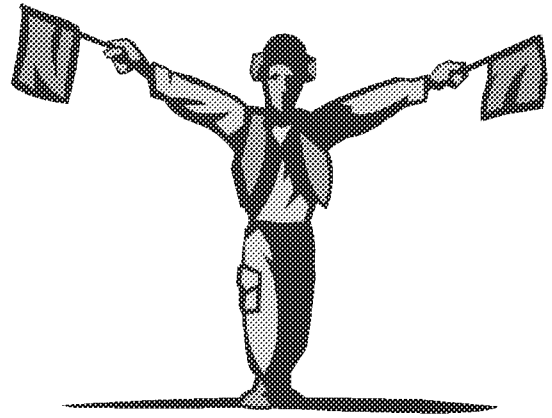
- Facially suspicious product offers and marketing scripts
  - Grant offers
  - Prescription discount cards
  - Travel Programs
  - Free Gift Cards
  - Free Computers
- Merchants mostly based overseas and/or using foreign banks
- Exploited names of legitimate companies, such as Wal-Mart, K-Mart, Home Depot, Carnival Cruises, AIG

Eyes Wide Shut

- PPC merchants were fraudsters well-known to Better Business Bureaus, state Attorneys General, and consumer protection websites
  - Star Communications
  - Advantage America
  - Suntasia
- As successive payment processers were shut down by law enforcement, Wachovia continued to process RCCs for same fraudulent merchants

Returns – Charge Backs

- At inception, Wachovia **anticipated returns exceeding 35 percent** (compared to approximately 1/2 of 1 percent for all checks)
- Actual returns exceeded **50 percent**
- Wachovia charged PPC substantial fee for returns
- Wachovia offered PPC volume discounts on return fees



Return Reasons

- More than 50 percent of PPC's returns facially identified as:
  - UNAUTHORIZED
  - FRAUD
  - REFER TO MAKER

- Every month Wachovia received and hand-processed thousands of **sworn affidavits from consumers alleging that PPC debit transactions were not authorized**

Banknorth, N.A.

AFFIDAVIT OF UNAUTHORIZED CONSUMER DRAFT

(Type or Print Neatly)

Bank: Banknorth Massachusetts
Banking Center: SW Commons/39
RC: 3390
Telephone #: (508) 754 - 6745

Use this form for drafts with the following tran codes only:
184 POD Check
187 Check

[redacted] Customer's Name
[redacted] Account Number
[redacted] Street
Apt. #
P.O. Box
Worcester City MA State 01604 Zip
[redacted] Daytime Telephone
Home Telephone

I declare, swearing under oath, that a draft charged to my account and appearing on my account statement is UNAUTHORIZED.

Check appropriate Section I OR Section II:

I. Draft Never Authorized:

☒ I have never authorized the company named above to debit my account

☐ I authorized the company named above to debit my account, but I revoked ** the authorization on _____ in the manner specified in said authorization.
Date of Revocation

** Customer must provide Bank with a copy of the written revocation

I further declare that the above transaction was not initiated by me or by any person acting on my behalf. In signing this form, I understand that the Bank will reverse any credit(s) to my account if it receives proof from the payee of the draft that I, in fact, authorized this draft.

[redacted] 5-17-05 [signature]
Customer Signature (required) Date Banking Center Representative

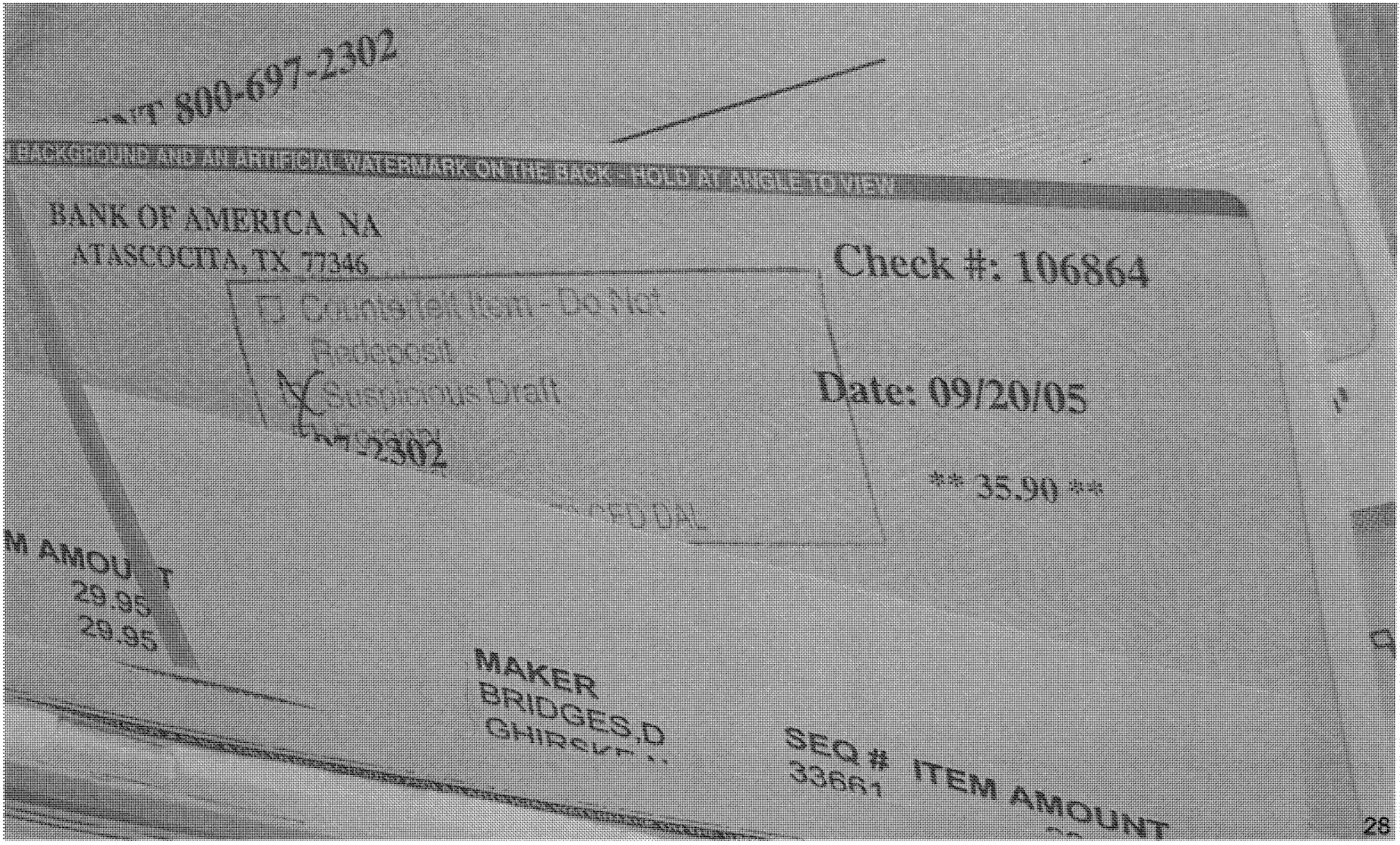
FOR USE ON PERSONAL ACCOUNTS ONLY

Instructions:

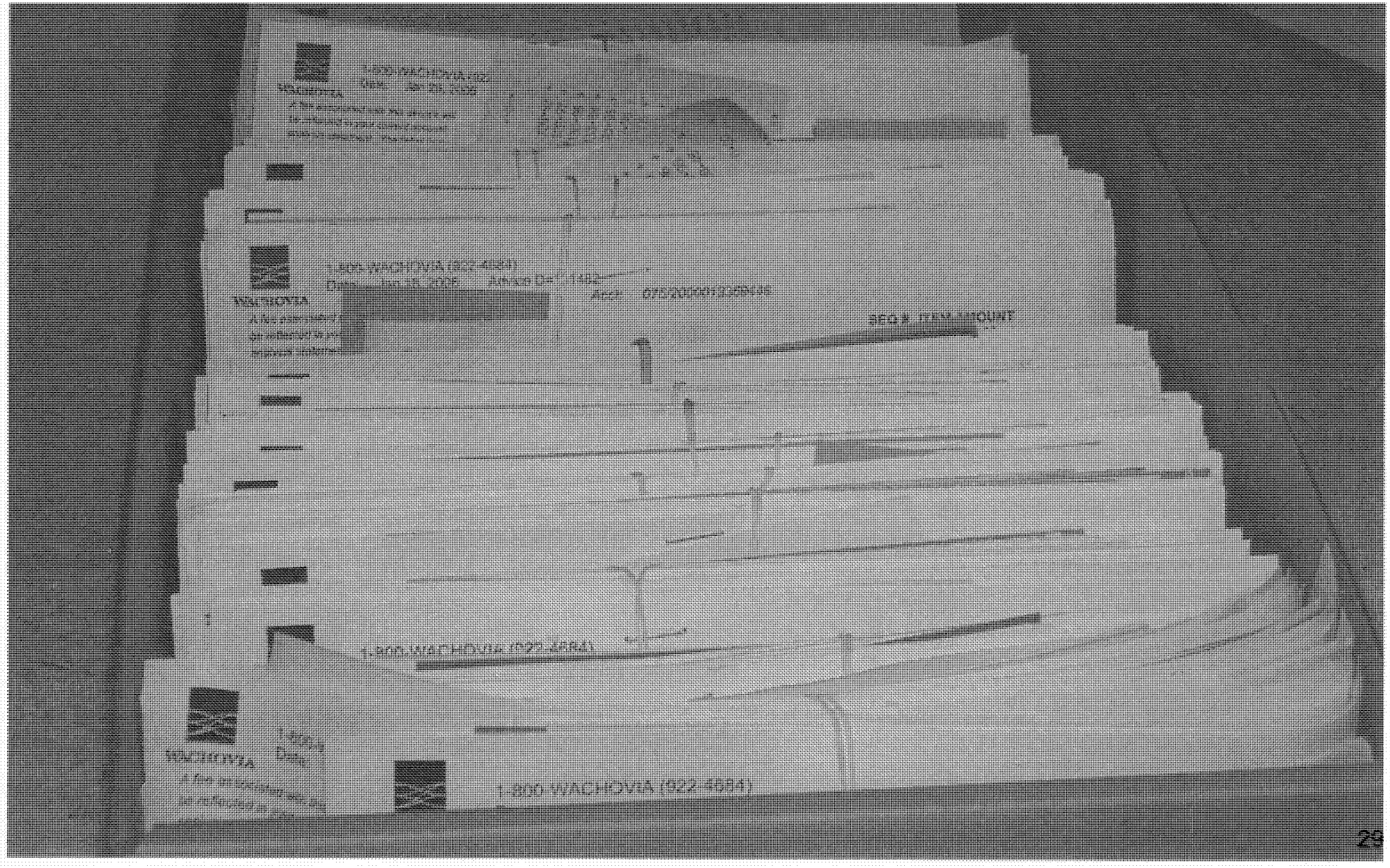
1. Fax to Adjustment Department 207-755-6315 OR Send a copy of the returned item (if available) and the signed affidavit through interoffice mail to: *Adjustment Department ME091-31*
2. Place a stop payment for the amount of the draft on the customer's account to prevent any future drafts from processing to the account. Have customer sign Stop Payment Order and remit form as usual.
3. Advise customer that provisional credit will NOT be granted on this transaction. Customer account will only be credited upon Bank receiving credit back from draft originator.

Affidavit of Unauthorized Consumer Draft Rev. 03/2004

A Returned Item



A Box of Returned Items

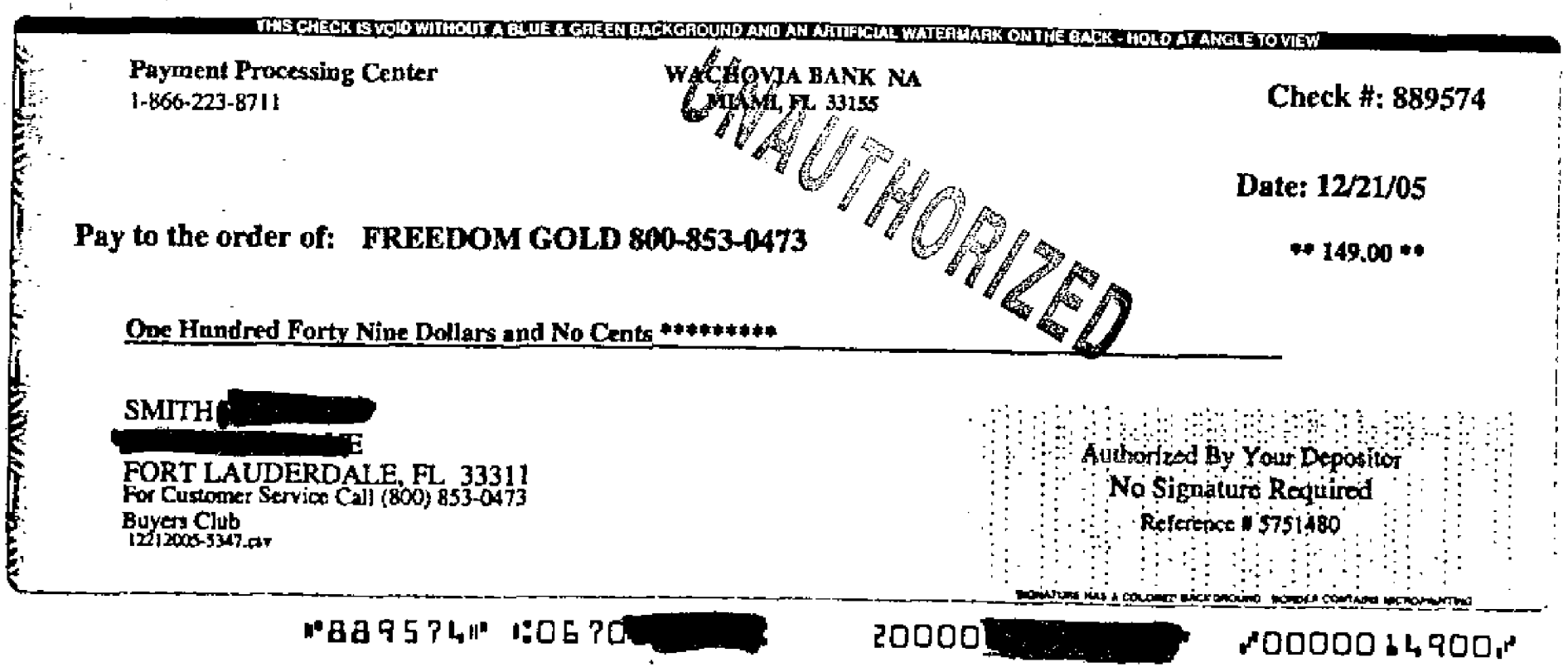


A Room of Boxes of Returned Items

Outlier Business Practices

- PPC regularly transferred large amounts of money to overseas accounts.
- Wachovia allowed PPC to deposit RCCs payable to third-party merchants into its own accounts – without agency agreements.
- The Wachovia/PPC business model was based on large volumes of returns – an ordinarily suspect and undesired result.
- Wachovia's own customers often treated differently than other banks' customers.

"On the House" Returns



THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK - HOLD AT ANGLE TO VIEW

Payment Processing Center
1-866-223-8711

WACHOVIA BANK NA
MIAMI, FL 33155

UNAUTHORIZED

Check #: 889574

Date: 12/21/05

Pay to the order of: FREEDOM GOLD 800-853-0473

** 149.00 **

One Hundred Forty Nine Dollars and No Cents *********

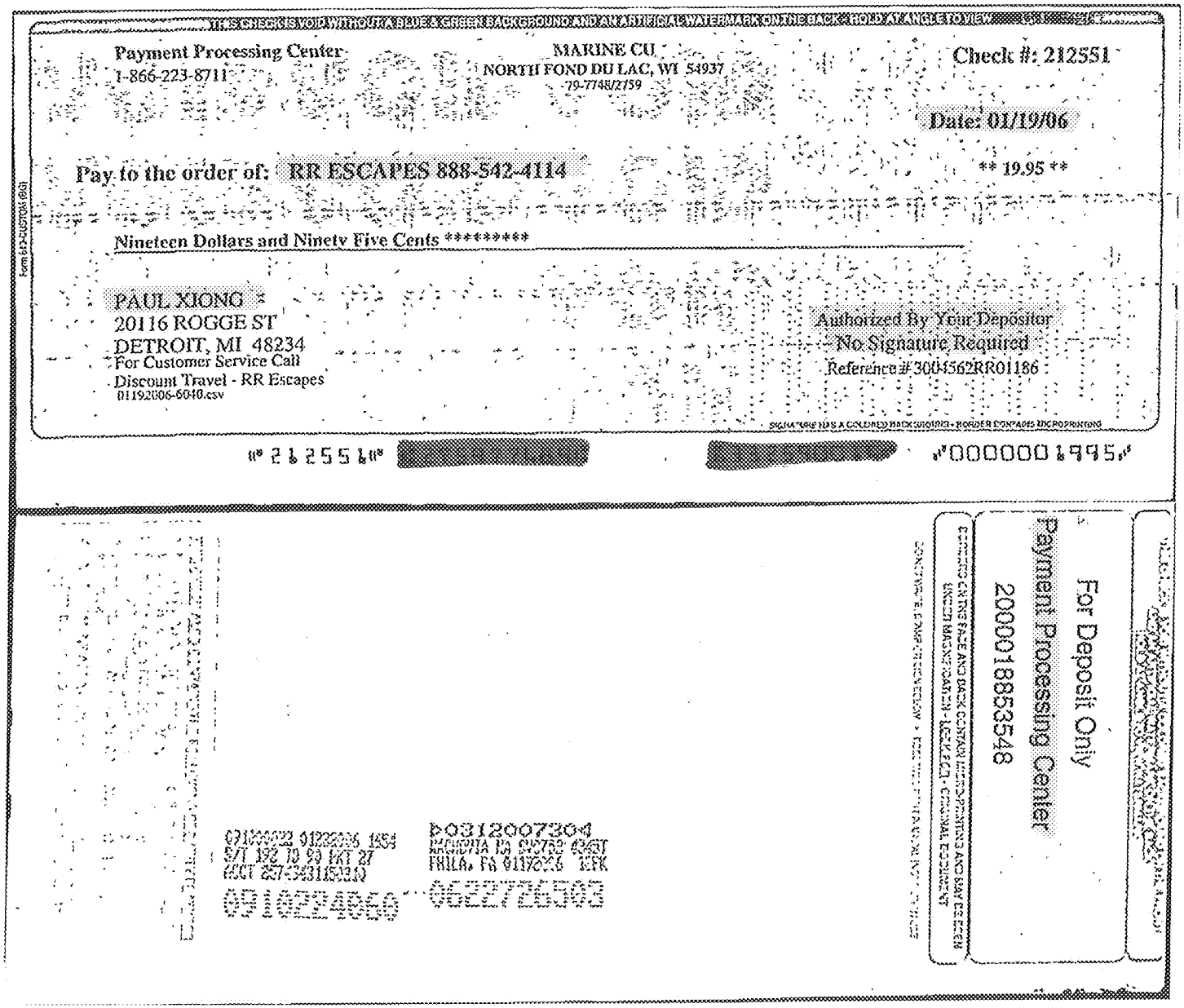
SMITH [redacted]
[redacted]
FORT LAUDERDALE, FL 33311
For Customer Service Call (800) 853-0473
Buyers Club
12212005-5347.csv

Authorized By Your Depositor
No Signature Required
Reference # 5751480

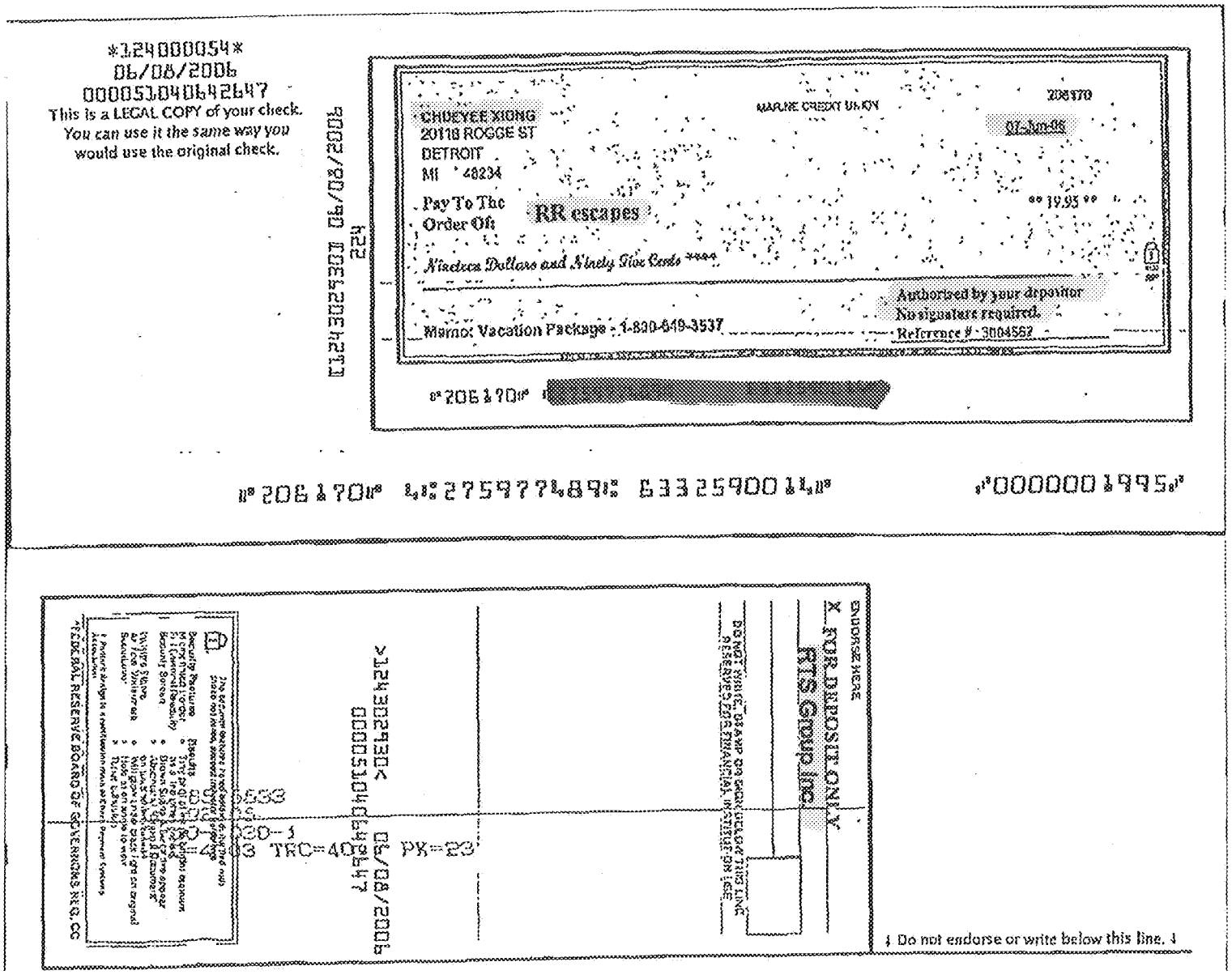
SIGNATURE HAS A COLORED BACKGROUND BORDER CONTAINS MICROPRINTING

⑈889574⑈ ⑆0670[redacted] 20000[redacted] ⑈000001 4900⑈

"Whack-a-Mole"


Payment Processing Center
1-866-223-8711
MARINE CU
NORTH FOND DU LAC, WI 54937
Check #: 212551
Date: 01/19/06
Pay to the order of: RR ESCAPES 888-542-4114
** 19.95 **
Nineteen Dollars and Ninety Five Cents **********
PAUL XIONG
20116 ROGGE ST
DETROIT, MI 48234
For Customer Service Call
Discount Travel - RR Escapes
01192006-6040.csv
Authorized By Your Depositor
No Signature Required
Reference#3004562RR01186
"212551"
"0000001995"
For Deposit Only
Payment Processing Center
200001885348

Migration from National Bank to Community Bank



Wachovia Ignored Internal Concerns

Return "volumes are tremendous" and "payment of these items is not our normal process"

Returns Operations Supervisor to VP of Loss Management

"Nothing [PPC] could ever do would make me comfortable . . ."

Bank Loss Management Official after learning about Bank relationship with PPC

After Loss Management official recommended closing PPC accounts, wrote "business line has assumed risk for the customer and decided to keep their accounts open"

Communication between Bank Loss Management Officials

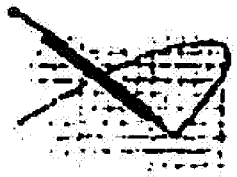
Wachovia Ignored Internal Concerns

"Please consider the regulatory and reputational risks involved here. **We have now been put on notice that accounts at [Bank] are being used . . . to further these schemes.**

"If PPC has in place 'a standing agreement with [Bank] to pay all claims without dispute,' then they know they have rogue telemarketers in their customer base."

Internal E-mail from Bank's In-house Counsel after receiving fraud warning from another bank

DOUBLE YIKES!!!!



08/23/2005 06:35 PM

To

cc

Subject Guardian Marketing # 2000027007068

Tom,
Bob, Tim & I need to huddle with you on this account relationship. It is a Business Banking account, it has been actively making deposits since 6/23/05 and there is a current balance of $743,000+ in the account. The account came to us from B of A (so we are advised by ; n Bus. Bnkg.) and she is

ALL their deposits are THIRD PARTY DRAFTS!!! DOUBLE YIKES!!!!

YIKES!!!! Moreover, the drafts that are being deposited and are charging back, are not $99.99; these items are all over the place in terms of their amount. Moreover, there is another account, Suntasia, #2000027027721. Same address, same principals. $ from the Guardian acct is transferred to Suntasia and then the $ is wired out to Bank of America (funny, I thought I said they were leaving B of A at the beginning of this note, didn't I??). And, there is more, but nothing more that I want to put into a note. Bob and I really need to talk o you on tomorrow,

Thanks,

Wachovia Ignored Explicit Fraud Warnings From Other Banks

"The purpose of this message is to **put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam . . .** instigate an investigation into whether [PPC is] conducting legitimate business and whether [Bank is] getting **a high volume of return items on those accounts (that should place your bank on notice of potential fraud).**"

E-Mail from Citizens Bank

Bank's "Oral Agreement" With PPC To Pay All Returns

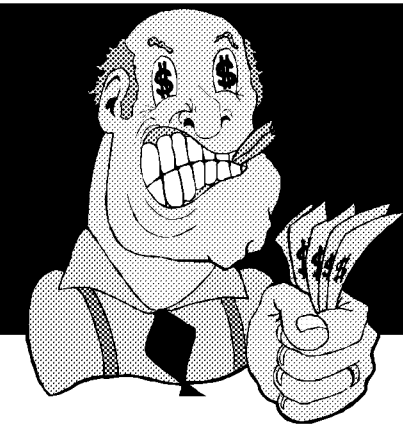
- Intended to protect Bank's reputation rather than consumers

"[I]f we can find a way to pay the returns . . . without sending them back to other banks, I think that will go a long way to preserve our reputation. **The sooner the complaint gets paid the quicker it goes away."**

Internal Bank e-mail

- Demonstrates that UCC warranty rule is not an effective anti-fraud tool

Money Motivates



"[P]lease mark your calendar – we will take them somewhere nice for lunch. We are making a ton of money from them."

Bank Relationship Manager to Senior Business Development Officer

"[T]his is our most profitable account. $1mm per year in profit. They have asked for Eagle tickets. What can we do?? They deserve them with all we make from them."

Bank Relationship Manager to Senior Business Development Officer

What's a reputation worth?

CNNMoney.com News | Markets | Technology | Personal Finance | Small Business | CNN.com

FORTUNE

Yikes: Wachovia and the telemarketers

...have taken corporate spin to a new low with its ... to a lawsuit against the big bank show... ...marketing scams. Docum... ...Times rep...

April 25, 2008

Wachovia to Pay as Much as $144 Million ... arketing Case

By CHAR...

...tory. The Times ...mpanies it knew ...her banks and ...g services ...erly. ...reports.

...e banking giant, has agreed to pay as ... investigation accusing the bank of ...ccounts to steal millions of dollars

Business Day

The New York Times

Papers Show Wachovia Knew of Thefts

By CHARLES DUHIGG

Last spring, **Wachovia** bank was accused in a lawsuit of allowing fraudulent telemarketers to use the bank's accounts to steal millions of dollars from unsuspecting victims. When asked about the suit, bank executives said they had been unaware of the thefts.

But newly released documents from that lawsuit now show that Wachovia had long known about allegations of fraud and that the bank, in fact, solicited business from companies it knew had been accused of telemarketing crimes.

"YIKES!!!!"

"DOUBLE YIKES!!!!"

"There is more but nothing more that I want to put into a note."

Yes – it *is* a crime.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 10-20165 CR - LENARD
31 U.S.C. § 5318(h)
31 U.S.C. § 5322(a)

MAGISTRATE JUDGE
BRANNON

UNITED STATES OF AMERICA

v.

WACHOVIA BANK, N.A.,

Defendant.

FILED by D.C.
MAR 12 2010
STEVEN M. LARIMORE
CLERK U. S. DIST. CT.
S. D. of FLA. – MIAMI

INFORMATION

The United States Attorney charges that:

GENERAL ALLEGATIONS

At all times material to this Information

1. Defendant **WACHOVIA BANK, N.A.** was a national banking association based in Charlotte, North Carolina.

It's not over until it's over.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	CRIMINAL NO. 11-
	:	DATE FILED: February 10, 2011
v.		
	:	VIOLATIONS:
DONALD HELLINGER		18 U.S.C. § 371 (conspiracy – 1 count)
RONALD HELLINGER	:	18 U.S.C. § 1960 (operating an illegal money
MICHAEL WEISBERG		transmission business – 1 count)
RANDY TROST	:	18 U.S.C. § 1955 (operating an illegal gambling
JAMI PEARLMAN		business – 1 count)
MICHELE QUIGLEY	:	18 U.S.C. § 1084 (transmission of wagers and
		wagering information – 8 counts)
	:	18 U.S.C. § 1956(a)(2)(A) (international money
		laundering – 3 counts)
	:	Notice of forfeiture

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES THAT:

At all times relevant to this indictment:

BACKGROUND

1. Defendants DONALD HELLINGER, RONALD HELLINGER, MICHAEL WEISBERG, RANDY TROST, JAMI PEARLMAN, and MICHELE QUIGLEY

Financial accountability -- thanks to federal agents, prosecutors, and bank regulators, class action attorneys, local and state law enforcement, *The New York Times*, and many determined victims of consumer fraud !

A simple proposition.

Mass-market scammers need access to payment systems (RCC's, ACH, CC) to take consumers' money. Without bank access there are no unauthorized withdrawals.

Banks are stationary (no "whack-a-mole"), regulated, and are concerned about reputational risk.

Banks already are required to have systems in place to prevent criminals from accessing the banking system.

Cutting off the scammers' access to the payment systems is relatively efficient and fast, and protects consumers prospectively as we investigate.

Important steps forward . . .

- Guidance to banks from FDIC, OCC and FinCEN
- United States v. First Bank of Delaware
- Financial Fraud Enforcement Task Force/Consumer Protection Branch efforts to choke-off fraudsters' access to payment systems (DOJ, FTC, FDIC-OIG, USPIS, FBI, and others)
- May 21, 2013: FTC Notice of Proposed Rulemaking would ban the use of RCCs in connection with telemarketing

Operation Choke Point
So far . . .

- More than 50 subpoenas issued to banks and TPPPs.
- Several active criminal and civil investigations.
- Banks are self-disclosing problematic TPPP relationships.
- Banks are terminating TPPP relationships and scrutinizing scammer relationships.
- Internet Payday lending – collateral benefits.
- Investigative support from USPIS, FBI, SIGTARP, USSS

Regulatory Loophole

- Treasury Department regulation amended in 2011 arguably excludes third-party payment processors from the definition of "money transmitter" and thus is not a Money Services Business ("MSB").

- **A payment processor that originates tens of millions of dollars of debit transactions against consumers' bank accounts on behalf of Internet and telemarketing merchants may not be an MSB and may not be required to register with FinCEN or comply with the BSA.**

Thanks for your time and interest!

Questions?

Joel M. Sweet

[redacted]@usdoj.gov

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Tuesday, August 06, 2013 11:30 AM
To: Blume, Michael S.; Olin, Jonathan F. (CIV); Price, Allison W (OPA); Mansour, Linda
Cc: Sweet, Joel; Goldberg, Richard
Subject: RE: WSJ/online payday

Thanks, Mike. Allison/Linda: you will recall that Mike and Mike [redacted] buzz in the industry and with our partner agencies, and seems to be helping.

From: Blume, Michael S.
Sent: Tuesday, August 06, 2013 11:24 AM
To: Frimpong, Maame Ewusi-Mensah (CIV); Olin, Jonathan F. (CIV); Price, Allison W (OPA); Mansour, Linda
Cc: Sweet, Joel; Goldberg, Richard
Subject: FW: WSJ/online payday

Maame/Jon/Allison/Linda

See below. I will direct him to Allison to start. This is connected to our third party payment processing initiative, in which we have been starting to pay closer attention to banks and processors who deal with payday lenders. My view is that getting the message out that DOJ is interested in on-line payday lenders and the potential abuses is important.

Mike

From: Zibel, Alan [mailto[redacted]@wsj.com]
Sent: Tuesday, August 06, 2013 10:21 AM
To: Blume, Michael S.
Subject: WSJ/online payday

Mr. Blume:
I'm a reporter with the Wall Street Journal in DC. I've been told by a few sources that the DOJ is conducting a probe of online/tribal payday lending and has issued subpoenas to numerous companies in this field. Wondering if you could talk to me on background re-this issue.
Many thanks, Alan

Alan Zibel - Reporter
THE WALL STREET JOURNAL
1025 Connecticut Avenue NW, Suite 800
[redacted]

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Tuesday, August 06, 2013 2:36 PM
To: Toulou, Tracy (OTJ)
Cc: Blume, Michael S.; [redacted]
Subject: WSJ/CNN interview on online pay day lending

Hi Tracy -

We wanted to give you a heads up that Mike is doing a background interview this afternoon at 4pm on online pay day lending. As we described for you at last week's meeting, we are engaged in a third-party payment processor initiative in which we are looking into banks that deal with processors who work for payday lenders of all types. We think that the reporter is interested in tribal online payday lending, but we plan not to focus on tribal payday lending, but online payday lending in general.

Note that we also received a press inquiry from CNN about online tribal gaming, and indicating that the reporter thinks this is something the Consumer Protection Branch is investigating. We are not looking at online gaming at all. We plan to decline the interview if CNN is indeed interested in gaming; let us know if there is someone else to refer that inquiry to. We think it is possible that something got lost in translation, and CNN is indeed interested in payday lending, not gaming. If so, we will follow the same approach as described above with WSJ/CNN.

Thank you!

Regards,
Maame

From: Sweet, Joel
Sent: Thursday, August 08, 2013 1:21 PM
To: Toulou, Tracy (OTJ)
Cc: Blume, Michael S.; Frimpong, Maame Ewusi-Mensah (CIV)
Subject: FW: WSJ: Probe Turns Up Heat on Banks, Prosecutors Target Firms That Process Payments for Online Payday Lenders, Others

Tracy –

Wanted to make sure you saw this article. We had emphasized to the reporter that we are not focusing on payday lending, much less tribal involvement in payday lending. Our focus is far broader and is aimed at processors and banks that are complicit in consumer abuse. Please call if you want to discuss. We've been trying to get in touch with you for the past few days concerning requests for meetings we've received in recent days from lawyers representing tribal interests.

Best,

Joel

From: Price, Allison W (OPA)
Sent: Thursday, August 08, 2013 9:22 AM
To: Sweet, Joel; Blume, Michael S.
Cc: Olin, Jonathan F. (CIV); Jenkins, Adora (OPA)
Subject: WSJ: Probe Turns Up Heat on Banks, Prosecutors Target Firms That Process Payments for Online Payday Lenders, Others

A version of this article appeared August 8, 2013, on page A1 in the U.S. edition of The Wall Street Journal, with the headline: Probe Turns Up Heat on Banks.

Updated August 7, 2013, 10:27 p.m. ET

Probe Turns Up Heat on Banks

Prosecutors Target Firms That Process Payments for Online Payday Lenders, Others

By ALAN ZIBEL and BRENT KENDALL

WASHINGTON—The Justice Department is targeting banks that service a broad range of what it considers questionable financial ventures, including online payday lenders.

The government has issued subpoenas to banks and other companies that handle payments for an array of financial offerings, ramping up an investigation that has been under way for several months, according to Justice Department officials and other people familiar with the matter.

It's a shift in strategy: Rather than just targeting individual firms, the government is now going after the infrastructure that enables companies to withdraw money from people's bank accounts.

The volume of online payday lending—a term for smaller, short-term loans at high interest rates—grew to $18.6 billion in 2012, up 10% from the previous year, accounting for nearly 40% of industrywide payday-loan volume, according to investment bank Stephens Inc.

Regulators are also trying tamp down phone and online offers in which marketers try to get people to pay for services that they don't intend to deliver. These can include offerings to erase debt or offerings of work-from-home programs that don't lead to jobs, officials say.

"We are changing the structures within the financial system that allow all kinds of fraudulent merchants to operate," a Justice Department official said, with the intent of "choking them off from the very air they need to survive."

The move is sparking complaints among online lenders who say the government is attempting to kill a legitimate and fast-growing industry that millions of low-income people rely on to cope with financial emergencies.

Government pressure that forces banks to stop processing payments "would cut off an important credit choice for millions of underserved consumers," said Peter Barden, spokesman for the Online Lenders Alliance. "It should also send a troubling message to banks that at any point regulators can force them to stop processing legal transactions simply because they don't like a particular merchant or industry."

Electronic payment systems handled tens of trillions in transactions last year ranging from food stamps to utility bills to payrolls. Third-party payment firms help merchants and lenders process transactions through banks. Several government agencies have publicly expressed concern about suspicious activities, including fraudulent transactions and money laundering. Banks and payment processors generally collect a fee for each transaction.

The industry-run group overseeing electronic transactions, NACHA, says it has made clear that banks are responsible for ensuring the validity of all transactions on the system. "We welcome combined efforts to identify and address the worst abusers" of electronic payments and will cooperate with law enforcement and regulators, a spokeswoman said.

The Federal Deposit Insurance Corp. has begun warning banks to stop processing payments on behalf of online short-term lenders, including those connected to Indian tribes aiming to operate outside state regulation, according to people familiar with the matter. Some online lenders offer short-term loans with annual interest rates of more than 700%.

The Office of the Comptroller of the Currency has told the banks it regulates to review their business relationships with short-term lenders, out of concern that enabling automatic deductions from customers' accounts could harm a bank's reputation.

The FDIC is working to make sure banks are "effectively managing relationships with payment processors and higher-risk merchants, such as payday lenders," said FDIC spokesman Andrew Gray.

Thirty-five states allow payday lending, while 15 others and the District of Columbia effectively ban such loans, mainly through interest-rate caps. But numerous Indian tribes have begun making loans over the Internet and argue they are sovereign states not subject to state-level regulation. Other

lenders assert they don't have to comply with state laws if they set up shop offshore or in states with favorable regulations such as Delaware and Utah.

Earlier this week, Benjamin Lawsky, superintendent of the New York Department of Financial Services, sent 35 online and tribal lenders cease-and-desist orders telling them to stop offering "illegal payday loans that trap families in destructive cycles of debt." He also urged more than 100 banks to "choke off" access to payday loans.

Officials said banks have begun voluntarily self-disclosing wrongdoing to the Justice Department and cutting off access to payment processors they consider questionable. Several banks that had been working on payment-processing deals with Indian tribes have since backed out, according to a person familiar with the matter.

Justice Department officials said they are examining payment processors and banks of various sizes and are working closely with the Federal Trade Commission, which has been targeting alleged scammers and online lenders that engage in deception.

Banks say they are taking steps to curb abuses. J.P. Morgan Chase & Co reports unauthorized electronic transactions to NACHA, a spokeswoman said, and the bank earlier this year decided to charge one fee a month instead of multiple charges if a company such as a payday lender makes repeated attempts to deduct funds from a customer's account with insufficient funds.

The bank is circulating a proposed rule change for the electronic-payments network that would fine banks with an excessive number of returned payments. A high volume of returned payments can be a sign that a company is engaged in fraudulent activity or other illicit behavior, payment-industry experts say.

The Justice Department's move is an outgrowth of a financial-fraud task force established by President Barack Obama in the wake of the 2008 financial crisis.

In a preview of the type of case the government may bring, the Justice Department last November filed civil charges against First Bank of Delaware, alleging it knowingly processed fraudulent financial transactions. The bank, which dissolved last year after being stripped of its state charter, agreed to settle the case, denying liability and paying a $15 million penalty and another $500,000 in restitution for consumers.

A key focus, officials said, is whether the banks or processors violated a 1989 law—passed in the wake of the U.S. savings-and-loan crisis—that allows the U.S. to recover civil penalties for fraud and other violations.

—Andrew R. Johnson contributed to this article.

Write to Alan Zibel [redacted] and Brent Kendall at [redacted]@dowjones.com

From: Delery, Stuart F. (CIV)
Sent: Thursday, August 08, 2013 4:37 PM
To: Olin, Jonathan F. (CIV); Frimpong, Maame Ewusi-Mensah (CIV)
Subject: Re: press

Yes I agree.

From: Olin, Jonathan F. (CIV)
Sent: Thursday, August 08, 2013 02:58 PM
To: Frimpong, Maame Ewusi-Mensah (CIV); Delery, Stuart F. (CIV)
Subject: RE: press

I think that's a good idea.

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Thursday, August 08, 2013 2:55 PM
To: Delery, Stuart F. (CIV); Olin, Jonathan F. (CIV)
Subject: press

Hi –

FYI that Mike, et al, are doing a call with Bloomberg about 3PPP. I wanted to raise again the question of whether this might be a good time to do a briefing for leadership on the initiative. If it makes sense, perhaps we could work on scheduling something for when you (Stuart) return from vacation?

Regards,
Maame

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Thursday, August 08, 2013 4:40 PM
To: Blume, Michael S. [redacted]CIV.USDOJ.GOV)
Subject: 3PPP

I suggested to Stuart a while ago (I think after your NYT piece) that we organize a briefing on 3PPP for leadership. I raised it again with Stuart and Jon, and they think it is a good idea. We will shoot for end of August or beginning of September. I think this is a great way to place the Branch and our work in a positive light. Let's chat about the format when you have some time. Thanks!

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Friday, August 09, 2013 12:35 PM
To: West, Tony (OAAG)
Subject: RE: Really very proud

OK. We will keep you posted!

-----Original Message-----
From: West, Tony (OAAG)
Sent: Friday, August 09, 2013 12:28 PM
To: Frimpong, Maame Ewusi-Mensah (CIV)
Subject: RE: Really very proud

Think a briefing is a very good idea.

-----Original Message-----
From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Friday, August 09, 2013 10:59 AM
To: West, Tony (OAAG)
Subject: RE: Really very proud

Thank you, Tony! That means so much. The credit really should go to Mike, Rich, Joel and the third-party payment processor team and to you for your leadership and vision! Thank you for believing in me.

BTW - we would like to do a briefing for leadership on the third-party payment processor initiative (affectionately known as "3PPP"). We will probably shoot for the end of the month when everyone is back. We thought it made sense to sit down and explain what we have been doing and some of the great results we have been getting.

-----Original Message-----
From: West, Tony (OAAG)
Sent: Thursday, August 08, 2013 5:49 PM
To: Frimpong, Maame Ewusi-Mensah (CIV)
Subject: Really very proud

of you--great WSJ article on CPB. Well-deserved; you've really done a phenomenal job leading the branch and realizing the vision we all had a few years ago.

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Thursday, August 15, 2013 11:12 PM
To: Sweet, Joel
Cc: Blume, Michael S.
Subject: Re: NAFSA letter to banks

Good to know. Thank you for moving the ball forward on this in a productive way.

From: Sweet, Joel
Sent: Thursday, August 15, 2013 06:03 PM
To: Frimpong, Maame Ewusi-Mensah (CIV)
Cc: Blume, Michael S.
Subject: RE: NAFSA letter to banks

Maame –

I received a call this afternoon from [redacted] He recently was retained to represent NAFSA. I explained to him that NAFSA representatives will be meeting soon with DOJ. [redacted] was aware there would be a meeting organized by Rosette with individual tribal representatives – but [redacted] did not know there would be NAFSA representatives at the meeting. He will discuss with his client whether he also should attend.

[redacted] believes that his client's goal is to find a way to conduct Internet payday lending lawfully. I explained that our investigations are directed at banks and processors, that they are case-by-case and fact specific, that we are not focusing our attention only on the Internet payday lending industry, and that we certainly are not focusing on tribal IPDL. I also explained some of the problems we are seeing across the IPDL industry as a whole, such as fraudulent design, material omissions, and Rule E violations (prohibition against pre-authorized electronic debits as a condition of a loan).

I suggested to [redacted] that banks are becoming more sensitive about the risk of TPPP relationships and high risk merchants, and that rather than criticize DOJ's efforts to protect consumers from fraud, NAFSA perhaps should direct its efforts at convincing banks that tribal IPLD is lawful and not high risk.

[redacted]

[redacted] expressed appreciation for the phone call and said he would get back to us.

JMS

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Thursday, August 15, 2013 3:21 PM
To: Toulou, Tracy (OTJ); [redacted]; Blume, Michael S.; Sorgente, Natalia (CIV); Sweet, Joel; [redacted]

[redacted]
Subject: NAFSA letter to banks

Hi all –

I came across this in preparing for next week's meeting: a letter from NAFSA to the banks. I imagine that some of what is in the NAFSA letter will be raised in our meeting as well.

http://www.sacbee.com/2013/08/14/5649790/nafsa-to-banks-being-intimidated.html

Regards,
Maame

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

NAFSA NATIVE AMERICAN FINANCIAL SERVICES ASSOCIATION
www.nafsa.org

August 21, 2013

VIA EMAIL and U.S. MAIL
Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Consumer Protection Branch
Department of Justice
Civil Division
950 Pennsylvania Avenue, NW
Washington, DC 20530

RE: Follow up on meeting with tribal leadership regarding tribal government short-term lending on August 21, 2013

Dear Deputy Assistant Attorney General Frimpong:

I am writing to memorialize the meeting between our tribal membership and you and your colleagues today. We appreciate your willingness to accept our invitation for a meeting to begin a productive dialogue with tribal leadership and to strengthen the government-to-government relationship between tribal governments and the Department of Justice. In recent history, there is a proud tradition of consultation between our governments that was memorialized by Executive Order during the Clinton Administration. Both the George W. Bush and Obama Administrations have continued this legacy of cooperation and respect for the sovereign rights of American Indian tribal governments. President Obama confirmed this commitment on November 5, 2009 by reaffirming Executive Order 13175, requiring all heads of departments and executive agencies to consult with American Indian tribal governments before taking any action which may affect the sovereign rights of an Indian Tribe. The recent Executive Order, dated June 26, 2013, establishing the White House Council on Native American Affairs, specifically acknowledges, "that self-determination--the ability of tribal governments to determine how to build and sustain their own communities-- is necessary for successful and prospering communities."

As we shared with you in today's meeting, our tribal government short-term lending businesses have been severely harmed, and in some cases closed, by recent actions by the Department of Justice's Financial Fraud Task Force. For many of our tribes, these businesses are the primary source of governmental revenues to provide critical services to our communities, such as housing, education, and health care.

We were pleased to hear from you today that your actions are not directed at our tribal government short-term lending businesses. In particular, it was a relief to hear Deputy Assistant Attorney General Frimpong make the statement that, "It didn't occur to me that we should consult with tribes in advance because we are going after fraud. Never have we focused on tribal payday or payday. We go after financial fraud, so we are not going after you." Furthermore, and most importantly, you confirmed to us that, "banks may be mis-construing what they are hearing, that there is perceived risk to them, but that is not true." We were also encouraged to hear that the media reports have been incorrect with regard to DOJ efforts when Joel Sweet assured us that, "the context was us telling the reporter that we were not focusing on tribal or online lending."

We look forward to continuing our dialogue and appreciate the offer to include us in the new Consumer Protection Working Group since tribal governments share your dedication to protecting consumers by offering responsible financial services products and services.

Thank you for again your clear reassurance on these important issues.

If you have any questions, please feel free to contact me directly at JShotton@omdevelopment.org or by phone at (405) 880-5940.

Sincerely on behalf of all the tribes in attendance,

John Shotton
Chairman, Otoe-Missouria Tribe
Chairman, NAFSA

Sherry Treppa
Chairperson, Habematolel Pomo of Upper Lake
Vice Chairwoman, NAFSA

Sandra Knight, Vice Chairwoman
Mechoopda Indian Tribe of Chico Rancheria

Jonathan Windyboy
State Senator, SD 16, Montana Senate

James Williams, Jr.
Tribal Council Chairman, Lac Vieux Desert Band of Chippewa Indians

Sally Peterson
Vice Chairwoman, Middletown Rancheria of Pomo Indians

Reggie Lewis,
Chairman,
Picayune Rancheria of Chukchansi Indians of California

Chance Alberta,
Tribal Council & Chairman of Chukchansi, Inc.

U. S. Department of Justice

Civil Division

Deputy Assistant Attorney General

Washington, D.C. 20530

August 22, 2013

Sent via email to jshotton@omdevelopment.org
John Shotton
Chairman, Otoe-Missouria Tribe
Chairman, NAFSA
Native American Financial Services Association
Washington, DC

Dear Chairman Shotton:

Thank you very much for the meeting yesterday with NAFSA leadership and tribal leaders. We appreciated the opportunity to hear directly from you and other tribal leaders regarding your experiences in the online lending industry. In particular, the meeting went a long way to helping us understand your concerns and the challenges your members face.

As we discussed, the Department of Justice is committed to protecting consumers from fraudulent practices in all industries—without exception. To the extent we have evidence that any entity is engaged in fraudulent conduct and is harming consumers—in the short-term lending industry or in any other industry—we will use appropriate legal and equitable measures to combat that conduct.

As I emphasized in our meeting yesterday, the focus of our efforts at the Department of Justice has been combatting fraud; we have not singled out tribal government short-term lending businesses as an area of focus where such businesses engage in honest business practices. As we described, our efforts are aimed at eliminating fraud in the payment system by holding banks and processors accountable to their responsibilities under federal law not to engage in fraud or to aid others in engaging in fraud.

We do not understand our consultation obligations to require consultation with NAFSA or individual members concerning potential investigations of civil or criminal violations of law. Moreover, because our investigations are evidence-based and case-specific, we are not in a position to evaluate generally the lawfulness of tribal government short-term lending businesses.

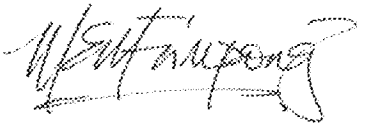
We were nevertheless encouraged to hear from you that you believe NAFSA members all comply with federal laws intended to protect consumers.

We appreciate your attempt to memorialize our meeting in your letter of yesterday, but I do feel compelled to note that your letter appears to mischaracterize some aspects of the discussion that we had. Your letter suggests that we stated that NAFSA members are off the table in our investigations. We did not. As I stated, we are focused on fraud, and to the extent that any NAFSA member is engaged in fraud, clearly that would be a concern for us. In addition, your letter suggests that we stated that the short-term lending the NAFSA members engage in poses no risk to banks. We did not make such a statement and are not in a position to make such a statement. It is the purview of the banks and the agencies that regulate them to assess the risk—if any—posed by the NAFSA members' lending models, and the Department of Justice will consider taking action against any bank or payment processor that knows or turns a blind eye to fraudulent proceeds passing through their accounts.

Finally, your letter suggests that we believe that the media incorrectly stated the aims of our initiative. In fact, the media report at issue accurately quoted a Department of Justice official as follows: "'We are changing the structures within the financial system that allow *all kinds of fraudulent merchants* to operate,' a Justice Department official said, with the intent of 'choking them off from the very air they need to survive.'"[1] It was your letter to the banks of August 14, 2013, as well as the White Paper you circulated yesterday, which incorrectly stated that we seek to "choke the air" of lenders or of tribal government short-term lending businesses. As the full quote makes clear, we seek to choke the air of "all kinds of fraudulent merchants." As discussed, this could include any entity engaged in fraud using the payment system, and does not exclude any lenders engaged in fraud.

Thank you for giving us the opportunity to clarify these points. Again, we found the dialogue extremely valuable, and look forward to a continued dialogue with you and your colleagues regarding consumer protection issues of mutual concern.

Very truly yours,



Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

[1] Alan Zibel and Brent Kendall, "Probe Turns Up Heat on Banks," *Wall Street Journal*, August 7, 2013.

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Friday, August 23, 2013 12:19 PM
To: Blume, Michael S.; Goldberg, Richard; Sweet, Joel; [redacted]
Subject: Re: Regulators Gang up on Banks, Third-Party Payment Processors

Got it.

From: Blume, Michael S.
Sent: Friday, August 23, 2013 12:08 PM
To: Goldberg, Richard; Frimpong, Maame Ewusi-Mensah (CIV); Sweet, Joel; [redacted]
Subject: Re: Regulators Gang up on Banks, Third-Party Payment Processors

What is more, the return rates in our cases are just a part of the story, a red flag. We also often have internal bank discussions that all but acknowledge that the merchants are fraudulent.

From: Goldberg, Richard
Sent: Friday, August 23, 2013 12:01 PM
To: Frimpong, Maame Ewusi-Mensah (CIV); Sweet, Joel; Blume, Michael S.; [redacted]
Subject: RE: Regulators Gang up on Banks, Third-Party Payment Processors

We have not identified any specific percent as a threshold. Most of the banks and processors we are targeting had total return rates much much higher. 30 – 70%

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Friday, August 23, 2013 12:00 PM
To: Sweet, Joel; Blume, Michael S.; Goldberg, Richard; [redacted]
Subject: Re: Regulators Gang up on Banks, Third-Party Payment Processors

Is what he says about our "3% benchmark" correct?

From: Sweet, Joel
Sent: Friday, August 23, 2013 10:55 AM
To: Frimpong, Maame Ewusi-Mensah (CIV); Blume, Michael S.; Goldberg, Richard; [redacted]
Subject: Fw: Regulators Gang up on Banks, Third-Party Payment Processors

FYI - from FDIC. Good to have American Banker spread the word.

Joel M. Sweet
[redacted]@usdoj.gov

From: Benardo, Michael B. [mailto[redacted]@FDIC.gov]
Sent: Friday, August 23, 2013 10:49 AM
To: Sweet, Joel
Subject: Regulators Gang up on Banks, Third-Party Payment Processors

And, I assume you saw this Op Ed from Peter Weinstock who leads the Financial Institutions Corporate and Regulatory practice at Hunton & Williams LLP. It is very critical of the DOJ and the FDIC's efforts to ensure that FIs are appropriately monitoring and managing risk associated with TPPPs.

Regulators Gang up on Banks, Third-Party Payment Processors

08/22/2013
American Banker
Peter Weinstock

State and federal regulators appear to be orchestrating a series of actions to force financial institutions and third-party payment processors to stop doing business with certain online consumer installment lenders.

The Department of Justice has reportedly issued subpoenas to banks and processors. The Federal Deposit Insurance Corp, seemingly in conjunction with the DOJ, is descending upon financial institutions that do business with processors. Such efforts go beyond the FDIC's traditional skepticism and antipathy for processors. Also, Benjamin Lawsky, New York's Superintendent of Financial Services, has sent letters to many of the biggest banks in the country, advising them that they should not accept automated clearing house transactions from a number of online lenders. These developments are likely to have significant implications for community banks, as well as for innovation, consumer choice and the efficiency of the retail payment networks.

At the crux of this attack on banks and processors is an effort to choke off access to the payment network for certain online lenders and merchants with "high" return rates, or percentages of ACH debits that the consumer's bank returns unpaid or for a refund. An anonymous DOJ official told The Wall Street Journal that the merchants need to be "chok[ed] off from the very air they need to survive" and Lawsky has used similar language in reference to the lenders.

The DOJ and the FDIC, in particular, are seeking to use threats and coercion to convince community banks and processors to cease doing business with these online lenders. In the case of the DOJ, there is the prospect of expensive litigation. Such costs cause a financial institution to enter into a settlement agreement to stop the bleeding. The DOJ would then use such a document as a warning to any financial institution that seeks to provide such services.

For instance, the DOJ has alleged that an overall return rate of 3% on all of a merchant's ACH transactions should be the benchmark for what is considered fraud, since it is higher than the industry average tracked by the trade group NACHA. But this is misleading. This rate does not distinguish among the type of the return (unauthorized entries are very different from returns due to insufficient funds), the nature of the transaction or the customer base (poor people tend to bounce more items). Under NACHA rules, a paper check that has bounced may be converted to an electronic form and re-presented using the RCK standard entry class code. According to NACHA, in 2012, 60.48% of RCK transactions were returned, and of those, 83.7% were returned for non-sufficient funds. Yet, no one is claiming these transactions are fraudulent. The DOJ also compares the card networks' rates of disputed transactions to the overall ACH return rates. But these are two completely disparate numbers. Card network disputed rates do not include transactions that are declined when the card is swiped. ACH returns, on the other hand, can include cases of insufficient funds or incorrect account information, along with debits disputed by the accountholder.

The FDIC has been descending on banks threatening enforcement action to the extent they can find any weakness in compliance management systems. Examinations are lasting weeks during which management teams are burdened with extensive document requests.

The question is whether the government should be able to use its full enforcement arsenal to force institutions to stop doing business with parties who provide a legal product, albeit one that those agencies apparently find distasteful. We who work in relatively well-paid professions like law and banking can all agree we are pleased that we have viable credit alternatives, and therefore, do not need to resort to small-dollar loans with high rates of interest and high fees. Our preference for, and ability to access, cheaper credit should not lead us to conclude others do not want this product.

Interestingly enough, the people who actually borrow on such terms advised the Consumer Financial Protection Bureau that they overwhelmingly like having access to such credit and understand the costs of the loans they are receiving. Nonetheless, the CFPB, in its study of "payday" lending, stated its belief that such credit could create a "debt trap."

The CFPB was authorized by Congress, in the Dodd-Frank Act, to adopt regulation governing payday lenders. To date, it has not done so. So, here we have an instance where two agencies have taken it upon themselves to use the might of

government to eliminate a product that they do not believe consumers should be able to access (despite the desires of those consumers themselves) without going through the rulemaking process that is the exclusive province of the CFPB in the case of such products.

One way to consider this issue is that it is a fight between the online lenders, on one hand, and the DOJ and the FDIC, on the other hand. Unfortunately, the FDIC and the DOJ are painting with an extremely broad brush as to whom they consider bad actors when they include the banks and processors. The precedential effect is alarming. After online installment consumer lending, what comes next? New York Attorney General Eric Schneiderman is investigating whether payroll cards shortchange employees. Should payroll cards be outlawed by the threat of enforcement action without appropriate rulemaking?

Also, what do regulatory efforts to interfere with the payment system do to innovation? Do we really want to be empowering regulators using enforcement powers to be deciding what technological innovations are in the best interests of the American people?

A processor is generally a software company that processes a variety of payment instruments, such as ACH transfers. They are so prevalent in the banking system that we do not even consider them as third parties. They include firms such as PayChex, Fiserv, Jack Henry, and FIS. There are even software companies that process payments for registering for a marathon, for filing tax returns with tax preparers, and for the vast majority of online businesses that are too small to do this work themselves. In fact, the vast majority of payroll in this country and the tax payments for payroll are performed by third party payment processors.

In short, what is occurring is not the appropriate use of enforcement sanctions against malfeasance. Instead, it is a systematic effort to root out a product under the guise of claims of inappropriate conduct. Bankers should insist that efforts like these go through the rulemaking process of the CFPB. The CFPB is required by law to weigh such issues as availability of credit in deciding whether to adopt a rule. This is a much better approach than the use of unchecked police powers.

Peter G. Weinstock leads the Financial Institutions Corporate and Regulatory practice at Hunton & Williams LLP.

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Friday, August 23, 2013 12:39 PM
To: Sweet, Joel; Blume, Michael S.; Goldberg, Richard; [redacted]
Subject: Re: Regulators Gang up on Banks, Third-Party Payment Processors

Understood. Thanks.

From: Sweet, Joel
Sent: Friday, August 23, 2013 12:35 PM
To: Blume, Michael S.; Goldberg, Richard; Frimpong, Maame Ewusi-Mensah (CIV); [redacted]
Subject: RE: Regulators Gang up on Banks, Third-Party Payment Processors

What is true is that our subpoenas ask banks to produce documents identifying TPPP and merchants with total return rates of 3 percent or more.

VISA and NACHA use 1 percent as a warning threshold for excessive returns identified as unauthorized. NACHA does not presently have a total return threshold, but plans to introduce one in the Fall. Excluding one outlier business activity (representment of bounced checks), the national average for all ACH returns (all businesses, all return reasons) is 1.38 percent. For RCCs, the industry average for returns is far lower, closer to ½ of 1 percent.

As described below, we use 3 percent only as a benchmark to identify potentially fraudulent merchants – not as conclusive evidence of wrongdoing. It's a starting point.

From: Blume, Michael S.
Sent: Friday, August 23, 2013 12:08 PM
To: Goldberg, Richard; Frimpong, Maame Ewusi-Mensah (CIV); Sweet, Joel; [redacted]
Subject: Re: Regulators Gang up on Banks, Third-Party Payment Processors

What is more, the return rates in our cases are just a part of the story, a red flag. We also often have internal bank discussions that all but acknowledge that the merchants are fraudulent.

From: Goldberg, Richard
Sent: Friday, August 23, 2013 12:01 PM
To: Frimpong, Maame Ewusi-Mensah (CIV); Sweet, Joel; Blume, Michael S.; [redacted]
Subject: RE: Regulators Gang up on Banks, Third-Party Payment Processors

We have not identified any specific percent as a threshold. Most of the banks and processors we are targeting had total return rates much much higher. 30 – 70%

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Friday, August 23, 2013 12:00 PM
To: Sweet, Joel; Blume, Michael S.; Goldberg, Richard; [redacted]
Subject: Re: Regulators Gang up on Banks, Third-Party Payment Processors

Is what he says about our "3% benchmark" correct?

From: Sweet, Joel
Sent: Friday, August 23, 2013 10:55 AM
To: Frimpong, Maame Ewusi-Mensah (CIV); Blume, Michael S.; Goldberg, Richard; [redacted]
Subject: Fw: Regulators Gang up on Banks, Third-Party Payment Processors

FYI - from FDIC. Good to have American Banker spread the word.

Joel M. Sweet
202-532-4663
joel.sweet@usdoj.gov

From: Benardo, Michael B. [mailto:[redacted]@FDIC.gov]
Sent: Friday, August 23, 2013 10:49 AM
To: Sweet, Joel
Subject: Regulators Gang up on Banks, Third-Party Payment Processors

And, I assume you saw this Op Ed from Peter Weinstock who leads the Financial Institutions Corporate and Regulatory practice at Hunton & Williams LLP. It is very critical of the DOJ and the FDIC's efforts to ensure that FIs are appropriately monitoring and managing risk associated with TPPPs.

Regulators Gang up on Banks, Third-Party Payment Processors

08/22/2013
American Banker
Peter Weinstock

State and federal regulators appear to be orchestrating a series of actions to force financial institutions and third-party payment processors to stop doing business with certain online consumer installment lenders.

The Department of Justice has reportedly issued subpoenas to banks and processors. The Federal Deposit Insurance Corp, seemingly in conjunction with the DOJ, is descending upon financial institutions that do business with processors. Such efforts go beyond the FDIC's traditional skepticism and antipathy for processors. Also, Benjamin Lawsky, New York's Superintendent of Financial Services, has sent letters to many of the biggest banks in the country, advising them that they should not accept automated clearing house transactions from a number of online lenders. These developments are likely to have significant implications for community banks, as well as for innovation, consumer choice and the efficiency of the retail payment networks.

At the crux of this attack on banks and processors is an effort to choke off access to the payment network for certain online lenders and merchants with "high" return rates, or percentages of ACH debits that the consumer's bank returns unpaid or for a refund. An anonymous DOJ official told The Wall Street Journal that the merchants need to be "chok[ed] off from the very air they need to survive" and Lawsky has used similar language in reference to the lenders.

The DOJ and the FDIC, in particular, are seeking to use threats and coercion to convince community banks and processors to cease doing business with these online lenders. In the case of the DOJ, there is the prospect of expensive litigation. Such costs cause a financial institution to enter into a settlement agreement to stop the bleeding. The DOJ would then use such a document as a warning to any financial institution that seeks to provide such services.

For instance, the DOJ has alleged that an overall return rate of 3% on all of a merchant's ACH transactions should be the benchmark for what is considered fraud, since it is higher than the industry average tracked by the trade group NACHA. But this is misleading. This rate does not distinguish among the type of the return (unauthorized entries are very different from returns due to insufficient funds), the nature of the transaction or the customer base (poor people tend to bounce more items). Under NACHA rules, a paper check that has bounced may be converted to an electronic form and re-presented using the RCK standard entry class code. According to NACHA, in 2012, 60.48% of RCK transactions were returned, and of those, 83.7% were returned for non-sufficient funds. Yet, no one is claiming these transactions are fraudulent. The DOJ also compares the card networks' rates of disputed transactions to the overall ACH return rates. But these are two completely disparate numbers. Card network disputed rates do not include transactions that are declined

when the card is swiped. ACH returns, on the other hand, can include cases of insufficient funds or incorrect account information, along with debits disputed by the accountholder.

The FDIC has been descending on banks threatening enforcement action to the extent they can find any weakness in compliance management systems. Examinations are lasting weeks during which management teams are burdened with extensive document requests.

The question is whether the government should be able to use its full enforcement arsenal to force institutions to stop doing business with parties who provide a legal product, albeit one that those agencies apparently find distasteful. We who work in relatively well-paid professions like law and banking can all agree we are pleased that we have viable credit alternatives, and therefore, do not need to resort to small-dollar loans with high rates of interest and high fees. Our preference for, and ability to access, cheaper credit should not lead us to conclude others do not want this product.

Interestingly enough, the people who actually borrow on such terms advised the Consumer Financial Protection Bureau that they overwhelmingly like having access to such credit and understand the costs of the loans they are receiving. Nonetheless, the CFPB, in its study of "payday" lending, stated its belief that such credit could create a "debt trap."

The CFPB was authorized by Congress, in the Dodd-Frank Act, to adopt regulation governing payday lenders. To date, it has not done so. So, here we have an instance where two agencies have taken it upon themselves to use the might of government to eliminate a product that they do not believe consumers should be able to access (despite the desires of those consumers themselves) without going through the rulemaking process that is the exclusive province of the CFPB in the case of such products.

One way to consider this issue is that it is a fight between the online lenders, on one hand, and the DOJ and the FDIC, on the other hand. Unfortunately, the FDIC and the DOJ are painting with an extremely broad brush as to whom they consider bad actors when they include the banks and processors. The precedential effect is alarming. After online installment consumer lending, what comes next? New York Attorney General Eric Schneiderman is investigating whether payroll cards shortchange employees. Should payroll cards be outlawed by the threat of enforcement action without appropriate rulemaking?

Also, what do regulatory efforts to interfere with the payment system do to innovation? Do we really want to be empowering regulators using enforcement powers to be deciding what technological innovations are in the best interests of the American people?

A processor is generally a software company that processes a variety of payment instruments, such as ACH transfers. They are so prevalent in the banking system that we do not even consider them as third parties. They include firms such as PayChex, Fiserv, Jack Henry, and FIS. There are even software companies that process payments for registering for a marathon, for filing tax returns with tax preparers, and for the vast majority of online businesses that are too small to do this work themselves. In fact, the vast majority of payroll in this country and the tax payments for payroll are performed by third party payment processors.

In short, what is occurring is not the appropriate use of enforcement sanctions against malfeasance. Instead, it is a systematic effort to root out a product under the guise of claims of inappropriate conduct. Bankers should insist that efforts like these go through the rulemaking process of the CFPB. The CFPB is required by law to weigh such issues as availability of credit in deciding whether to adopt a rule. This is a much better approach than the use of unchecked police powers.

Peter G. Weinstock leads the Financial Institutions Corporate and Regulatory practice at Hunton & Williams LLP.

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Monday, August 26, 2013 9:42 AM
To: McKenzie, Peggy (CIV); Blume, Michael S.
Cc: Olin, Jonathan F. (CIV)
Subject: Re: 3PPP briefing

One hour. Thank you!

----- Original Message -----
From: McKenzie, Peggy (CIV)
Sent: Monday, August 26, 2013 09:40 AM
To: Blume, Michael S.; Frimpong, Maame Ewusi-Mensah (CIV)
Cc: Olin, Jonathan F. (CIV)
Subject: RE: 3PPP briefing

Thanks, will this be a one hour or half hour meeting?

-----Original Message-----
From: Blume, Michael S.
Sent: Monday, August 26, 2013 9:39 AM
To: Frimpong, Maame Ewusi-Mensah (CIV); McKenzie, Peggy (CIV)
Cc: Olin, Jonathan F. (CIV)
Subject: RE: 3PPP briefing

Thanks, all.

It should be Maame, Rich Goldberg, Joel Sweet, [redacted] and myself.

Mike

-----Original Message-----
From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Monday, August 26, 2013 9:36 AM
To: McKenzie, Peggy (CIV)
Cc: Olin, Jonathan F. (CIV); Blume, Michael S.
Subject: Re: 3PPP briefing

Copying Mike who can let you know. Date will be September 4. Thanks!

----- Original Message -----
From: McKenzie, Peggy (CIV)
Sent: Monday, August 26, 2013 09:25 AM
To: Frimpong, Maame Ewusi-Mensah (CIV)
Cc: Olin, Jonathan F. (CIV)
Subject: RE: 3PPP briefing

Maame,

Who should be invited to this briefing?

Thanks,
Peggy

-----Original Message-----
From: Olin, Jonathan F. (CIV)
Sent: Sunday, August 25, 2013 3:35 PM
To: Frimpong, Maame Ewusi-Mensah (CIV)
Cc: McKenzie, Peggy (CIV)
Subject: RE: 3PPP briefing

Peggy, can you please schedule this? Maybe start at 945 (and reschedule Maame's individual)?

Thanks,
Jon

-----Original Message-----
From: Olin, Jonathan F. (CIV)
Sent: Saturday, August 24, 2013 3:08 PM
To: Frimpong, Maame Ewusi-Mensah (CIV)
Subject: Re: 3PPP briefing

That makes sense to me.

On Aug 23, 2013, at 12:33 PM, "Frimpong, Maame Ewusi-Mensah (CIV)" <[redacted]@CIV.USDOJ.GOV> wrote:

> Hi Jon -
>
> Any thoughts on when you want to schedule this? We were thinking Wednesday morning after Labor Day, to avoid conflicts (leave, other meetings, holidays) and give us a chance to prepare a summary memo and have a pre-meet. [redacted]
>
> Let me know.
>
> Thanks!
> Maame

U.S. Department of Justice

Civil Division

Washington, DC 20530

September 9, 2013

TO: Stuart F. Delery
Assistant Attorney General
Civil Division

THROUGH: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

FROM: Michael S. Blume
Director
Consumer Protection Branch

SUBJECT: Operation Choke Point: Six-Month Status Report

This memo addresses our efforts during the past six months to combat mass-market consumer fraud by focusing on payment systems vulnerabilities. Our goal is to protect consumers by imposing obstacles to scammers through an investigatory focus on third-party payment processors and banks that enable fraudulent merchants to access consumers' bank accounts.

I. Efforts and Progress

To date, we have served subpoenas on [redacted] banks and [redacted] payment processors as part of Operation Choke Point. Based upon information obtained in response to these subpoenas and upon corroboration from other sources, we have determined that we are accurately identifying banks and processors engaged in illicit conduct. We have opened civil and criminal investigations into several of these entities. Decisions to open investigations on several more entities are pending and subject only to availability of resources.

Moreover, we have observed a dramatic shift in the banking industry with respect to third-party payment processor risk assessment and risk tolerance, as will be described further below. Segments of the banking industry that had been doing business with third party payment processors have chosen to exit or severely curtail that business, thereby making it harder – and in some cases, impossible – for untold numbers of merchants who prey on consumers to run their illegitimate operations.

We have accomplished a great deal as a result of our subpoenas and our engagement with the banks and processors that have received them. The following is a broad sketch of what has happened since we began the initiative in February 2013:

- We opened or initiated criminal investigations of four payment processors and their principals, as well as a bank and responsible bank officials.

- We have opened civil FIRREA investigations into more than [redacted] banks, and we are attempting to negotiate consent decrees with t[redacted] banks.

- Several banks and payment processors -- after receiving our subpoenas and understanding our concerns -- have stopped processing payments for fraudulent merchants, thereby providing immediate and enduring relief to millions of consumer fraud victims and would-be victims. We are working on a method of quantifying the impact, and will provide a measure as soon as we have settled on an appropriate method.

- We have outlined our initiative and the illicit practices of banks and payment processors to several federal agencies, including officials at the Department of Treasury's Office of Terrorist Financing and Financial Crimes and to the bank regulatory community more generally. The Treasury has requested information and data from our initiative to develop legislative and/or regulatory cures to prevent payment systems fraud.

- We have organized presentations by experts on the topics of electronic payments through the Automated Clearing House (ACH) network and check payment systems. The presentations were attended by CPB personnel and more than 150 others from law enforcement agencies and regulatory agencies.

- We have engaged with industry representatives to ensure that our initiative targets illegal conduct but permits lawful conduct to proceed unhindered.

- We have garnered additional resources to implement Choke Point – at no cost to the Department – including two Postal Inspectors, two Postal Inspection Service analysts, an FBI analyst, an FTC attorney assigned as a Special Assistant U.S. Attorney, and as described below, [redacted] U.S. Attorney's Offices.

- Front page articles in the Wall Street Journal on August 7, 2013,[1] and the New York Times on June 10, 2013,[2] have educated the public and, more importantly, the banking and payment processor industries, about our initiative. The articles have acted as a kind

[1] "Probe Turns Up Heat On Banks," available at http://online.wsj.com/article/SB10001424127887323838204578654411043000772.html

[2] "Banks Seen as Aid in Fraud Against Older Consumers," available at http://www.nytimes.com/2013/06/11/business/fraud-against-seniors-often-is-routed-through-banks.html?pagewanted=all&_r=0

of "deterrence multiplier;" we have learned that the articles have pushed banks to take proactive steps to improve their internal operations without our having to engage them.

All signs indicate that Operation Choke Point is having an unprecedented effect on banks doing business with illicit third-party payment processors and fraudulent merchants. We believe we already have denied fraudsters access to tens, if not hundreds, of millions of dollars from consumers' bank accounts, and that amount will increase daily and indefinitely. This unparalleled level of deterrence is corroborated by payment processors and banks that have informed us that they have stopped providing services to fraudulent merchants; undercover recordings of fraudulent operators – including those who provided Internet payday loans – who, citing pressure from our initiative, have decided to shut down their operations; and FTC attorneys describing increased cooperation by banks and processors in FTC investigations.

Most importantly, we have learned directly from many sources that banks that have received our subpoenas, and others aware of our efforts, are scrutinizing their relationships with high risk third-party payment processors. In several cases, after receiving a subpoena, banks and processors have self-disclosed potentially problematic relationships and have informed us that they have taken corrective action. We have encouraged this type of positive conduct. As a consequence, we have a backlog of matters in which the bank or processor has agreed to stop bad conduct and has indicated an interest in attempting to negotiate an agreed resolution.

The following sections contain brief summaries of the criminal and civil investigations we have initiated. The sections are ordered to correspond to the level of activity we currently are devoting to each investigation, with the most active investigations listed first.

[redacted]

L. Other Matters

Upon receiving our subpoenas, several other banks took action to change their practices. Each bank warrants further investigation, which we will undertake as resources become available. A few examples are:

[redacted]

[redacted]

II. Challenges and Our Strategies for Success

As Operation Chokepoint has progressed, we have encountered challenges from those who do not wish our efforts to succeed and resource constraints that limit our ability to address each and every one of the potential targets that we have identified. The sections below describe these obstacles and our strategies for overcoming them.

A. The Internet Payday Lending Industry and Its Relationship to Indian Tribes

Many of the banks that have received our FIRREA subpoenas have reported extensive relationships with Internet payday lenders, via payment processors. Several banks have informed us that, as a result of our subpoenas, they have taken a deeper look at these Internet payday lenders and their business practices. Finding substantial questions concerning the legality of the Internet payday lending business models and the loans underlying debits to consumers' bank accounts, many banks have decided to stop processing transactions in support of Internet payday lenders. We consider this to be a significant accomplishment and positive change for consumers, given that a large number of consumer advocates and federal and state authorities have been trying with limited success – and for many years – to stem the growth of unlawful practices by the Internet payday lending industry.

A payday loan typically is a short-term, high interest loan made without collateral.[3] Instead of collateral or other security, unlawful Internet payday lenders rely on their ability to access borrowers' banks accounts to take money based on a purported authorization buried in a misleading loan document. Most payday loans are for $250 to $700. Internet payday lenders generally have operated outside any regulatory framework and have successfully evaded efforts by state attorneys general and federal agencies (CFPB and FTC) to stop abuses against consumers.

Internet payday lenders charge interest rates of 400 to 1,800 percent. Borrowers often are misled to believe that the loan will end in a limited period of time, but the lenders manipulate ACH debits from the borrowers' accounts so that the borrower ends up paying much more in

[3] For ease of reference, we are referring to all short-term, unsecured loans as "payday" loans. We recognize that not all such loans are traditional payday loans, those whose repayment dates coincide with a borrower's next payday. For present purposes, the differences between payday loans and other short-term, unsecured loans is not relevant.

interest and other fees than the consumers anticipated. Many of these Internet payday lenders evade state usury and other laws by claiming to operate from overseas, or by claiming the protection of tribal sovereign immunity.

1. Tribal Involvement and Claims of Sovereignty

As banks have terminated their relationships with Internet payday lenders, Indian tribes affiliated with certain payday lenders have lost a stream of income. Internet payday lenders originally sought tribal affiliation as a shield to state usury laws that bar the high interest rates they charge borrowers. Evidence we have collected reveals that a number of these Internet payday lenders have little or no true connection to the tribes and simply use the nominal relationship as a cover for their illicit practices.

Internet payday lenders affiliated with tribes, and the tribes themselves, take the position that state lending laws and many federal lending and consumer protection laws do not apply to their lending activities. They claim that tribal sovereignty shields them from state usury and consumer protection laws. Although many tribal-affiliated lenders claim to follow some federal laws voluntarily, such as the Truth in Lending Act, they claim federal laws do not apply to them absent an express Congressional statement to that effect. These entities cite the Indian law canons of construction, judicially-created canons stating that courts should resolve ambiguities in federal law in favor of Indians and that only a clear expression of Congressional intent can overcome tribal sovereignty. *See e.g., Mont. v. Blackfeet Tribe*, 471 U.S. 759, 766 (1985). Tribes and tribal-affiliated lenders read the canons to mean that laws of general applicability do not apply to tribes unless Congress explicitly states that the law applies to tribes.

Some government entities, including the FTC and the Department of Labor, have taken the position that laws of general applicability do apply to Indian tribes unless Congress explicitly excludes tribes. Thus, while the CFPB, the FTC, and state law enforcement issue subpoenas to lenders to investigate their activities and bring suit to enforce such laws, Internet payday lenders affiliated with tribes refuse to respond to subpoenas and raise tribal sovereign immunity as a bar to enforcement actions.

There is considerable disagreement in the courts about the applicability of laws of general applicability to Indian tribes. In the most recent case on the matter, a magistrate judge held that the FTC Act, the Truth in Lending Act, and the Electronic Funds Transfer Act – all laws of general applicability – applied to tribal business entities. *See FTC v. AMG Services, Inc.*, 12–cv–00536 (D. NV July 16, 2013). The case was especially relevant in that it arose in the context of an FTC enforcement action against a tribally-affiliated Internet payday lender. The defendants in the FTC's case engaged in deceptive practices nearly identical to those of the Internet payday lenders we see in our bank and processor investigations.

We have consulted extensively with the Justice Department's Office of Tribal Justice. It is our understanding that there is not an official DOJ position on the issue of the intersection of laws of general applicability and tribal sovereignty. It is our further understanding that there is disagreement within DOJ about what that position should be. The Office of Tribal Justice has

stated that criminal law does apply in Indian Country, although they did not know of examples in which a tribe had been prosecuted.

Our investigations do not directly implicate these questions of tribal sovereignty. We have no intention of prosecuting a tribe or tribal entity. We are focused on banks and the responsibilities they have to ensure that they are not aiding fraudulent schemes. If a bank or processor is facilitating a scheme to defraud, then they would be the proper subject of a civil or criminal case, regardless of who is committing the fraud.

On August 21, 2013, we met with the Native American Financial Services Association ("NAFSA"), a trade association formed "to protect and advocate for Native American sovereign rights and enable tribes to offer responsible online lending products." NAFSA representatives expressed deep concern for the manner in which our investigation was affecting their banking relationships. At the meeting and in follow up correspondence, NAFSA asserted that we were targeting their membership for dissolution and sought assurances that no NAFSA member would be the subject of a federal case. We informed them that our effort was not directed at lawful conduct and sought to eliminate fraudulent practices that victimized consumers. We did not provide assurances that NAFSA members were off the table in our investigations, but, as stated above, we reiterated that we are focused on investigating fraudulent conduct.

As our initiative proceeds, more banks likely will review and terminate their relationships with tribal-affiliated Internet payday lenders engaged in suspicious or outright fraudulent conduct. This will continue to cause concern from tribes whose lose a source of revenue. Our intention is not to stray from our course – pursuing financial entities that aid and abet fraudulent business practices, while avoiding statements that could be read as targeting lawful behavior.

2. Our Efforts Should Not Deter Banks from Dealing with Legitimate Lenders

A recent letter to both DOJ and the FDIC from several members of the U.S. House of Representatives accuses us of targeting the entire Internet payday lending industry and of sweeping too broadly with our enforcement brush. The claim is that our efforts are directed at legitimate Internet payday lenders.

As discussed above, we are focused on fraud and not legitimate lending businesses. Because of our efforts, many banks have realized that they have opened the payment systems to potentially fraudulent merchants without sufficient due diligence and monitoring. As a result, processors and merchants will face additional scrutiny from banks, which are now more focused on the legal, systemic, and reputational risks associated with these relationships. This scrutiny has led some banks to determine that it is not in their best interest – from a risk assessment and risk tolerance perspective – to continue to do business with internet lenders. Although we recognize the possibility that banks may have therefore decided to stop doing business with legitimate lenders, we do not believe that such decisions should alter our investigative plans. Solving that problem – if it exists – should be left to the legitimate lenders themselves who can, through their own dealings with banks, present sufficient information to the banks to convince them that their business model and lending operations are wholly legitimate.

B. Application of FIRREA and Appropriate Penalties

As you know, the principal tool we are using to investigate banks and processors under Operation Choke Point is FIRREA. FIRREA allows us to subpoena documents and take depositions in our efforts to collect evidence. Ultimately, this evidence could form the basis for a civil penalty action under FIRREA, and possibly a request for injunctive relief under the Anti-Fraud Injunction Act, 18 U.S.C. § 1345. The latter statute provides a mechanism for enjoining mail fraud, wire fraud, and bank fraud schemes.

1. Violations of FIRREA

FIRREA's penalty provision was not designed principally to address consumer fraud. It penalizes fraud offenses "affecting a federally insured financial institution." 12 U.S.C. § 1833a(c)(2). FIRREA penalties are paid to the Treasury, and the statute does not include a provision for restitution to victims of fraud.

The offenses by the banks and payment processors under investigation "affect a financial institution" under FIRREA in that they create a variety of risks to those institutions. The banks are at risk because they could be held responsible for the bogus or fraudulently procured charges to consumer bank accounts. They also risk reputational harm from becoming known as institutions that help fraud schemes to victimize consumers.

The financial institutions we are investigating have not suffered any actual losses, but such actual losses are not necessary under FIRREA. There is only one case interpreting the phrase "affecting a financial institution" in the context of FIRREA, and that case supports our theory. In United States v. The Bank of New York Mellon, - F. Supp. 2d - , 2013 WL 1749418, *8-10 (S.D.N.Y. April 24, 2013), the court held that a financial institution need not have been victimized for a violation to have occurred. Nor does the scheme need to be "directed at" the institution. Id.

A number of courts have interpreted the phrase "affect a financial institution" in contexts other than FIRREA. The U.S. Sentencing Guidelines, for example, contain a sentencing enhancement for fraud offenses that "affect a financial institution." Under this provision, courts have found that the financial institution need not suffer actual harm in order to be "affected;" a showing of realistic and foreseeable exposure to substantial potential liability is sufficient. United States v. Johnson, 130 F.3d 1352, 1355 (9th Cir. 1997). In fact, there is a good argument that a financial institution can be affected in non-financial ways by damaging "employee morale and customer relationships, marr[ing] the bank's reputation and influenc[ing] the bank's immediate and long-term operations and policies." Id. See also United States v. Bennett, 161 F.3d 171, 193 (3d Cir. 1998) (citing, among other things, negative publicity that harmed the financial institution's reputation as "affecting a financial institution" under the Sentencing Guidelines). Banks that facilitate fraudulent transactions undoubtedly risk this sort of damage to their reputations and operations.

Although the clear majority of the case law addressing the phrase "affects a financial institution" supports a broad application of the concept, not all cases interpret the phrase as expansively. In United States v. Agne, 214 F.3d 47, 52-53 (1st Cir. 2000), for example, the court gave a narrower reading of the phrase as it is used in 18 U.S.C. § 3293(2), which provides a 10-year statute of limitations for fraud offenses that "affect a financial institution." The court stated that "the bank suffered no actual financial loss and experienced no realistic prospect of loss." Id.

The First Circuit began by noting that "affect" was not defined in section 3293(2) and looked to the definition in the Random House Dictionary. The dictionary gave the definition as "to act on; produce an effect or change in," and listed the synonyms as "influence, sway; modify, alter." Id. at 51 (quoting The Random House Dictionary of the English Language 33 (2d ed. 1983)). To the court, this lent "support to defendant's position that there must be some negative consequence to the financial institution to invoke the statute of limitations." Id. The First Circuit's opinion in Agne did not hold that placing a bank at a risk of loss was insufficient to affect a financial institution for purposes of the extended statute of limitations. In fact, the court stated: "Even assuming, without deciding, that being exposed to a risk of loss is sufficient to 'affect' a bank, within the ordinary meaning of that term, we cannot agree with the district court that this defendant created such a risk." Id. The Court rejected any argument that the bank was at risk of losing its client and tarnishing its reputation, finding: "We cannot construe a criminal statute to sweep so broadly as to make one guilty of wire fraud for merely arousing these possibilities." Id. at 52-53. See also United States v. Ubakanma, 215 F.3d 421 (4th Cir. 2000) (stating that a wire fraud offense only affects a financial institution "if the institution itself were victimized by the fraud, as opposed to the scheme's mere utilization of the financial institution in the transfer of funds.").

Although there is a split in the case law, the weight of authority leans toward a broad reading of the phrase "affects a financial institution." The Bank of New York Mellon case, cited above, provides strong support for our theory and is the only case interpreting the phrase in the context of FIRREA. Under that case, the financial and reputational risks created when banks facilitate fraud would be sufficient evidence to support a FIRREA case.

The Bank of New York Mellon case also supports our position that a defendant can violate FIRREA even if the defendant itself is the affected financial institution. The court issued a well-reasoned opinion stating:

> In sum, the essential point is this: the statute permits penalties against "whoever" commits a fraud affecting a federally insured financial institution. The purpose of that provision is to deter frauds that might put federally insured deposits at risk. Here, BNYM has been charged with participating in a fraudulent scheme and harming itself in the process. Just as Congress clearly intended to deter bank employees from engaging in fraud that results in harm to these institutions, Congress was entitled to conclude that penalties against financial institutions in cases like this would deter such institutions from similar, harmful, fraudulent conduct. If anything, the urgency may even be greater when the fraud allegedly pervades an institution that the government has backstopped. Both the text and purpose of FIRREA amply encompass the alleged conduct here.

Bank of New York Mellon, 2013 WL 1749418, at *15. Any FIRREA case we bring against a bank will be based, at least in part, upon this same theory – that the financial institution affected by the scheme to defraud was the bank that perpetrated the scheme. We therefore will rely on the well-reasoned opinion in that case to support our enforcement actions.

2. Penalties Under FIRREA

FIRREA provides for civil monetary penalties of $1 million per violation. A penalty for a "continuing violation" cannot exceed $5 million. The statute authorizes a higher penalty as follows: "If any person derives pecuniary gain from the violation, or if the violation results in pecuniary loss to a person other than the violator, the amount of the civil penalty may exceed the amounts described in paragraphs (1) and (2) but may not exceed the amount of such gain or loss." 18 U.S.C. § 1833a(b)(3)(A).

The banks and processors under investigation profited from their illicit actions and their gain could be considered a factor to consider to determine an appropriate penalty. In many of the cases we are investigating, consumer harm is much greater than the bank's profit or revenue. It is difficult to quantify consumer harm without a detailed analysis of the activities and financials of each of the bank's processors and their underlying merchants. Thus, we may use a multiple of the bank's revenue or profits as an appropriate penalty where loss to consumers is large but not readily quantifiable. These penalties will obtain the deterrent effect we seek, by illustrating to banks that they stand to lose much more than they gain from facilitating fraud. In particularly egregious cases in which a bank had specific knowledge (rather than deliberate ignorance) of a fraud and the extent of consumer losses, we may seek penalties in the amount of consumer losses.

Two of the banks with which we are attempting to negotiate consent decrees are in poor financial condition. These banks have presented "inability to pay" figures and arguments to justify low penalties. We recognize that if our early cases are settled for low amounts, it could be perceived by other banks as a benchmark and it may make it difficult to obtain higher penalties in other cases. We intend to maximize recovery in every case. We recognize, however, that the main benefit from our resolutions will be the immediate and continuing injunctive benefits and the deterrence of bad conduct by other banks.

C. Addressing Resource Limitations

The Consumer Protection Branch has assigned several attorneys to work with detailee Joel Sweet on the most active Operation Chokepoint investigations, in addition to their other assignments. Three United States Attorney's Offices – those in the District of Nevada, the Eastern District of North Carolina, and the Middle District of Florida – have eagerly joined our efforts by assigning AUSAs to work with us on particular investigations. Other U.S. Attorneys Offices have offered to assign AUSAs to assist once we are ready.

The U.S. Postal Inspection Service has also increased its commitment to our effort, adding a second full-time financial analyst. Postal Team Leader Clayton Gerber also has personally taken the lead in investigating some of our most important cases.

Notwithstanding our success in attracting partners to Choke Point, we have active investigations in need of resources (*see* Section II, above) and many more potential targets to investigate. We cannot fully staff and deeply probe every worthy case. The following is a list of the strategies we have developed for pursuing cases in light of our limited staff:

- We intend to try to reach consensual agreements with as many targets as possible. If we can obtain meaningful injunction relief and reasonable civil penalties from the banks, we set benchmarks – and define best practices – for the industry. And, we can then deploy our resources to pursue more investigations and therefore have a broader impact.

- We principally are pursing civil, rather than criminal, investigations. Criminal investigations can take considerably longer to complete and generally require a more intensive investigation. Only if an investigation presents particularly egregious criminal conduct are we opening it as a criminal investigation.

- We are targeting banks more than payment processors, and payment processors more than merchants. Any one case, whether against a bank, a processor, or a merchant, takes substantial time and attention from our team. Bank cases will deter other banks, thereby stopping the processing of transactions for fraudulent merchants and the processors with which they work. This may mean filing civil complaints or criminal cases against banks based on transactions with fraudulent merchants and/or processors -- but not filing actions against the underlying fraudulent merchants or processors. This practice is not optimal and may present litigation risks. But it may be necessary to prevent the initiative from grinding to a halt due to resources used pursuing merchants and processors.

In addition to our case-specific efforts, we have been collaborating with a number of partners in an attempt to increase their knowledge and attention to the roles banks and payment processors play in facilitating fraud. In this regard, we are in frequent contact with several state attorneys general, FTC, FDIC, and the Federal Reserve Bank of Atlanta, and we hope to begin working with the OCC soon. We have been working closely with NACHA, the entity created by the banking industry to supervise the ACH payment system.

Through these ongoing discussions, we hope to enhance each entity's appreciation of its responsibility and unique role in identifying fraudsters and bad actors, addressing these situations directly, and working with others toward combating consumer fraud. As these entities strengthen their efforts at identifying and combatting payment systems abuses, we expect that there will be fewer incidents of mass market fraud that DOJ and the FTC will need to address through litigation. Our relationships with each of these entities has been positive, active, and growing stronger.

III. Conclusion

Operation Choke Point has met with remarkable success in its first few months. Shining a spotlight on fraud facilitated through payment systems has pressured a number of banks and payment processors to stop aiding fraudulent merchants. Our specific investigations are varied and well-founded. And the obstacles placed in our way will not prevent us from putting a serious dent in consumer fraud perpetrated against the American consumer. (Goldberg, Sweet, [redacted]

FFIEC Information Technology Conference

Agenda

Tuesday, September 17, 2013

8:30 AM	**ADMINISTRATIVE REMARKS** **Jennifer C. Herring** Senior Program Administrator Federal Financial Institutions Examination Council Arlington, Virginia
8:40 AM	**MISSION ASSURANCE THROUGH RESILIENCE MANAGEMENT** **Dr. Nader Mehravari,** *Research Scientist* **Lisa Young,** *Senior Engineer* Carnegie Mellon University Software Engineering Institute CERT Program Pittsburg, Pennsylvania *Download Session Materials*
10:15 AM	**Break**
10:30 AM	**THIRD PARTY PAYMENT PROCESSORS: RELATIONSHIPS, GUIDANCE, AND CASE EXAMPLES** **Moderator:** **Michael Benardo,** *Chief, Cyber-Fraud and Financial Crimes Section* Federal Deposit Insurance Corporation Washington, D.C. **Joel Sweet,** *Trial Attorney* U.S. Department of Justice, Consumer Protection Branch Washington, D.C. **Jennifer LaRoche,** *Special Counsel* Office of the Comptroller of the Currency Washington, D.C. *Download Session Materials*
11:45 AM	**Lunch**
1:00 PM	**CLOUD STORAGE SOLUTIONS** **Karen Jaworski** Senior Director Portfolio Strategy & Planning EVault San Francisco, California *Download Session Materials*
2:30 PM	**Break**
3:00 PM	**DISASTER RECOVERY / BUSINESS CONTINUITY PLANNING** **Karen Alderson** National Bank Examiner Office of the Comptroller of the Currency Overland Park, Kansas *Download Session Materials*
3:40 PM	**Break**
3:50 PM	**FOREIGN-BASED TECHNOLOGY SERVICE PROVIDER (FB-TSP) RISKS** **Samuel Stuckal**, Research Director CEB TowerGroup Cheshire, Connecticut *Download Session Materials*
5:00 PM	**Reception for Attendees and Speakers** Virginia Square Auditorium Atrium

Wednesday, September 18, 2013

8:00 AM	**INCIDENT RESPONSE: A CASE STUDY OF AN INSIDER ATTACK** **Jason Garman**, Principal & Co-Founder **Keith Jones**, Director of Computer Forensics, Expert Witness Services & Training Practices Kyrus Tec, Inc. Sterling, Virginia AGENCY EXAMINER PANEL: **Ken Fortier**, Sr. IT Specialist Federal Reserve Bank of Boston Boston, Massachusetts **Brian Houlihan**, IT Specialized Examiner National Credit Union Administration Surprise, Arizona **Robert Swoyer**, IT Examiner Office of the Comptroller of the Currency New Ringgold, Pennsylvania *Download Session Materials* *Additional Reference Material*
9:30 AM	**Break**
10:00 AM	**ACH & ATM FRAUD** **Jeanette A. Fox, AAP**, Senior Director, Risk Investigations & Research NACHA Herndon, Virginia *Download Session Materials*
11:30 AM	**Lunch**
1:00 PM	**CYBER ATTACKS AND COUNTERMEASURES** **Mischel Kwon**, President and CEO Mischel Kwon Associates Fairfax, Virginia *Download Session Materials - Part 1* *Part 2* *Part 3* *Part 4*
2:45 PM	**Break**
3:15 PM	**TECHNOLOGY SERVICE PROVIDERS: ENSURING THE FINANCIAL INSTITUTIONS INTERESTS ARE PROTECTED** **Jeff VanSickel**, Practice Leader – Security Compliance SystemExperts Corp. Philadelphia, Pennsylvania *Download Session Materials*
4:30 PM	**Adjourn**

Thursday, September 19, 2013

8:00 AM	**MOBILE BANKING & PAYMENTS SECURITY** **Alphonse Pascual**, Senior Analyst of Security, Risk and Fraud Javelin Strategy & Research Pleasanton, California *Download Session Materials*
9:30 AM	**Break**
10:00 AM	**BRING YOUR OWN DEVICE (BYOD): SHOULD CONVENIENCE TRUMP SECURITY?** **Francis Tam**, Partner **Kevin Villanueva**, Senior Manager Moss Adams, LLP, Moss Adams Advisory Services Los Angeles, California

	Download Session Materials
11:30 AM	**Lunch**
1:00 PM	**SOCIAL MEDIA: FFIEC GUIDANCE** **Elizabeth Khalil**, Senior Policy Analyst Federal Deposit Insurance Corporation Washington, D.C. *Download Session Materials*
2:30 PM	**Break**
3:00 PM	**HARNESSING THE POWER OF BIG DATA & ANALYTICS IN BANKING & FINANCIAL MARKETS** **Vivek Bajaj** Director, Global Banking and Financial Markets, IBM Big Data Industry Team IBM Corporation Brussels, Belgium *Download Session Materials (Part 1)* *Download Session Materials (Part 2)*
4:30 PM	**CLOSING REMARKS** **Jennifer C. Herring** Senior Program Administrator Federal Financial Institutions Examination Council Arlington, Virginia

3501 Fairfax Drive • Room B3030 • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 516-5487 • http://www.ffiec.gov

Third Party Payment Processors: Relationships, Guidance, and Case Examples

Michael Benardo
Chief, Cyber-Fraud and Financial Crimes Section
Federal Deposit Insurance Corporation
Washington, D.C.

Joel Sweet
Trial Attorney
U.S. Department of Justice; Consumer Protection Branch
Washington, D.C.

Jennifer LaRoche
Special Counsel
Office of the Comptroller of the Currency
Washington, D.C.

Michael B. Benardo
Chief, Cyber Fraud and Financial Crimes Section
Federal Deposit Insurance Corporation
Washington, DC
[redacted]@fdic.gov

Michael B. Benardo is the Chief of the Cyber Fraud and Financial Crimes Section in the FDIC's Division of Supervision and Consumer Protection. He oversees all aspects of fraud-related initiatives, including establishment of regulatory policies and procedures. He is instrumental developing and implementing fraud-related supervisory programs including examination techniques, and represents the FDIC on interagency working groups with a goal of developing consistent interagency programs for combating financial institution fraud.

Mr. Benardo has nineteen years of progressive experience with the FDIC, including serving as a Manager in the Technology Supervision Branch. He also served as a key member of the FDIC's Year 2000 project team from 1997 through the century date change.

Prior to his employment wit the FDIC, Mr. Benardo spent six years working in the commercial banking industry. He worked in a variety of areas including several assignments in bank operations.

Mr. Benardo is a graduate of the University of South Florida with a B. S. degree in Finance.

Joel M. Sweet
Trail Attorney
U.S. Department of Justice, Consumer Protection Branch

Joel M. Sweet, a Trail Attorney for the U.S. Department of Justice; Consumer Protection Branch, was the lead prosecutor in United States v. Payment Processing Center, LLC, C.A. 06-725 (E.D. Pa.), in which the government shut down a third-party payment processor, seized the assets of the company and its principals, and litigated with Wachovia Bank concerning its business relationship with the payment processor. That action led to an investigation and enforcement action by the Office of the Comptroller of the Currency, a private class action alleging racketeering by Wachovia Bank, and the implementation of a $150 million victim restitution program.

In addition to consumer fraud, Mr. Sweet prosecutes cases involving healthcare and defense contract fraud, and also defends the government in a variety of civil matters. Mr. Sweet consults regularly with the Federal Reserve Board, the Federal Trade Commission, and state Attorneys General, concerning payment systems abuse and consumer fraud. He is a member of the Department of Justice's Mass-Marketing Fraud Working Group.

Before joining government, Mr. Sweet was a commercial litigator specialization in business disputes, class action litigation, and securities fraud. Mr. Sweet was a member of the Plaintiffs' Counsel Executive Committee in In re Holocaust Victim Assets Litigation, C.A. No. 4849 (E.D.N.Y.), a class action against Switzerland's three largest banks that settled in 1998 for $1.25 billion.

Jennifer LaRoche is an Attorney in the Enforcement and Compliance Division since September 1999. As an attorney in the E&C Division, she has worked extensively on issues involving credit card banks and predatory and abusive lending. T Bank was her first payment processor case. Jennifer Graduated from University of Maryland Law School in 1999.

Third Party Payment Processor Relationships

September 17, 2013

Michael B. Benardo
Chief, Cyber Fraud & Financial Crimes Section
Division of Risk Management Supervision
Federal Deposit Insurance Corporation

Third Party Payment Processors

- TPPPs: What they are?
  - A deposit customer that uses its banking relationship to process payments for merchant clients
- Merchant Clients
  - Legitimate
  - High Risk
  - Illegal

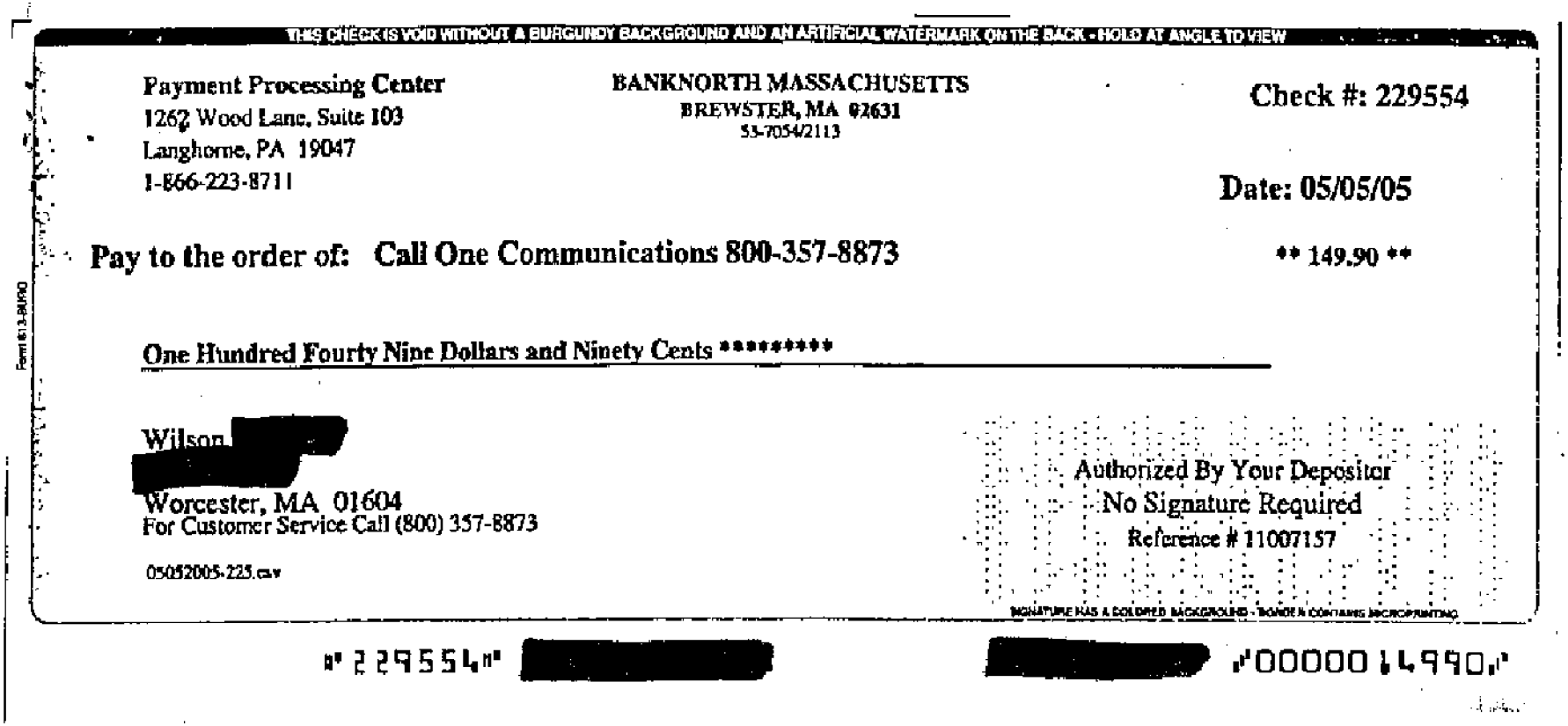
High Risk Merchants / Activities

- Ammunition Sales
- "As Seen on TV"
- Credit Card Schemes
- Credit Repair Services
- Drug Paraphernalia
- Escort Services
- Firearms/Fireworks Sales
- Gambling
- Get Rich Products
- Government Grants
- Home Based Charities
- Life Time Guarantees
- Pyramid Type Sales
- Pay Day Loans
- Pharmaceutical Sales
- Pornography
- Ponzi Schemes
- Racist materials
- Raffles/Sweepstakes
- Surveillance equipment
- Telemarketing
- Tobacco Sales

Typical Payment Types

- Remotely Created Checks (RCC)/Demand Drafts
- Automated Clearing House (ACH)

Remotely Created Check



THIS CHECK IS VOID WITHOUT A BURGUNDY BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK - HOLD AT ANGLE TO VIEW

Payment Processing Center
1262 Wood Lane, Suite 103
Langhorne, PA 19047
1-866-223-8711

BANKNORTH MASSACHUSETTS
BREWSTER, MA 02631
55-7054/2113

Check #: 229554

Date: 05/05/05

Pay to the order of: Call One Communications 800-357-8873

** 149.90 **

One Hundred Fourty Nine Dollars and Ninety Cents *********

Wilson [redacted]
Worcester, MA 01604
For Customer Service Call (800) 357-8873

05052005-225.csv

Authorized By Your Depositor
No Signature Required
Reference # 11007157

SIGNATURE HAS A GOLDFIED BACKGROUND - BORDER CONTAINS MICROPRINTING

⑈229554⑈ [redacted] [redacted] ⑈000014990⑈

Warning Signs / Red Flags

- Consumer Complaints (i.e., unauthorized, misrepresented, merchant error-armed consumer into providing account information)
- High rates of unauthorized returns/charge backs
- TPPP likely to use more than one financial institution to process payments and activity may periodically move between financial institutions

Enhanced Due Diligence

- Policies and procedures
- Know Your TPPPs customers
- Develop a processor approval program that extends beyond credit risk management
- Perform background checks on TPPPs and merchant clients
- Authenticate the TPPPs business operations and assess the risk level

Enhanced Due Diligence (Continued)

- Review promotional materials, including Websites, to determine target clientele
- Identify processors major customers
- Review corporate documentation
- Visit business operation center
- Review information of merchant clients; the principle business activity; geographic location; and sales techniques

Ongoing Monitoring Systems

- Monitoring high rates of return
- Setting return rate thresholds
- Setting transaction volume limits
- Auditing third party processors program
- Monitoring reserve adequacy
- Monitoring consumer complaints about merchant clients on Internet blogs and industry databases
- Developing contract language addressing access to records, conditions requiring account closing, and reserve adequacy

Potential Supervisory Responses

- May require the bank to terminate the relationship with the high-risk TPPP
- [illegible]
- [illegible]
- [illegible]

Unfair or Deceptive Practices?

- A bank may be viewed as facilitating a TPPP's or a merchant's fraudulent or unlawful activity
- Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices affecting commerce" and applies to all persons engaged in commerce, including banks
- Authority under section 8 of the FDI Act to take appropriate action when unfair or deceptive acts or practices are discovered

When a Bank Suspects Fraudulent Activity

- File a Suspicious Activity Report
- Require the TPPP to cease processing for that specific merchant
-

Resources

- FDIC Revised Guidance on Payment Processor Relationships (FIL-3-2012, dated January 31, 2012 (FDIC Guidance was first issued in 2008 (FIL-127-2008) but was updated in 2012)
- FinCEN Advisory on Risks Associated with Third-Party Payment Processors (FIN-2012-A010), dated October 22, 2012
- Supervisory Insights – Summer 2011

Resources (Continued)

- FDIC Guidance for Managing Third-Party Risk (FIL-44-2008), dated June 6, 2008
- OCC Bulletin on Payment Processors (OCC-2008-12), dated April 24, 2008
- FFIEC Handbook on Retail Payment Systems (March 2004) – Coverage of ACH Activities
- 2010 FFIEC BSA/AML Examination Manual

Comptroller of the Currency
Administrator of National Banks

Payment Processors:
Guidance for Examiners & Fraud Specialists

Jennifer J. LaRoche
Special Counsel, Enforcement & Compliance
Office of the Comptroller of the Currency
[redacted]@occ.treas.gov
[redacted]

Disclaimer

The views and opinions expressed in this presentation are my own and do not necessarily reflect the views of the OCC or any other government agency or official.

OCC Bulletin 2008-12 Risk Management Guidance for Payment Processor Accounts

- Heightened risks
- Appropriate due diligence on processors and their clients
- Effective underwriting
- Ongoing account monitoring, including of return volumes
- Banks without proper controls may be viewed as facilitating underlying fraud
- Take immediate action upon identifying improper activity (i.e., file SAR, terminate relationship)
- Additional guidance: OCC Bulletins 2006-39, 2006-13, 2001-47, Comptroller's Handbook, FFIEC BSA/AML Exam Manual and FDIC FIL 3-2012 and FIL-127-2008

Risk Mitigation Practices

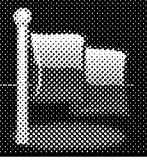
- Abide by all applicable guidance, laws and regulations
- Understand the risks and have appropriate controls, policies and procedures
- Know your customer, and your customer's customers
- Monitor account activity, particularly returns
- Investigate complaints and fraud warnings
- Validate information provided by the processor
- Obtain collateral and institute a debit restraint
- Be aware of current scams and schemes
- Act immediately upon identifying suspicious activity

Examining Guidance

- Verify the bank's due diligence and underwriting
- Review the bank's controls, policies and procedures for high-risk accounts
- If you find suspicious activity:
  - Gather information to support your findings
  - Escalate your findings to your supervisors
  - Communicate to the bank the seriousness of potentially facilitating consumer fraud
  - Encourage the bank to file a SAR and to contact law enforcement

Red Flags

- High return rates
- Merchants selling questionable products and services
- 100% refund policy
- Prior civil, criminal and regulatory actions against processor or its principals
- Consumer and other bank complaints
- Inquiries from law enforcement



If there are internet merchants, watch for the following:

- Reliance by bank on real time transaction details obtained from the merchant.
- Merchants who market via pop-ups on websites.

Notice of Affidavit received.

Bank Name
Address

RE: Affidavit for Account Number and Check 9999
Affidavit received on 02/22/07 for Customer Name

Dear Bank,

Your account holder has submitted an affidavit stating that the above mentioned item that was drafted against their account was not authorized.

We dispute this claim on the basis that this was a transaction that was generated in a secure area on our customer's website that required your account holder to agree to the terms and conditions and provide the information necessary to create an electronic draft. We have confirmed the information showing that your customer was on www.xyz.org when he opted to purchase the service offered by www.abc.com. His IP address was captured as well as the name of the internet provider he currently uses. If your customer would like a copy of the information or would like a refund, please have them go to www.abc.com complete the customer service form and someone will contact her immediately. Your assistance is greatly appreciated.

Sincerely

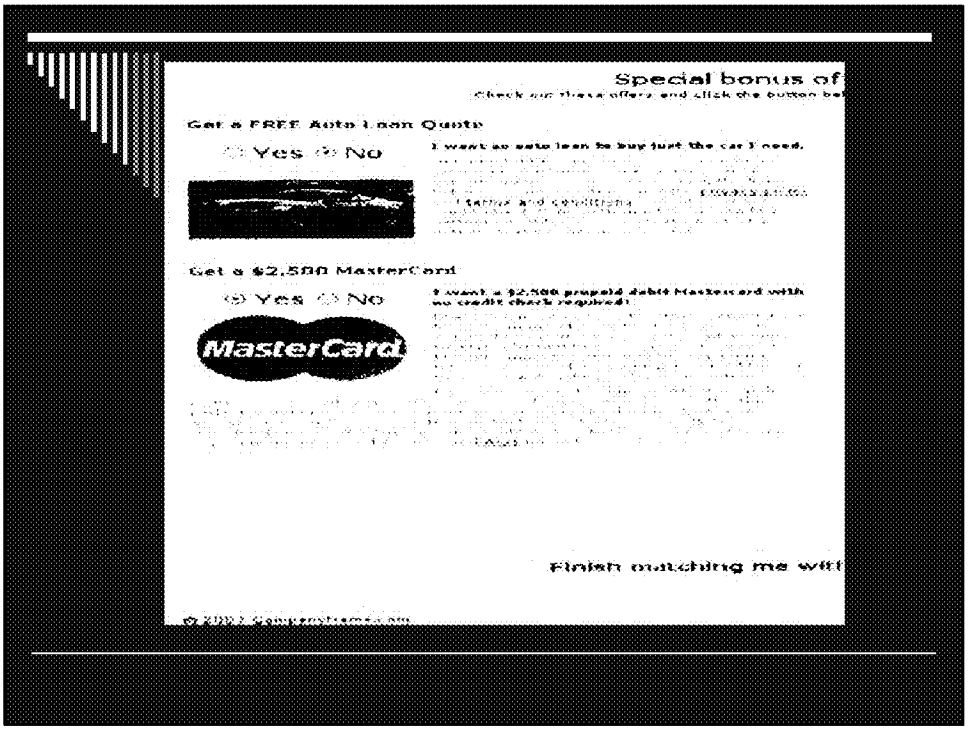
VP
T Bank
Telephone number
E-mail Address

Real-Time Checks Transactions Details

Transaction ID	212765
Timestamp	11/27/2006 4:07:34 PM
Customer ID (old)	0
Order ID (old)	0
Customer ID	65.4.146.169:www.xyz.org:1469
Order ID	rage13_dbl@yahoo.cor
Name On Check	Customer Name
Address Line 1	Customer's Street Address
Address Line 2	
Address Line 3	Customer's city, state
Name of Bank	Bank Name
Bank Address Line 1	

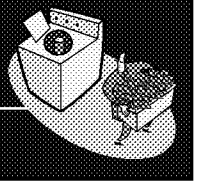
Real-Time Checks Transactions Details Continued

Bank Address Line 2	
Routing Number	Routing Number
Account Number	Account Number
Check Number	9999
Amount	$49.45
Error	☐
Passed	☑
Details	pass
Batch ID	4925
Check ID	354847



BSA/AML Risks

- 31 U.S.C. §§ 5311 et seq. & 31 C.F.R. Part 103
- T Bank Consent Order
- Upstate National Bank Consent Order
- Need for enhanced BSA/AML program that can identify, monitor and address the greater than normal risk posed by payment processor relationships



Legal Basis for Enforcement Actions

- Recklessly engaged in unsafe or unsound banking practices
- Engaged in unfair practices in violation of Section 5 of the FTC Act
- Banks directly liable because "but for" the banks the TPPP and their merchant-clients would not have had access to the payments system

OCC v. Wachovia

- OCC Formal Investigation
- Wachovia-PPC relationship

Wachovia-PPC Relationship

- PPC accounts opened at Wachovia in Philadelphia
- High returns projected
- PPC assurances
  - Strict controls over telemarketers
  - 100% refund policy for consumers who complained
  - Telemarketer calls monitored and recorded
- Deposits began in March 2005
- 1.8 million RCCs totaling $142 million
- 950,000 RCCs returned generating $1.45 million in return item fees for Wachovia

OCC v. T Bank

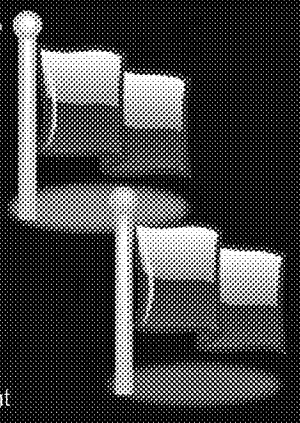
- Giact-referred merchants opened accounts at T Bank into which they deposited RCCs
  - 13 of these merchants engaged in fraud or deceptive practices; some were telemarketers and others were internet merchants
  - First of the 13 merchants opened an account in June 2006
  - At OCC direction, Bank terminated all Giact-related accounts in August 2007
- Genesis--Routine safety and soundness exam found:
  - high return rates
  - inadequate due diligence
  - Lack of monitoring of return rates and reasons for returns
- OCC Formal Investigation

T Bank-Giact Relationship

- Bank focused on the fee income generated by returns
- $22.6 million in RCCs deposited into the 13 merchants' accounts
- $16.6 million of this amount was returned
- $1.95 million in return fees for T Bank

Fraud Warnings at T Bank

- Return rate of over 50%
- High volume of returns as unauthorized, fraud, NSF, and account closed
- Consumer complaints
- Complaints from other financial institutions
- Internal Warnings
- Law Enforcement Inquiries/State AG Complaints or Injunctions
- Types of merchants (check FTC website)
  - merchant finance cards;
  - prepaid debit cards;
  - credit repair companies;
  - travel discount clubs; and
  - telemarketing services/call fulfillment companies



What Went Wrong at Both Wachovia and T Bank

- Inadequate due diligence and underwriting
- Poor risk recognition and response
- Weak controls, policies and procedures
- Inadequate account monitoring
- Inadequate case management tools
- Failure to heed consumer complaints

What Went Wrong at Both Wachovia and T Bank (Continued)

- Policy exception instituted to handle PPC returns
- Poor coordination of internal investigations
- Lack of follow-up on law enforcement inquiries
- Relied on Giact to conduct due diligence on the merchants
- Failure to consider Giact's AML practices
- Ignored information contained in due diligence reports conducted by its outside counsel

Comptroller's Findings in Both Wachovia and T Bank

- Unsafe or unsound banking practices
- Unfair practices in violation of Section 5 of the FTC Act
- Consumers harmed

Enforcement Actions

- Wachovia
  - Over $150 million in restitution to 740,000 consumers
  - $10 million civil money penalty
  - $8.9 million contribution to consumer education
  - Corrective action
- T Bank
  - $5.3 million in restitution to 55,997 consumers
  - $100,000 civil money penalty
  - Corrective action—both a BSA Consent Order and a Consent Order requiring policies, procedures, and controls should the Bank enter into a relationship with an entity that deposits RCCs.

United States of America
v.
Payment Processing Center

A Case Study of Remotely Created Check Abuse and Payment System Vulnerabilities

Joel M. Sweet, Trial Attorney, Consumer Protection Branch, DOJ
(detailed from United States Attorney's Office for the Eastern District of Pennsylvania)

1

Disclaimer

Any opinions reflected in this presentation are those of the presenter and are not necessarily those of the Department of Justice, or any government official, agency, department, or branch.

The information in this presentation is from public sources.

2

Mass Market Consumer Fraud – a National Scourge

Bernie Madoff swindled more than $40B from a select group of mostly wealthy investors.

Fraudsters steal more than $40B from consumers – mostly the elderly and those in the lower middle class – every year!

Which is most likely to receive attention from law enforcement, regulators, and the press: a single theft of $100 million, or one million thefts of $100?

3

Common Methods of Payment System Abuse

- Debit transactions originated by payment processors and banks on behalf of telemarketing and Internet fraudsters
- Phone company bills used to originate unauthorized charges ("cramming")
- Mortgage payment mechanisms used to originate unauthorized charges

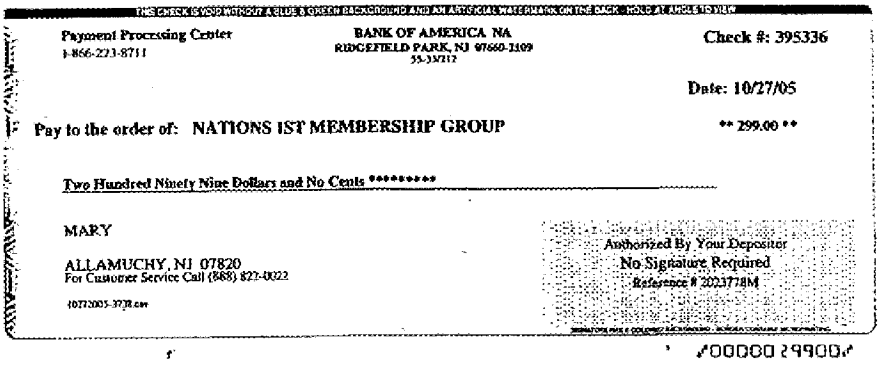
4

Law Enforcement Challenges to Prosecuting Telemarketing/Internet Fraud

- Jurisdictional limitations (state and international)
- Fraudsters change corporate identities and law enforcement plays "whack-a-mole"
- Victims are dispersed geographically
- Victims cannot identify fraudsters – no face-to-face contact
- Plausible deniability – cross-pointing among call centers, mail houses, fulfillment centers, payment processors, and banks
- Limited investigative and prosecutorial resources
- Limited reach of State Attorneys General and FTC

5

A Remotely Created Check ("RCC")



Payment Processing Center
1-866-223-8711

BANK OF AMERICA NA
RIDGEFIELD PARK, NJ 07660-2109
55-337212

Check #: 395336

Date: 10/27/05

Pay to the order of: NATIONS IST MEMBERSHIP GROUP

** 299.00 **

Two Hundred Ninety Nine Dollars and No Cents ********

MARY

ALLAMUCHY, NJ 07820
For Customer Service Call (888) 822-0022

Authorized By Your Depositor
No Signature Required
Reference # 20237788

⑈000029900⑈

6

RCC Fraud: Well-Known to Banks

"Demand drafts can be misused to commit check fraud. This practice involves the misuse of account information to obtain funds from a person's bank account without that person's signature on a negotiable instrument. . . **demand drafts have been used by deceptive telemarketers who obtain bank account information and withdraw unauthorized funds from consumers' bank accounts**, without their realizing that such withdrawals are occurring. . . ."

A Guide to Checks and Check Fraud, published by **Wachovia**, 2003

7

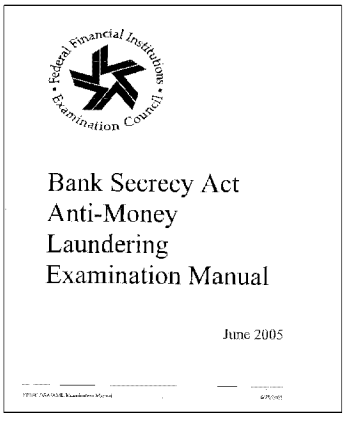
RCC Fraud: Well-Known to State Law Enforcement and FRB

- In 2005, 35 state attorneys general jointly request that the Federal Reserve ban RCCs from the payments system:
  - "demand drafts are frequently used to perpetrate fraud on consumers"
  - "such drafts should be eliminated" in favor of other forms of payment
  - If not eliminated, mandatory marking of RCCs and other measures to protect consumers

8

RCC Fraud: Well-Known to Bank Regulators

BSA/AML Examination Manual (FRB, FDIC, NCUA, OCC, and OTS)

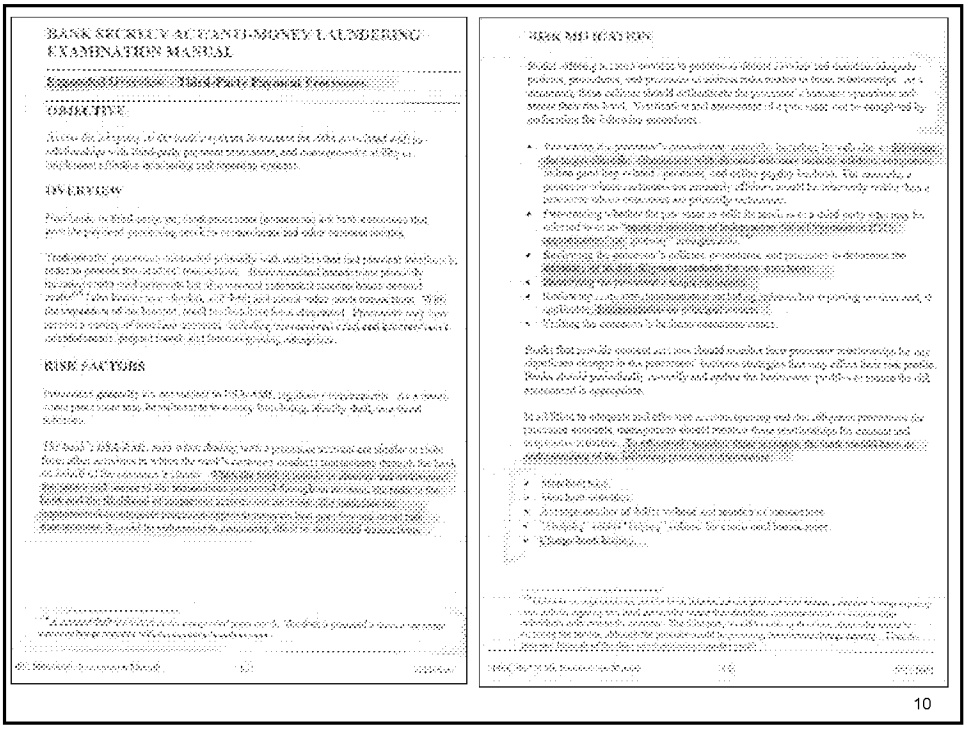


Federal Financial Institutions Examination Council

Bank Secrecy Act
Anti-Money
Laundering
Examination Manual

June 2005

9



BANK SECRECY ACT/ANTI-MONEY LAUNDERING
EXAMINATION MANUAL

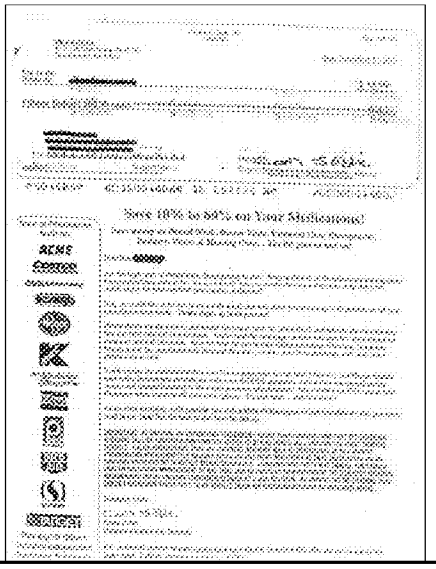
OBJECTIVE

OVERVIEW

RISK FACTORS

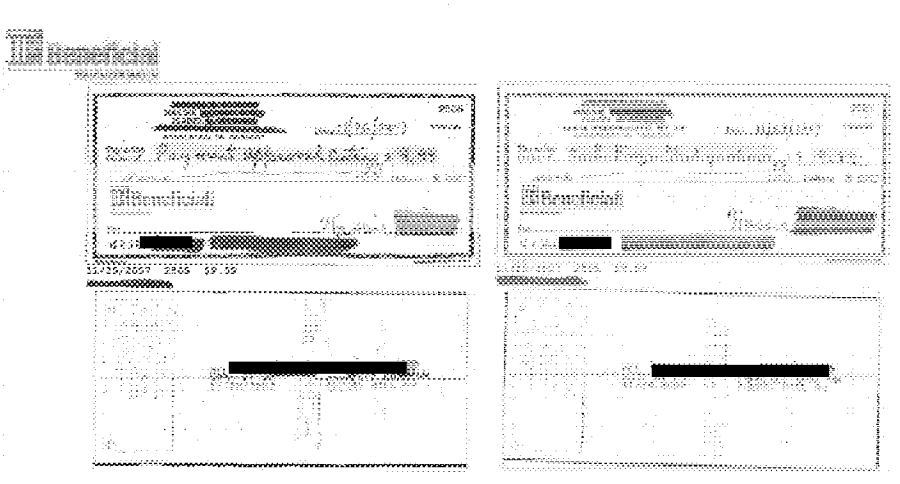
10

Incentives to Induce Authorization

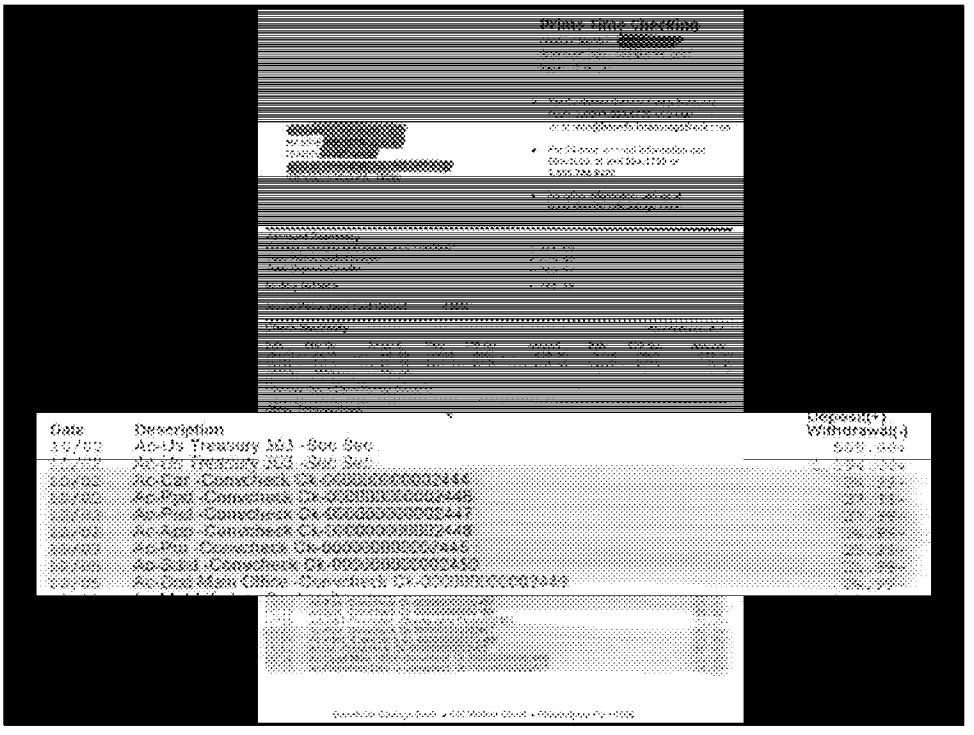


11

Incentives for Purported Authorization



12



From Target Gift Card to Automated Electronic Mortgage Payment

WACHOVIA

MORTGAGE STATEMENT

ACCOUNT INFORMATION:
Statement Date: 10/05/06
Loan Number:
Interest Rate: 5.9500
NEXT PAYMENT DUE DATE: 11/01/06
Current Payment: $949.28

Philadelphia PA 19144-5725

Property Address:
PHILADELPHIA PA 19144

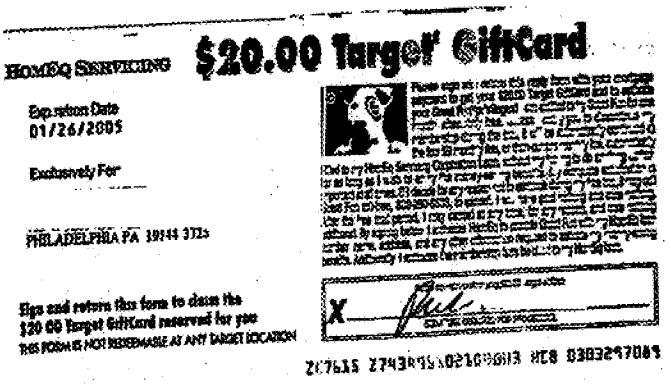
Activity Since Your Last Statement:

Date	Description	Principal	Interest	Escrow	Other	Total
08/01	Payment	$176.59	$764.69		$9.00	$949.28
09/01	Payment	$176.49	$763.92		$9.00	$949.28
10/02	Payment	$177.55	$762.83		$9.00	$949.28

Account Summary:
Loan Balance* As of 10/05/06
Interest Paid Year to Date
Escrow Balance As of 10/05/06
Escrow Paid Year to Date

14

Incentives to Induce Authorization


HOMEQ SERVICING

$20.00 Target GiftCard

Expiration Date
01/26/2005

Exclusively For

PHILADELPHIA PA 19144 3725

Sign and return this form to claim the $20.00 Target GiftCard reserved for you
THIS FORM IS NOT REDEEMABLE AT ANY TARGET LOCATION

X

15

Payment Processing Center, LLC

- Provides "end-to-end solutions" for telemarketing merchants
- Specializes in "Bank Draft origination for telephone **transactions that may be prohibited**" by NACHA rules

16

[illegible]justin@paymentprocessingcenter.com
00000C353
[illegible]
To the fine people that made hellish phone abuse a little more bearable,

. I am glad to have shared the daily death-threats, hate-filled rants, and ignorance with all of you. I think sometime in the next couple weeks I may almost (in some kind of sick way) miss the sound of shit-kickers screamed obsenities over the verification playback.

bacon-speckled tomato soup, dealt with a phonebook's worth of customer callbacks, and a lot of soggy bread from the sandwich club.
When you come into work on Monday don't be sad that my cute little ass isn't around, be happy... because finally one of us will get to know what daylight

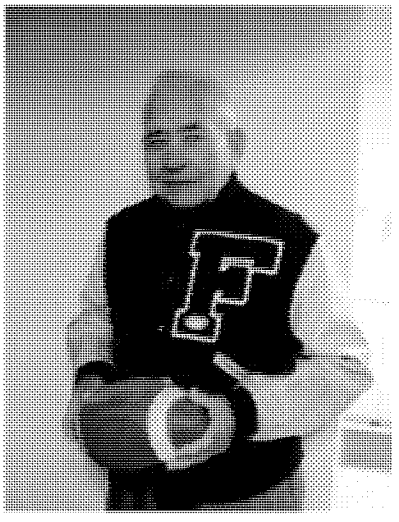
I know the customer service number and I'm not afraid to call with my bank rep on the line)

Now, as I hang up my Steno Pad and descend back in to a world of relative normality I would like to say THANK YOU to everyone.

Side note to Michael: How much exactly do I owe you for the knowledge that it takes a total of 16 combined brain cells and teeth to provide your bank account information to a stranger on the phone to order something with as stupid a name as Washballs? or; the knowledge that old people are just plain easy to trick?

stay in touch,
Justin

Purported Authorization Obtained By Telemarketer



David XXX, Sr.
1933-2006

University Football Coach

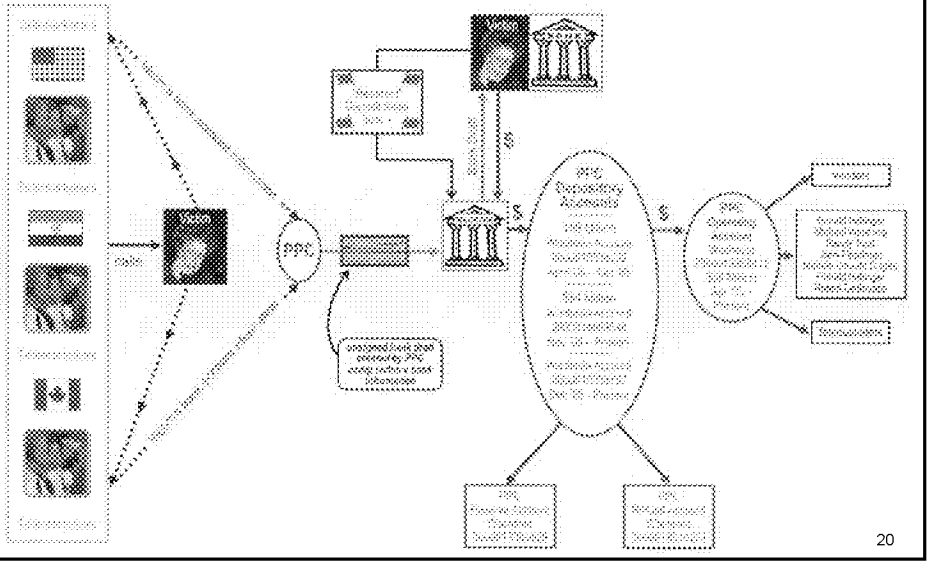
Little League Coach

Sunday School Teacher

Husband, Father, Grandfather, Brother

19

The Payment Process



20

A Mutually Profitable Relationship!

Dollar value of RCCs deposited by PPC with Wachovia in 12-month period: **$162,000,000**

Income from RCC fees:

PPC – **approx. $8,000,000**
Bank – **approx. $1,900,000**

21

Wachovia: Victim or Participant?

- Knew or remained willfully blind to fact that PPC serviced mass market fraudsters
- Ignored glaring red flags
- Suppressed internal concerns
- Ignored express warnings from other banks
- Entered agreements with PPC to protect its own interests at the expense of the interests of other banks and their customers

22

Failure in Due Diligence
PPC's Telemarketing Merchants

- Facially suspicious product offers and marketing scripts
  - Grant offers
  - Prescription discount cards
  - Travel Programs
  - Free Gift Cards
  - Free Computers
- Merchants mostly based overseas and/or using foreign banks
- Exploited names of legitimate companies, such as Wal-Mart, K-Mart, Home Depot, Carnival Cruises, AIG

23

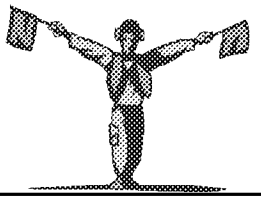
Eyes Wide Shut

- PPC merchants were fraudsters well-known to Better Business Bureaus, state Attorneys General, and consumer protection websites
  - Star Communications
  - Advantage America
  - Suntasia
- As successive payment processers were shut down by law enforcement, Wachovia continued to process RCCs for same fraudulent merchants

24

Returns – Charge Backs

- At inception, Wachovia **anticipated returns exceeding 35 percent** (compared to approximately 1/2 of 1 percent for all checks)
- Actual returns exceeded **50 percent**
- Wachovia charged PPC substantial fee for returns
- Wachovia offered PPC volume discounts on return fees

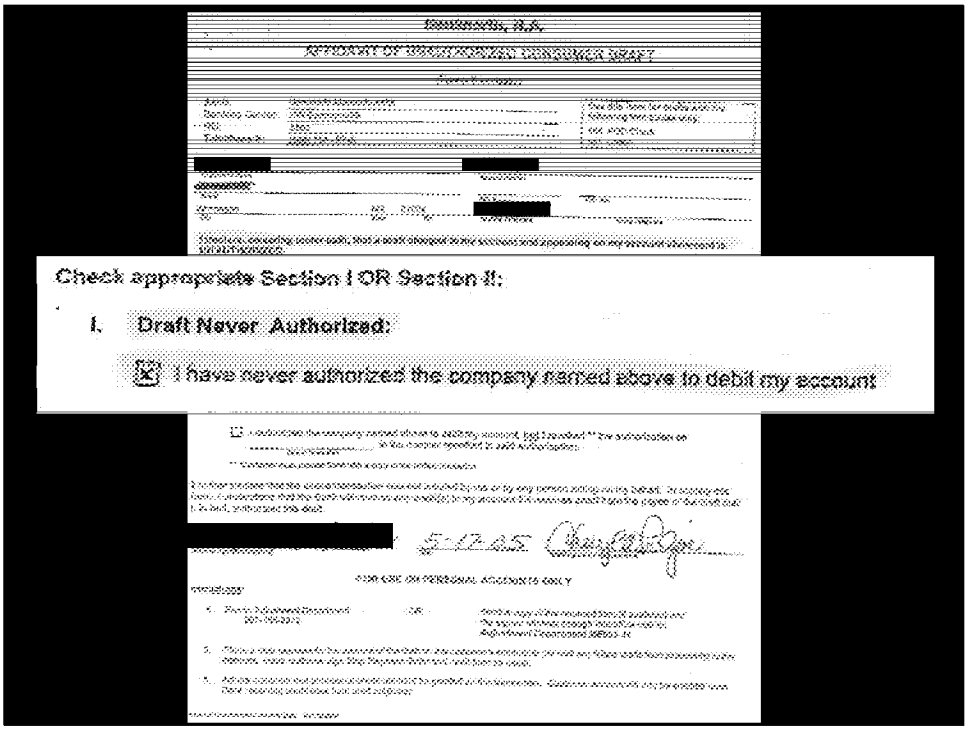


25

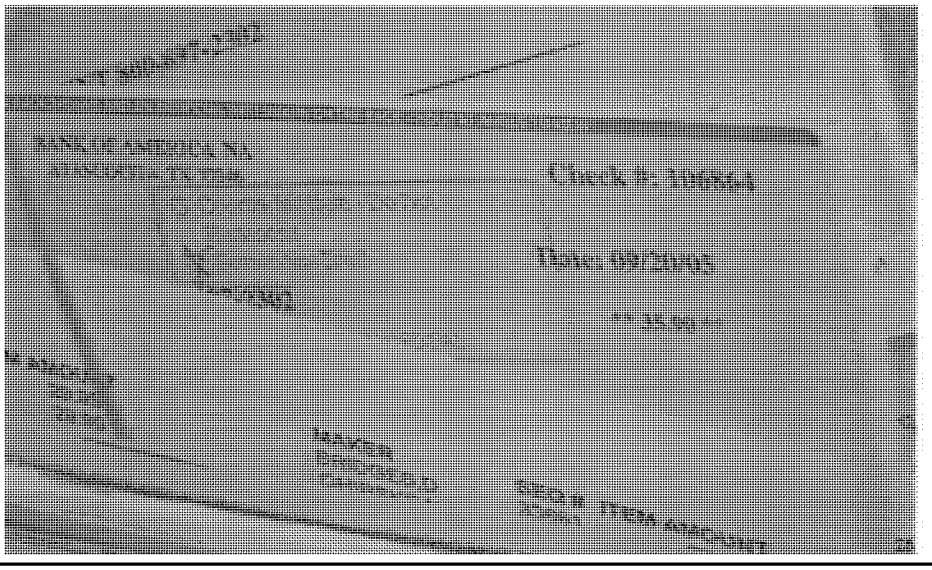
Return Reasons

- More than 50 percent of PPC's returns facially identified as:
  - UNAUTHORIZED
  - FRAUD
  - REFER TO MAKER
- Every month Wachovia received and hand-processed thousands of **sworn affidavits from consumers alleging that PPC debit transactions were not authorized**

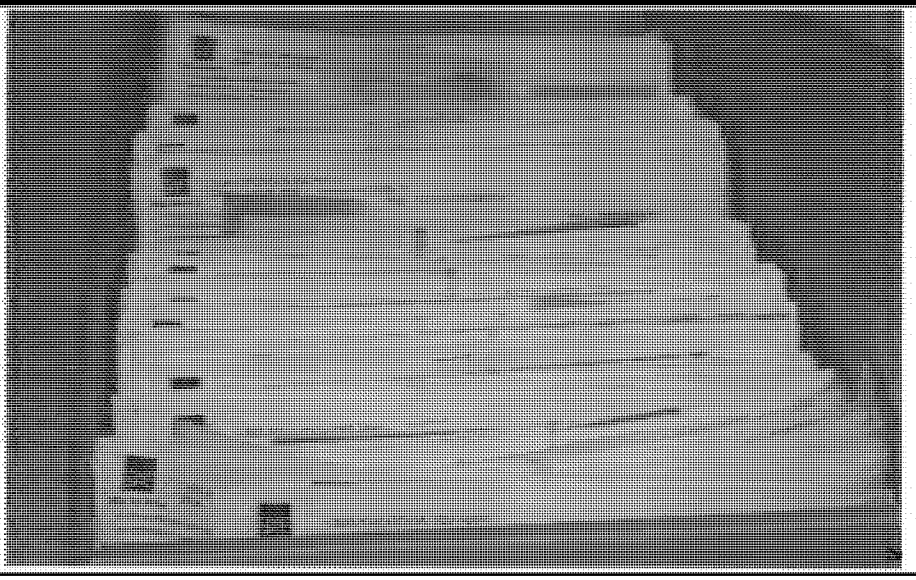
26



A Returned Item



A Box of Returned Items



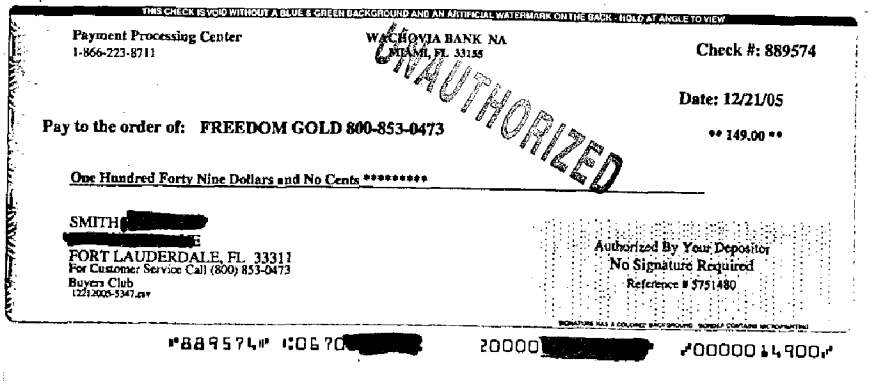
A Room of Boxes of Returned Items

Outlier Business Practices

- PPC regularly transferred large amounts of money to overseas accounts.
- Wachovia allowed PPC to deposit RCCs payable to third-party merchants into its own accounts – without agency agreements.
- The Wachovia/PPC business model was based on large volumes of returns – an ordinarily suspect and undesired result.
- Wachovia's own customers often treated differently than other banks' customers.

31

"On the House" Returns


THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK - HOLD AT ANGLE TO VIEW

Payment Processing Center
1-866-223-8711

WACHOVIA BANK NA
MIAMI, FL 33135

Check #: 889574

UNAUTHORIZED

Date: 12/21/05

Pay to the order of: FREEDOM GOLD 800-853-0473

** 149.00 **

One Hundred Forty Nine Dollars and No Cents *********

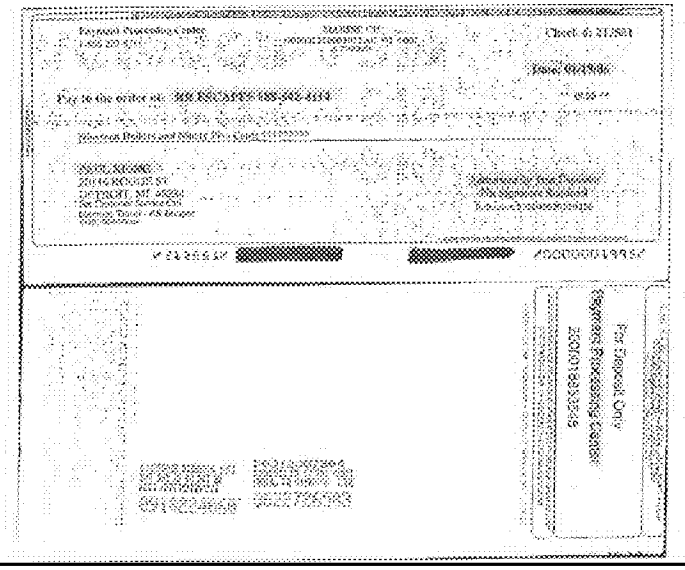
SMITH [redacted]
[redacted]
FORT LAUDERDALE, FL 33311
For Customer Service Call (800) 853-0473
Buyers Club
1221200833347.csv

Authorized By Your Depositor
No Signature Required
Reference # 5751480

"889574" :0570[redacted] 20000[redacted] "000001 4900"

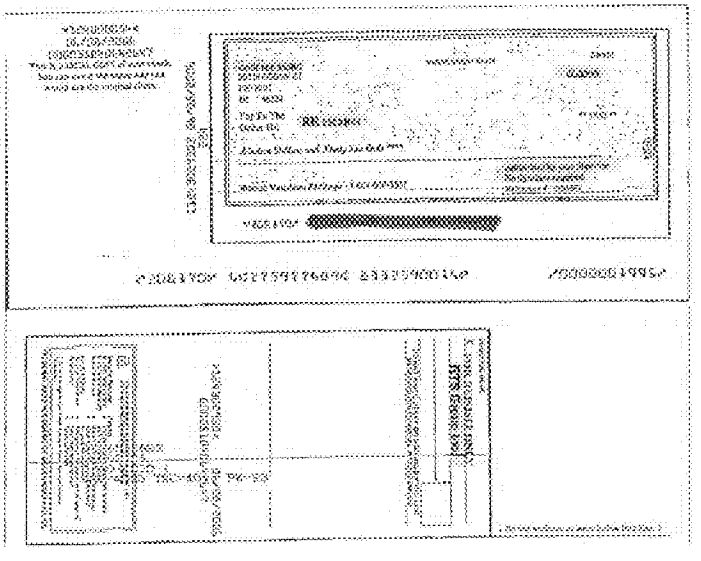
32

"Whack-a-Mole"



33

Migration from National Bank to Community Bank



34

Wachovia Ignored Internal Concerns

Return "volumes are tremendous" and "payment of these items is not our normal process"

Returns Operations Supervisor to VP of Loss Management

"Nothing [PPC] could ever do would make me comfortable . . ."

Bank Loss Management Official after learning about Bank relationship with PPC

After Loss Management official recommended closing PPC accounts, wrote "business line has assumed risk for the customer and decided to keep their accounts open"

Communication between Bank Loss Management Officials

35

Wachovia Ignored Internal Concerns

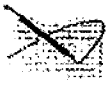
"Please consider the regulatory and reputational risks involved here. **We have now been put on notice that accounts at [Bank] are being used . . . to further these schemes.**

"If PPC has in place 'a standing agreement with [Bank] to pay all claims without dispute,' then they know they have rogue telemarketers in their customer base."

Internal E-mail from Bank's In-house Counsel after receiving fraud warning from another bank

36

DOUBLE YIKES!!!!



08/23/2005 05:35 PM

To
cc
Subject Guardian Marketing # 2000027007068

Tom,
Bob, Tim & I need to huddle with you on this account relationship. It is a Business Banking account. It has been actively making deposits since 6/23/05 and there is a current balance of $743,000+ in the account. The account came to us from B of A (so we are advised by) in Bus. Bnkg.) and she is

ALL their deposits are THIRD PARTY DRAFTS!!! DOUBLE YIKES!!!!

YIKES!!!! Moreover, the drafts that are being deposited and are charging back, are not $99.99; these items are all over the place in terms of their amount. Moreover, there is another account, Suntasia, #2000027027721. Same address, same principals. $ from the Guardian acct is transferred to Suntasia and then the $ is wired out to Bank of America (funny, I thought I said they were leaving B of A at the beginning of this note, didn't I?!). And, there is more, but nothing more that I want to put into a note. Bob and I really need to talk o you on tomorrow.

Thanks,

37

Wachovia Ignored Explicit Fraud Warnings From Other Banks

"The purpose of this message is to **put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam . . .** instigate an investigation into whether [PPC is] conducting legitimate business and whether [Bank is] getting **a high volume of return items on those accounts (that should place your bank on notice of potential fraud).**"

E-Mail from Citizens Bank

38

Bank's "Oral Agreement" With PPC To Pay All Returns

- Intended to protect Bank's reputation rather than consumers

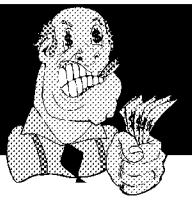
"[I]f we can find a way to pay the returns . . . without sending them back to other banks, I think that will go a long way to preserve our reputation. **The sooner the complaint gets paid the quicker it goes away."**

Internal Bank e-mail

- Demonstrates that UCC warranty rule is not an effective anti-fraud tool

39

Money Motivates



"[P]lease mark your calendar – we will take them somewhere nice for lunch. We are making a ton of money from them."

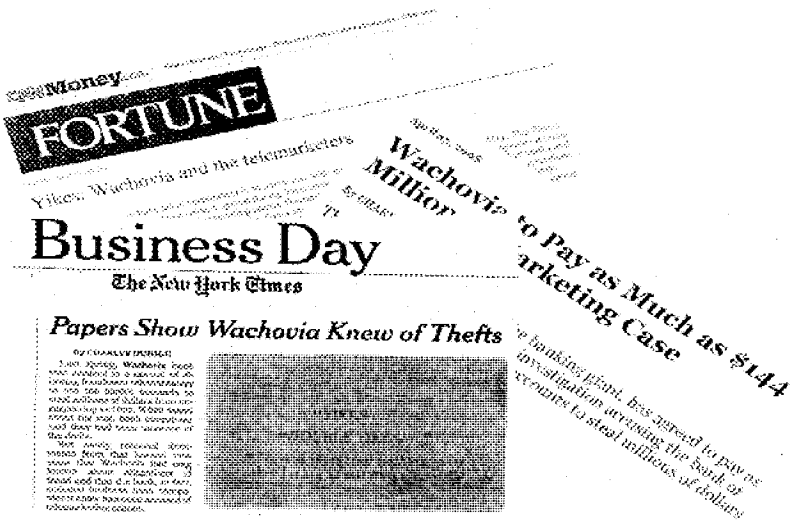
Bank Relationship Manager to Senior Business Development Officer

"[T]his is our most profitable account. $1mm per year in profit. They have asked for Eagle tickets. What can we do?? They deserve them with all we make from them."

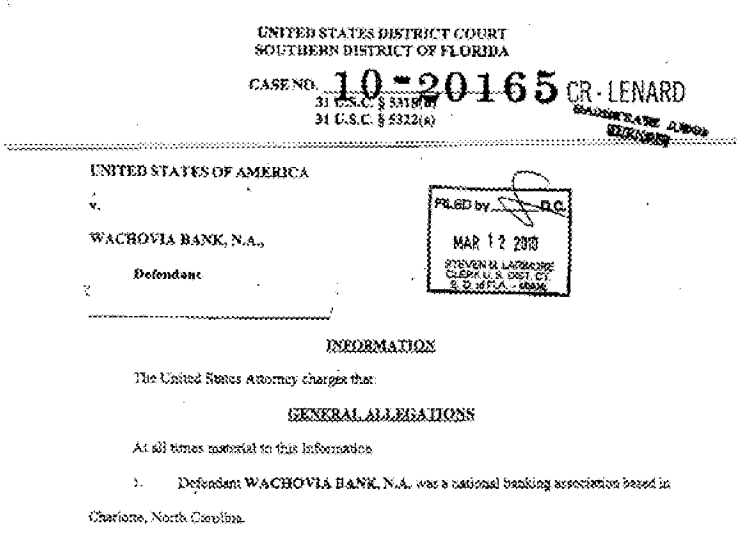
Bank Relationship Manager to Senior Business Development Officer

40

What's a reputation worth?



Yes – it *is* a crime.



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 10-20165 CR-LENARD

31 U.S.C. § 5318(h)
31 U.S.C. § 5322(a)

UNITED STATES OF AMERICA

v.

WACHOVIA BANK, N.A.,

Defendant.

FILED by D.C.
MAR 12 2010
STEVEN M. LARIMORE
CLERK U.S. DIST. CT.
S. D. of FLA. - MIAMI

INFORMATION

The United States Attorney charges that:

GENERAL ALLEGATIONS

At all times material to this Information:

1. Defendant WACHOVIA BANK, N.A. was a national banking association based in Charlotte, North Carolina.

42

It's not over until it's over.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA : CRIMINAL NO. 11-

: DATE FILED: February 16, 2011

v. : VIOLATIONS:

DONALD HELLINGER : 18 U.S.C. § 371 (conspiracy – 1 count)
RONALD HELLINGER : 18 U.S.C. § 1960 (operating an illegal money transmission business – 1 count)
MICHAEL WEISBERG : 18 U.S.C. § 1955 (operating an illegal gambling business – 1 count)
RANDY TROST : 18 U.S.C. § 1084 (transmission of wagers and wagering information – 8 counts)
JAMI PEARLMAN : 18 U.S.C. § 1956(a)(1)(A)(i) (international money laundering – 3 counts)
MICHELE QUIGLEY : Notice of forfeiture

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES THAT:

At all times relevant to this Indictment:

BACKGROUND

1. Defendants DONALD HELLINGER, RONALD HELLINGER, MICHAEL WEISBERG, RANDY TROST, JAMI PEARLMAN, and MICHELE QUIGLEY

Financial accountability -- thanks to federal agents, prosecutors, and bank regulators, class action attorneys, local and state law enforcement, *The New York Times*, and many determined victims of consumer fraud !

A simple proposition.

Mass-market scammers need access to payment systems (RCC's, ACH, CC) to take consumers' money. Without bank access there are no unauthorized withdrawals.

Banks are stationary (no "whack-a-mole"), regulated, and are concerned about reputational risk.

Banks already are required to have systems in place to prevent criminals from accessing the banking system.

Cutting off the scammers' access to the payment systems is relatively efficient and fast, and protects consumers prospectively as we investigate.

45

Important steps forward . . .

- Guidance to banks from FDIC, OCC and FinCEN
- United States v. First Bank of Delaware
- Financial Fraud Enforcement Task Force/Consumer Protection Branch efforts to choke-off fraudsters' access to payment systems (DOJ, FTC, FDIC-OIG, USPIS, FBI, and others)
- May 21, 2013: FTC Notice of Proposed Rulemaking would ban the use of RCCs in connection with telemarketing

46

Operation Choke Point
So far . . .

- More than 50 subpoenas issued to banks and TPPPs.
- Several active criminal and civil investigations.
- Banks are self-disclosing problematic TPPP relationships.
- Banks are terminating TPPP relationships and scrutinizing scammer relationships.
- Internet Payday lending – collateral benefits.
- Investigative support from USPIS, FBI, SIGTARP, USSS

47

Regulatory Loophole

- Treasury Department regulation amended in 2011 arguably excludes third-party payment processors from the definition of "money transmitter" and thus is not a Money Services Business ("MSB").
- **A payment processor that originates tens of millions of dollars of debit transactions against consumers' bank accounts on behalf of Internet and telemarketing merchants may not be an MSB and may not be required to register with FinCEN or comply with the BSA.**

48

Thanks for your time and interest!

Questions?

Joel M. Sweet

[redacted]@usdoj.gov

49

From: Olin, Jonathan F. (CIV)
Sent: Thursday, September 26, 2013 9:59 AM
To: Price, Allison W (OPA)
Subject: RE: American Banker

Tracking:

Recipient	Read
Price, Allison W (OPA)	Read: 9/26/2013 9:59 AM

Thanks. I had not seen this.

From: Price, Allison W (OPA)
Sent: Thursday, September 26, 2013 9:44 AM
To: Olin, Jonathan F. (CIV)
Subject: FW: American Banker

Hey – in case you missed this:

From: Sweet, Joel
Sent: Wednesday, September 25, 2013 11:11 PM
To: Blume, Michael S.; Frimpong, Maame Ewusi-Mensah (CIV); Goldberg, Richard; Blume, Michael S.; [redacted] Jenkins, Adora (OPA); Price, Allison W (OPA)
Subject: American Banker

All –
Here is the latest. Overall, the reporter got it right and was fair, although we might quibble at the margins. The electronic version has a headshot of Bresnick with a caption that includes his quote emphasizing that our efforts are aimed at fraud – not a particular industry. Allison/Adora, great idea to provide the reporter with the paragraph we worked up previously. It is well integrated into the story. Also, the inclusion of the NACHA return averages (Bresnick?) is excellent, as it illustrates why our threshold for identifying potential fraud is reasonable. The bankers will understand.
JMS

http://www.americanbanker.com/issues/178_186/banks-pressured-to-settle-in-online-lending-probe-1062408-1.html

Banks Pressured to Settle in Online Lending Probe

by Kevin Wack
SEP 25, 2013 4:27pm ET

The Justice Department is pressuring banks under investigation for their ties to online lenders to reach a settlement soon, according to four industry sources familiar with the matter.

The investigation concerns electronic payments that banks process for online lenders suspected of fraudulently accessing their customers' bank accounts.

Roughly 50 banks and third-party payment processing firms have received subpoenas from the Justice Department, according to sources. The Justice Department's strategy is to reach a settlement in the coming weeks with one of the banks and then to use the terms of that agreement as a template in talks with other banks, the sources said.

A Justice Department official declined to comment on settlement talks. But the official said that the department's investigation — first disclosed publicly in March — has had an "immediate effect" on the ability of certain lenders to access customer funds through the banking system. The DOJ says it is zeroing in only on fraudulent online lenders, though many in the banking and payment-processing industries take issue with that characterization.

"Banks are lining up to self-disclose wrongdoing to DOJ and have proactively cut off their relationship with suspect payment processors," the Justice Department official said. "As a result, legitimate payment processors are volunteering to stop processing debits against consumers' bank accounts on behalf of scammers. The banks are being forced to look closely at relationships and their own business conduct."

"The banks we are investigating are represented by many of country's leading law firms, and news of our investigations is beginning to drift into the industry conversation," the Justice Department official said. "The system is working, and as a result, banks are cutting off processors, processors are cutting off scammers, and scammers are starting to get desperate for a way to access consumers' bank accounts."

The Justice Department's investigation of online lenders and their access to customers' bank accounts is part of a broader effort by the department to crack down on mass-market consumer fraud, including Medicare scams, Internet pharmacy scams, and others.

The DOJ effort also comes at a time when the Federal Deposit Insurance Corp. has stepped up its scrutiny of banks that process payments for online lenders. Both the Justice Department and the FDIC are members of the Financial Fraud Enforcement Task Force, which has played a role in coordinating related efforts by different federal agencies.

In a March speech, Michael Bresnick, who was then the task force's executive director, detailed its efforts with respect to online lending. One issue that he flagged was whether specific online lenders are violating the laws of the states where their customers live.

"Understandably, it may not be so simple a task for a bank to determine whether the loans being processed through it are in violation of the state law where the borrower resides," Bresnick acknowledged, before adding: "Yet, at a minimum, banks might consider determining the states where the payday lender makes loans, as well as what types of loans it offers, the APR of the loans, and whether it make loans to consumers in violation of state, as well as federal, laws."

The relevant legal issues are complicated by the fact that many online lenders — a category that includes both payday lenders and installment lenders — maintain they are not required to hold licenses in every state in which their borrowers live.

Online lenders that are making such legal arguments include, but are not limited to, firms owned by Indian tribes. Firms owned by tribes maintain they are not subject to state law because of tribal sovereignty. Many online loans are so expensive that the companies making them would be unable to get licensed in states with strict caps on interest rates.

Under the proposed settlement terms being shopped by the Justice Department, a subpoenaed bank would agree to stop processing certain types of payments and pay a fine, according to the four industry sources.

Some of the sources said that additional settlement terms are possible: an independent review to ensure that the bank remains in compliance with the settlement's terms, a stipulation to a set of facts that could then be used in future civil litigation against the bank, or both of those provisions.

Many of the banks that have received subpoenas are small institutions, but some large banks have gotten them as well, sources said.

One implication that banks are taking from their talks with the Justice Department, according to sources, is that banks that reach a settlement sooner will get a better deal than those that wait.

So far, the only bank to acknowledge publicly that it has come into the Justice Department's crosshairs is the $342 million-asset National Bank of California in Los Angeles. In a Sept. 16 press release, the bank disclosed that its $25 million recapitalization is contingent on resolving pending inquiries by the DOJ related to its relationships with companies that may have processed payments for payday lenders.

In a brief interview last week, National Bank of California President Henry Homsher said that he was working to reach a settlement, but declined to comment further.

In settlement talks between banks and the Justice Department, one key issue will be the breadth of the language barring the bank from processing certain payments. Some online lenders are licensed in every state in which their borrowers reside, so there is no ambiguity about the legality of their businesses.

"I think it's important to note that this is at base an attack on fraudulent conduct," says Bresnick, who recently left the Financial Fraud Enforcement Task Force and is now in private law practice in Washington, D.C. "It's not an attack on an entire industry."

But officials in the banking industry as well as at third-party payment processors are chafing at the Justice Department's methods for ferreting out fraud.

The DOJ has established the following benchmark, according to numerous sources: a specific merchant, such as an online lender, that has at least a 3% return rate on electronic transactions, should raise a red flag for the bank. In other words, the Justice Department is telling banks to be wary of online lenders if at least 3% of their requests to withdraw cash from a customer account get returned. The return rate for all electronic payments was just under 1% in 2012, according to Nacha, the bank-owned group that runs the ACH network.

Officials in the banking and payment processing industries argue that a 3% threshold is too low because a returned transaction does not necessarily mean the lender was making an unauthorized withdrawal.

For example, the return rate includes instances where the customers do not have sufficient funds in their accounts — a situation that likely happens more frequently with high-interest rate online loans than for many other forms of online commerce, because the loans tend to go to cash-strapped consumers.

Using a 3% return rate as a threshold is "ridiculous," argues Marsha Jones, director of the Third Party Payment Processors Association, which was formed last month in response to the heightened regulatory scrutiny of the industry. "It's just not something that supports evidence of fraud."

But Bresnick, the former head of the financial fraud task force, says that elevated return rates are "a significant red flag," and that even high return rates that stem from the depositor having insufficient funds can be an indication of fraud.

From: Blume, Michael S.
Sent: Tuesday, October 01, 2013 10:55 AM
To: Frimpong, Maame Ewusi-Mensah (CIV)
Subject: TPPP

Maame

FYI – Rich, Joel, and I had a conversation about following up on Stuart's suggestions from last night. I'm happy to discuss in more detail, but the short of it is that they are already where Stuart wants them to be (i.e., pushing for the alternative, non-specific language rather than the specific language on payday lending). There are some nuances that we need to think through, which we are doing. For example, some proposals to banks have included specific bans doing business with debt relief companies, foreclosure rescue companies, and credit repair companies, and finding alternative, non-specific language presents unique challenges.

Mike

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Wednesday, October 02, 2013 2:13 PM
To: Delery, Stuart F. (CIV); Olin, Jonathan F. (CIV)
Subject: 3PPP

Hi –

I spoke to Mike about doing a team meeting next week. He agrees with me that it would be helpful to convey to the team your continued support for the initiative in spite of the recent press and Hill interest and to emphasize your vision for what the focus and scope should be (and accordingly, the tone and content of communications). When Jon returns, we can look at what works in terms of schedule (preferably not Monday for me).

With respect to the resolutions currently being negotiated, Mike conferred with the team, and they are on the same page with you with respect to alternatives to a blanket prohibition on working with a certain type of merchant. They included the alternative you saw for that reason, and are very much supportive of using that approach as opposed to the blanket approach. They are discussing how to make such an alternative work for the other industry areas they are concerned about (i.e., debt collection, where they had contemplated a blanket prohibition). Hopefully, we can discuss/brainstorm this further when we meet.

Thanks!
Maame

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Thursday, October 24, 2013 3:32 PM
To: Thompson, Karl (OAG); Martinez, Brian (OAAG); Taylor, Elizabeth G. (OAAG); Starks, Geoffrey (ODAG); Jacobsohn, Robin (ODAG)
Cc: Olin, Jonathan F. (CIV)
Subject: third-party payment processor initiative
Attachments: 131024_bankinregulators_paymentprocessing_letter.pdf

Hi –

You have heard me report on our successful third-party payment processor initiative, and on the press reports and Hill inquiries about it. (We are still planning to give you a short informal briefing on the initiative, and hope to schedule it soon.)

Today, several consumer groups (including the National Consumer Law Center, the Center for Responsible Lending, and the Consumer Federation of America) have written a letter and issued a press release to thank several agencies (including DOJ) for our work on safeguarding the payment system. The letter also urges us to continue our efforts, and to look at the check system as well. The groups plan to send the letter to House Financial Services and Senate Banking as well. Please see attached the letter.

To date, the consumer groups have not commented on our efforts, making today's letter, press release, and Hill outreach very positive and welcome. (I will note that The Department does not necessarily agree with their analysis of the tribal sovereignty questions concerning tribally-affiliated online lenders. We have shared it with our colleagues in OTJ and elsewhere who have equities in this.)

Thanks for the continued support and interest.

Regards,
Maame

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

October 24, 2013

The Honorable Benjamin Bernanke, Chairman
Board of Governors of the Federal Reserve System
20th Street and Constitution Ave., NW
Washington DC 20551

The Honorable Richard Cordray, Director
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

The Honorable Tom Curry, Comptroller
Office of the Comptroller of the Currency
250 E Street SW
Washington, DC 20219

The Honorable Martin Gruenberg, Chairman
Federal Deposit Insurance Corporation
550 17th Street Northwest
Washington, DC 20429

The Honorable Eric Holder
Attorney General of the United States
Department of Justice
950 Pennsylvania Ave
Washington, DC 20530

The Honorable Debbie Matz, Chairman
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428

The Honorable Edith Ramirez, Chairwoman
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20530

Dear Chairman Bernanke, Director Cordray, Comptroller Curry, Chairman Gruenberg, Attorney General Holder, Chairman Matz and Chairwoman Ramirez,

The undersigned organizations write to thank you for your efforts to date and to urge you to take further strong action to protect consumers and the integrity of the payment system by stopping depository institutions and payment processors from facilitating electronic payments for illegal transactions, including illegal payday loans. Numerous regulatory and court actions have highlighted the crucial role that banks and payment processors play, intentionally or unintentionally, in processing illegal payments for internet and telemarketing scammers, debt settlement companies, payday lenders and others. We appreciate the efforts of your agencies. We encourage you to continue to closely monitor payments networks in order to identify those merchants that operate outside of the law and rely on access to consumers' bank accounts to extract payments. Regulatory scrutiny of those who process payments for higher-risk merchants is necessary, not only to address the direct harm imposed upon consumers by the

illegal transaction, but also to reduce the legal and reputational risks to insured depository financial institutions, consistent with longstanding supervisory expectations.

The payment system is crucial to a wide variety of unscrupulous, higher-risk merchants

Higher-risk merchants that extract unauthorized, abusive or illegal payments raise numerous consumer protection concerns. As many of these high-risk merchants expand to the internet, they increasingly rely on payment processors and originating depository financial institutions (ODFIs) to access consumers' bank accounts. The payment processor and the ODFI enable a payment to be debited from a consumer's account through the automated clearinghouse (ACH) system, a remotely created check (RCCs) or remotely created payment order (RCPOs).

High-risk merchants perpetrating fraud are subject to legal action. But the responsibility does not stop there. Recognizing that fraudsters need help in accessing the payment system, over the last several years regulators have held that payment processors and ODFIs are responsible for managing legal and reputational risk by closely monitoring the activities of their clients. In extreme cases, when the payment processor or ODFI is reckless or even complicit, they may themselves be subject to legal action. Enforcement actions against payment processors or ODFIs by financial services regulators in recent years have involved abuse of the payment system to perpetrate fraud involving vulnerable seniors,[1] telemarketing scams,[2] internet schemes to extract payments for unwanted goods and services,[3] illegal debt settlement fees,[4] and other fraudulent activity. While many high-risk merchants may evade enforcement of consumer protections or be judgment proof, cracking down on those who abet illegal conduct is essential to protecting consumers, preventing abuse of the payment system and shielding financial institutions from legal and reputational risk.

Payment processors and depository financial institutions should not facilitate illegal loans

Online payday lenders are particularly high-risk merchants. These lenders typically market and originate loans to borrowers that reside in another state. Non-depository entities such as payday lenders must follow the law of the state where the consumer is located. Payday loans and other forms of high-cost lending are illegal in many states, and are legal in other states only if the lender is licensed and the loan complies with state consumer protection and other laws.[5]

Online payday lenders present different legal and consumer protection challenges than storefront high-cost lenders. These online lenders routinely market and originate loans with terms and conditions that violate the law of the state where the borrower resides. These lenders are regularly subject to investigation by state and federal officials and have been subject to numerous cease and desist orders and other enforcement actions.[6] Financial institutions that process payments for lenders operating illegally or subject to ongoing litigation are exposed to significant legal and reputational risk.

---

[1] *See* OCC Consent Order for a Civil Penalty, In re Wachovia Bank, 2008-027 (Apr. 24, 2008).
[2] Reyes v. Zion Nat'l Bank, 2012 WL 947139 (E.D. Pa. Mar. 21, 2012).
[3] *See* Complaint for Injunctive and Other Equitable Relief, FTC v. Landmark Clearing, Inc., et al., No. 4:11-cv-00826 (E.D. Tex. Dec. 15, 2011), available at www.ftc.gov/os/caselist/1123117/index.shtm
[4] *See* CFPB, Press Release, CFPB Takes Action Against Meracord for Processing Illegal Debt-Settlement Fee (Oct. 3, 2013), available at http://www.consumerfinance.gov/newsroom/cfpb-takes-action-against-meracord-for-processing-illegal-debt-settlement-fees/.
[5] *See* Consumer Federation of America, Legal Status of Payday Loans by State, available at http://paydayloaninfo.org/state-information; National Consumer Law Center, CONSUMER CREDIT REGULATION § 9.3 (2012).
[6] *See* Center for Responsible Lending, *CRL Issue Brief: Effective State and Federal Payday Lending Enforcement:*

Nonetheless, high-cost lenders have used choice of law provisions, purported tribal sovereign immunity, preemption claims and other arguments in efforts to circumvent state consumer protection laws such as interest rate caps or restrictions on intensity of use. Courts have rejected efforts of lenders to locate offshore or otherwise claim exemption from state laws through choice of law provisions.[7]

Tribal affiliation also does not insulate payday lenders from state laws. The Supreme Court has made clear that, "[a]bsent express federal law to the contrary, Indians going beyond reservation boundaries have generally been held subject to non-discriminatory state law otherwise applicable to all citizens of the State."[8] Similarly, tribal lenders cannot, by contract, subject borrowers to the laws and jurisdiction of the tribe for transactions outside of and unrelated to the reservation. While tribes have authority over their own members, "exercise of tribal power beyond what is necessary to protect tribal self-government or to control internal relations is inconsistent with the dependent statutes of the tribes, and so cannot survive without express congressional delegation."[9] Tribal laws and not state laws apply on a reservation, but once a payday lender begins lending to nontribal members, off reservation state laws apply.

Tribal sovereign immunity, where it applies, does not allow tribally-affiliated lenders to ignore state law. Sovereign immunity is immunity from being sued, not an exemption from compliance with state consumer protection and other laws. "There is a difference between the right to demand compliance with state laws and the means available to enforce them."[10] If a payday lender is truly an arm of the tribe and has a claim to tribal sovereign immunity, states may have difficulty bringing an enforcement action. The tribe, however, is still bound to comply with state law. Of course, many of the payday lenders who claim tribal sovereign immunity have a spurious claim to sovereign immunity or no claim at all.

Even in circumstances where a lender has claim to sovereign immunity, a payday loan or other transaction is illegal if made by an unlicensed lender in a state that requires a license to legally operate, or if the loan violates state consumer protection law in the state where the borrower resides. Tribal affiliation does not change the legality of the loan.

Payment processors and depository institutions, who have no claim of tribal sovereign immunity, are complicit in this illegal transaction if they permit themselves be used to facilitate payments for illegal loans. As with any other higher-risk activity, financial institutions have a duty to scrutinize their customers and their customer's customers to ensure that the institution is not being used to process illegal payments.

Scrutiny of payment processing for higher-risk merchants is consistent with longstanding supervisory expectations and warnings about relationships with third parties

Despite recent criticism of financial regulators scrutinizing the role of financial institutions in facilitating illegal transactions, these actions are consistent with long-standing supervisory expectations. Some of these criticisms have stemmed from actions by depository financial institutions that process payments for

---

Paving the Way for Broader, Stronger Protections (Oct. 4, 2013), available at http://www.responsiblelending.org/payday-lending/research-analysis/State-Enforcement-Issue-Brief-10-4-FINAL.pdf.

[7] *See* Consumer Federation of America, "States Have Jurisdiction over Online Payday Lenders" (May 2010) (discussing cases), available at http://www.consumerfed.org/pdfs/IPDL-States-Have-Jurisdiction.pdf.

[8] Mescalero Apache Tribe v. Jones, 411 U.S. 145, 149 (1973).

[9] Montana v. United States, 450 U.S. 544, 564 (citations omitted); *accord* Brief of the Federal Trade Comm'n as Amicus Curiae, Jackson et al. v. Payday Financial LLC,et al., No. 12-2617 (7th Cir. Sept. 13, 2013).

[10] Kiowa Tribe of Okla., v. Mfg. Technologies, Inc., 523 U.S. 751, 755 (1998).

high-risk merchants and have taken steps to ensure that they are not processing payments for illegal transactions.

Financial institutions have an obligation to know their customers, to conduct due diligence in their relationships with third parties, and to take actions to minimize risks presented by the processing of illegal transactions. ODFIs are the "gatekeepers of the ACH system."[11] They "undertake critical responsibilities under the NACHA rules that reflect the reliance of the ACH Network on appropriate underwriting and monitoring of Originators by ODFIs and the third parties with whom ODFIs have ACH origination arrangements."[12] Similarly, in the banking and payment processing industries, the monitoring of return rates is a well-established component of risk management practices.[13]

On March 30, 2013, Michael J. Bresnick, Executive Director of the U.S. Department of Justice Financial Fraud Enforcement Task Force, warned when discussing actions to clamp down on banks facilitating payday loan transactions in violation of laws such as the Bank Secrecy Act:

> "We are aware, for instance, that some payday lending businesses operating on the Internet have been making loans to consumers in violation of the state laws where the borrowers reside. And, as discussed earlier, these payday lending companies are able to take the consumers' money primarily because banks are originating debit transactions against consumers' bank accounts."

Depository institutions whose customers claim exemption from state law through aggressive interpretations of choice of law, preemption, or sovereign immunity doctrines expose financial institutions to legal and reputational risk.

Regulator scrutiny of bank relationships with online payday lenders and their payment processors is consistent with longstanding scrutiny of other higher risk third party relationships. To assist in this effort, NACHA regularly publishes two lists, one of high-risk operators,[14] and another of operators who have been terminated from the ACH system.[15]

Years ago, regulators warned financial institutions that they faced increased legal and reputation risks when they assisted payday lenders in offering loans on terms that the lenders could not offer directly.[16] This increased risk also applies in cases where the financial institution processes payments for payday lenders who claim exemption from state laws based on choice of law, preemption, or sovereign immunity doctrines.

---

[11] NACHA, ACH Operations Bulletin #2-2013, *High-Risk Originators and Questionable Debit Activity* (Mar. 14, 2013), available at www.nacha.org/OpsBulletins; 2013 NACHA Operating Rules § 2.1 at OR4.

[12] *Id.*

[13] *See, e.g.,* Complaint for Injunctive and Other Equitable Relief, FTC v. Landmark Clearing, Inc., et al., No. 4:11-cv-00826 (E.D. Tex. Dec. 15, 2011), available at www.ftc.gov/os/caselist/1123117/index.shtm; OCC Consent Order for a Civil Penalty, In re Wachovia Bank, 2008-027 (Apr. 24, 2008); Reyes v. Zion Nat'l Bank, 2012 WL 947139 (E.D. Pa. Mar. 21, 2012). However, return rates do not tell the entire story. Some unscrupulous players are adept at manipulating how they submit payments in order to avoid excessive returns in any one place. *See, e.g.,* FTC v. Automated Electronic Checking, Inc, et al., http://ftc.gov/os/caselist/1223102/130313aeccmpt.pdf; FinCEN Advisory, FIN-2012-A010, "Risk Associated with Third-Party Payment Processors" (Oct. 22, 2012), http://www.fincen.gov/statutes_regs/guidance/html/FIN-2012-A010.html. Also, monitoring only of returns coded as unauthorized will not catch high rates of returns for reasons of stop payment or insufficient funds, which can also be indications that consumers did not expect or authorize the payment or were defrauded.

[14] *See* www.nacha.org/originator_watch_list.

[15] *See* www.nacha.org/terminated_originator_database.

[16] *See, e.g., Payday Lending*, OCC, OCC Advisory Letter (Nov. 27, 2000); FDIC, *Guidelines for Payday Lending*, Financial Institution Letter (March 1, 2005).

In 2008, the OCC issued a risk management guidance outlining the need for effective monitoring of certain higher risk merchants, including but not limited to telemarketers. The guidance addressed the need for careful monitoring of consumer complaints, returned items and potential unfair or deceptive practices to limit legal, reputation, and other risks.[17] The FDIC issued a similar warning last year, and updated it in September of this year.[18]

Regulators must ensure that illegal operators do not turn to remotely created checks

The ACH system has a well-established system for monitoring fraud and high risk activity. But the check system is subject to far fewer systemic controls. Regulators must take actions to ensure that merchants who wish to process illegal payments do not turn use of remotely created checks and related electronic payments processed through the check system in order to evade scrutiny or impediments to using the ACH system.

The FTC recently proposed to ban use of remotely created checks (RCCs) and remotely created payment orders (RCPOs) in transactions governed by the Telemarketing Sales Rule. The FTC's well-documented proposal describes the way in which telemarketing scammers have turned to RCCs and RCPOs to escape the scrutiny and strong consumer protections for electronic payments. Our groups supported the FTC's proposal and have urged regulators to prohibit use of RCCs and RCPOs in consumer transactions.[19] We recognize, however, that a complete prohibition is a long term goal and cannot be accomplished immediately.

In the interim, we urge your agencies to consider other measures to ensure that illegal activity does not simply move from the electronic payment system to the check system, where it is subject to far fewer controls. Possible actions could include stronger monitoring requirements of merchants who use RCCs and RCPOs by depository institutions and payment processors and a prohibition on use of RCCs or RCPOs by operators who have been banned from the ACH system. Similarly, merchants should be banned from using RCCs or RCPOs after a consumer has stopped payment on or revoked authorization for an ACH payment, just as they may not process an ACH payment after a consumer has stopped payment on a check that was converted to an ACH payment.[20]

Conclusion

We encourage your agencies to continue to closely monitor the payment processing procedures and compliance safeguards in place at the payment processors and financial institutions that you supervise. Where you find indications that the institution has insufficient safeguards to avoid processing illegal

---

[17] *Risk Management Guidance: Payment Processors*. Office of the Comptroller of the Currency, April 24, 2008.
[18] *See* FDIC, FIL-3-2012, Payment Processor Relationships Revised Guidance (Jan. 31, 2012), available at www.fdic.gov/news/news/financial2012/fil12003.html; FDIC, FIL-43-2013, FDIC Supervisory Approach to Payment Processing Relationships with Merchant Custoerms that Engage in High-Risk Activities (Sept. 27, 2013).
[19] *See* Letter to the Federal Reserve Board and Consumer Financial Protection Bureau, "Supplemental Comments, 12 CFR Part 229, Regulation CC: Docket No. R-1409, 76 Fed. Reg. 16862 (Mar. 25, 2011), Remotely Created Items, Funds Availability Schedule for Prepaid Cards and Mobile Deposits," from the National Consumer Law Center (on behalf of its low income clients), Consumer Action, Consumer Federation of America, Consumers Union, National Association of Consumer Advocates, and National Consumers League (Sept. 18, 2013), available at http://www.nclc.org/images/pdf/rulemaking/comments-regulation_cc_rcc_efaa_9-18-2013.pdf.
[20] *See* NACHA, ACH Operations Bulletin #3-2013, Reinitiation of Returned Debit Entries (July 15, 2013), available at https://www.nacha.org/OpsBulletins.

payments, or is exposed to excessive legal, compliance, reputation or other risks through arrangements with third parties, we urge you to take swift action.

We thank you for protecting the integrity of the payment system, financial institutions, and consumers and look forward to your efforts to strengthen this important role going forward.

Respectfully submitted,

Americans for Financial Reform
Arkansans against Abusive Payday Lending
California Reinvestment Coalition
Center for Responsible Lending
Coalition of Religious Communities (UT)
Consumer Action
Consumers for Auto Reliabilty and Safety
Consumers Union
Economic Fairness Oregon
Georgia Watch
GRO Missouri
Jacksonville Area Legal Aid (FL)
Jesuit Social Research Institute at Loyola University
The Leadership Conference on Civil and Human Rights
Maryland Consumer Rights Coalition
NAACP
National Association of Consumer Advocates
National Community Reinvestment Coalition
National Consumer Law Center (on behalf of its low income clients)
New Economy Project (NY)
Policy Matters Ohio
Rhode Island State Council of Churches
Rhode Island Payday Lending Reform
South Carolina Appleseed Legal Justice Center
Southwest Center for Economic Integrity (AZ)
Texas Appleseed
US Public Interest Research Group
Virginia Poverty Law Center
Woodstock Institute (IL)

October 24, 2013

The Honorable Benjamin Bernanke, Chairman
Board of Governors of the Federal Reserve System
20th Street and Constitution Ave., NW
Washington DC 20551

The Honorable Richard Cordray, Director
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

The Honorable Tom Curry, Comptroller
Office of the Comptroller of the Currency
250 E Street SW
Washington, DC 20219

The Honorable Martin Gruenberg, Chairman
Federal Deposit Insurance Corporation
550 17th Street Northwest
Washington, DC 20429

The Honorable Eric Holder
Attorney General of the United States
Department of Justice
950 Pennsylvania Ave
Washington, DC 20530

The Honorable Debbie Matz, Chairman
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428

The Honorable Edith Ramirez, Chairwoman
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20530

Dear Chairman Bernanke, Director Cordray, Comptroller Curry, Chairman Gruenberg, Attorney General Holder, Chairman Matz and Chairwoman Ramirez,

The undersigned organizations write to thank you for your efforts to date and to urge you to take further strong action to protect consumers and the integrity of the payment system by stopping depository institutions and payment processors from facilitating electronic payments for illegal transactions, including illegal payday loans. Numerous regulatory and court actions have highlighted the crucial role that banks and payment processors play, intentionally or unintentionally, in processing illegal payments for internet and telemarketing scammers, debt settlement companies, payday lenders and others. We appreciate the efforts of your agencies. We encourage you to continue to closely monitor payments networks in order to identify those merchants that operate outside of the law and rely on access to consumers' bank accounts to extract payments. Regulatory scrutiny of those who process payments for higher-risk merchants is necessary, not only to address the direct harm imposed upon consumers by the

illegal transaction, but also to reduce the legal and reputational risks to insured depository financial institutions, consistent with longstanding supervisory expectations.

The payment system is crucial to a wide variety of unscrupulous, higher-risk merchants

Higher-risk merchants that extract unauthorized, abusive or illegal payments raise numerous consumer protection concerns. As many of these high-risk merchants expand to the internet, they increasingly rely on payment processors and originating depository financial institutions (ODFIs) to access consumers' bank accounts. The payment processor and the ODFI enable a payment to be debited from a consumer's account through the automated clearinghouse (ACH) system, a remotely created check (RCCs) or remotely created payment order (RCPOs).

High-risk merchants perpetrating fraud are subject to legal action. But the responsibility does not stop there. Recognizing that fraudsters need help in accessing the payment system, over the last several years regulators have held that payment processors and ODFIs are responsible for managing legal and reputational risk by closely monitoring the activities of their clients. In extreme cases, when the payment processor or ODFI is reckless or even complicit, they may themselves be subject to legal action. Enforcement actions against payment processors or ODFIs by financial services regulators in recent years have involved abuse of the payment system to perpetrate fraud involving vulnerable seniors,[1] telemarketing scams,[2] internet schemes to extract payments for unwanted goods and services,[3] illegal debt settlement fees,[4] and other fraudulent activity. While many high-risk merchants may evade enforcement of consumer protections or be judgment proof, cracking down on those who abet illegal conduct is essential to protecting consumers, preventing abuse of the payment system and shielding financial institutions from legal and reputational risk.

Payment processors and depository financial institutions should not facilitate illegal loans

Online payday lenders are particularly high-risk merchants. These lenders typically market and originate loans to borrowers that reside in another state. Non-depository entities such as payday lenders must follow the law of the state where the consumer is located. Payday loans and other forms of high-cost lending are illegal in many states, and are legal in other states only if the lender is licensed and the loan complies with state consumer protection and other laws.[5]

Online payday lenders present different legal and consumer protection challenges than storefront high-cost lenders. These online lenders routinely market and originate loans with terms and conditions that violate the law of the state where the borrower resides. These lenders are regularly subject to investigation by state and federal officials and have been subject to numerous cease and desist orders and other enforcement actions.[6] Financial institutions that process payments for lenders operating illegally or subject to ongoing litigation are exposed to significant legal and reputational risk.

---

[1] *See* OCC Consent Order for a Civil Penalty, In re Wachovia Bank, 2008-027 (Apr. 24, 2008).
[2] Reyes v. Zion Nat'l Bank, 2012 WL 947139 (E.D. Pa. Mar. 21, 2012).
[3] *See* Complaint for Injunctive and Other Equitable Relief, FTC v. Landmark Clearing, Inc., et al., No. 4:11-cv-00826 (E.D. Tex. Dec. 15, 2011), available at www.ftc.gov/os/caselist/1123117/index.shtm
[4] *See* CFPB, Press Release, CFPB Takes Action Against Meracord for Processing Illegal Debt-Settlement Fee (Oct. 3, 2013), available at http://www.consumerfinance.gov/newsroom/cfpb-takes-action-against-meracord-for-processing-illegal-debt-settlement-fees/.
[5] *See* Consumer Federation of America, Legal Status of Payday Loans by State, available at http://paydayloaninfo.org/state-information; National Consumer Law Center, CONSUMER CREDIT REGULATION § 9.3 (2012).
[6] *See* Center for Responsible Lending, *CRL Issue Brief: Effective State and Federal Payday Lending Enforcement:*

Nonetheless, high-cost lenders have used choice of law provisions, purported tribal sovereign immunity, preemption claims and other arguments in efforts to circumvent state consumer protection laws such as interest rate caps or restrictions on intensity of use. Courts have rejected efforts of lenders to locate offshore or otherwise claim exemption from state laws through choice of law provisions.[7]

Tribal affiliation also does not insulate payday lenders from state laws. The Supreme Court has made clear that, "[a]bsent express federal law to the contrary, Indians going beyond reservation boundaries have generally been held subject to non-discriminatory state law otherwise applicable to all citizens of the State."[8] Similarly, tribal lenders cannot, by contract, subject borrowers to the laws and jurisdiction of the tribe for transactions outside of and unrelated to the reservation. While tribes have authority over their own members, "exercise of tribal power beyond what is necessary to protect tribal self-government or to control internal relations is inconsistent with the dependent statutes of the tribes, and so cannot survive without express congressional delegation."[9] Tribal laws and not state laws apply on a reservation, but once a payday lender begins lending to nontribal members, off reservation state laws apply.

Tribal sovereign immunity, where it applies, does not allow tribally-affiliated lenders to ignore state law. Sovereign immunity is immunity from being sued, not an exemption from compliance with state consumer protection and other laws. "There is a difference between the right to demand compliance with state laws and the means available to enforce them."[10] If a payday lender is truly an arm of the tribe and has a claim to tribal sovereign immunity, states may have difficulty bringing an enforcement action. The tribe, however, is still bound to comply with state law. Of course, many of the payday lenders who claim tribal sovereign immunity have a spurious claim to sovereign immunity or no claim at all.

Even in circumstances where a lender has claim to sovereign immunity, a payday loan or other transaction is illegal if made by an unlicensed lender in a state that requires a license to legally operate, or if the loan violates state consumer protection law in the state where the borrower resides. Tribal affiliation does not change the legality of the loan.

Payment processors and depository institutions, who have no claim of tribal sovereign immunity, are complicit in this illegal transaction if they permit themselves be used to facilitate payments for illegal loans. As with any other higher-risk activity, financial institutions have a duty to scrutinize their customers and their customer's customers to ensure that the institution is not being used to process illegal payments.

Scrutiny of payment processing for higher-risk merchants is consistent with longstanding supervisory expectations and warnings about relationships with third parties

Despite recent criticism of financial regulators scrutinizing the role of financial institutions in facilitating illegal transactions, these actions are consistent with long-standing supervisory expectations. Some of these criticisms have stemmed from actions by depository financial institutions that process payments for

---

Paving the Way for Broader, Stronger Protections (Oct. 4, 2013), available at http://www.responsiblelending.org/payday-lending/research-analysis/State-Enforcement-Issue-Brief-10-4-FINAL.pdf.

[7] *See* Consumer Federation of America, "States Have Jurisdiction over Online Payday Lenders" (May 2010) (discussing cases), available at http://www.consumerfed.org/pdfs/IPDL-States-Have-Jurisdiction.pdf.

[8] Mescalero Apache Tribe v. Jones, 411 U.S. 145, 149 (1973).

[9] Montana v. United States, 450 U.S. 544, 564 (citations omitted); *accord* Brief of the Federal Trade Comm'n as Amicus Curiae, Jackson et al. v. Payday Financial LLC,et al., No. 12-2617 (7th Cir. Sept. 13, 2013).

[10] Kiowa Tribe of Okla., v. Mfg. Technologies, Inc., 523 U.S. 751, 755 (1998).

high-risk merchants and have taken steps to ensure that they are not processing payments for illegal transactions.

Financial institutions have an obligation to know their customers, to conduct due diligence in their relationships with third parties, and to take actions to minimize risks presented by the processing of illegal transactions. ODFIs are the "gatekeepers of the ACH system."[11] They "undertake critical responsibilities under the NACHA rules that reflect the reliance of the ACH Network on appropriate underwriting and monitoring of Originators by ODFIs and the third parties with whom ODFIs have ACH origination arrangements."[12] Similarly, in the banking and payment processing industries, the monitoring of return rates is a well-established component of risk management practices.[13]

On March 30, 2013, Michael J. Bresnick, Executive Director of the U.S. Department of Justice Financial Fraud Enforcement Task Force, warned when discussing actions to clamp down on banks facilitating payday loan transactions in violation of laws such as the Bank Secrecy Act:

> "We are aware, for instance, that some payday lending businesses operating on the Internet have been making loans to consumers in violation of the state laws where the borrowers reside. And, as discussed earlier, these payday lending companies are able to take the consumers' money primarily because banks are originating debit transactions against consumers' bank accounts."

Depository institutions whose customers claim exemption from state law through aggressive interpretations of choice of law, preemption, or sovereign immunity doctrines expose financial institutions to legal and reputational risk.

Regulator scrutiny of bank relationships with online payday lenders and their payment processors is consistent with longstanding scrutiny of other higher risk third party relationships. To assist in this effort, NACHA regularly publishes two lists, one of high-risk operators,[14] and another of operators who have been terminated from the ACH system.[15]

Years ago, regulators warned financial institutions that they faced increased legal and reputation risks when they assisted payday lenders in offering loans on terms that the lenders could not offer directly.[16] This increased risk also applies in cases where the financial institution processes payments for payday lenders who claim exemption from state laws based on choice of law, preemption, or sovereign immunity doctrines.

---

[11] NACHA, ACH Operations Bulletin #2-2013, *High-Risk Originators and Questionable Debit Activity* (Mar. 14, 2013), available at www.nacha.org/OpsBulletins; 2013 NACHA Operating Rules § 2.1 at OR4.

[12] *Id.*

[13] *See, e.g.,* Complaint for Injunctive and Other Equitable Relief, FTC v. Landmark Clearing, Inc., et al., No. 4:11-cv-00826 (E.D. Tex. Dec. 15, 2011), available at www.ftc.gov/os/caselist/1123117/index.shtm; OCC Consent Order for a Civil Penalty, In re Wachovia Bank, 2008-027 (Apr. 24, 2008); Reyes v. Zion Nat'l Bank, 2012 WL 947139 (E.D. Pa. Mar. 21, 2012). However, return rates do not tell the entire story. Some unscrupulous players are adept at manipulating how they submit payments in order to avoid excessive returns in any one place. *See, e.g.,* FTC v. Automated Electronic Checking, Inc, et al., http://ftc.gov/os/caselist/1223102/130313aeccmpt.pdf; FinCEN Advisory, FIN-2012-A010, "Risk Associated with Third-Party Payment Processors" (Oct. 22, 2012), http://www.fincen.gov/statutes_regs/guidance/html/FIN-2012-A010.html. Also, monitoring only of returns coded as unauthorized will not catch high rates of returns for reasons of stop payment or insufficient funds, which can also be indications that consumers did not expect or authorize the payment or were defrauded.

[14] *See* www.nacha.org/originator_watch_list.

[15] *See* www.nacha.org/terminated_originator_database.

[16] *See, e.g., Payday Lending*, OCC, OCC Advisory Letter (Nov. 27, 2000); FDIC, *Guidelines for Payday Lending*, Financial Institution Letter (March 1, 2005).

In 2008, the OCC issued a risk management guidance outlining the need for effective monitoring of certain higher risk merchants, including but not limited to telemarketers. The guidance addressed the need for careful monitoring of consumer complaints, returned items and potential unfair or deceptive practices to limit legal, reputation, and other risks.[17] The FDIC issued a similar warning last year, and updated it in September of this year.[18]

Regulators must ensure that illegal operators do not turn to remotely created checks

The ACH system has a well-established system for monitoring fraud and high risk activity. But the check system is subject to far fewer systemic controls. Regulators must take actions to ensure that merchants who wish to process illegal payments do not turn use of remotely created checks and related electronic payments processed through the check system in order to evade scrutiny or impediments to using the ACH system.

The FTC recently proposed to ban use of remotely created checks (RCCs) and remotely created payment orders (RCPOs) in transactions governed by the Telemarketing Sales Rule. The FTC's well-documented proposal describes the way in which telemarketing scammers have turned to RCCs and RCPOs to escape the scrutiny and strong consumer protections for electronic payments. Our groups supported the FTC's proposal and have urged regulators to prohibit use of RCCs and RCPOs in consumer transactions.[19] We recognize, however, that a complete prohibition is a long term goal and cannot be accomplished immediately.

In the interim, we urge your agencies to consider other measures to ensure that illegal activity does not simply move from the electronic payment system to the check system, where it is subject to far fewer controls. Possible actions could include stronger monitoring requirements of merchants who use RCCs and RCPOs by depository institutions and payment processors and a prohibition on use of RCCs or RCPOs by operators who have been banned from the ACH system. Similarly, merchants should be banned from using RCCs or RCPOs after a consumer has stopped payment on or revoked authorization for an ACH payment, just as they may not process an ACH payment after a consumer has stopped payment on a check that was converted to an ACH payment.[20]

Conclusion

We encourage your agencies to continue to closely monitor the payment processing procedures and compliance safeguards in place at the payment processors and financial institutions that you supervise. Where you find indications that the institution has insufficient safeguards to avoid processing illegal

---

[17] *Risk Management Guidance: Payment Processors*. Office of the Comptroller of the Currency, April 24, 2008.
[18] *See* FDIC, FIL-3-2012, Payment Processor Relationships Revised Guidance (Jan. 31, 2012), available at www.fdic.gov/news/news/financial2012/fil12003.html; FDIC, FIL-43-2013, FDIC Supervisory Approach to Payment Processing Relationships with Merchant Custoerms that Engage in High-Risk Activities (Sept. 27, 2013).
[19] *See* Letter to the Federal Reserve Board and Consumer Financial Protection Bureau, "Supplemental Comments, 12 CFR Part 229, Regulation CC: Docket No. R-1409, 76 Fed. Reg. 16862 (Mar. 25, 2011), Remotely Created Items, Funds Availability Schedule for Prepaid Cards and Mobile Deposits," from the National Consumer Law Center (on behalf of its low income clients), Consumer Action, Consumer Federation of America, Consumers Union, National Association of Consumer Advocates, and National Consumers League (Sept. 18, 2013), available at http://www.nclc.org/images/pdf/rulemaking/comments-regulation_cc_rcc_efaa_9-18-2013.pdf.
[20] *See* NACHA, ACH Operations Bulletin #3-2013, Reinitiation of Returned Debit Entries (July 15, 2013), available at https://www.nacha.org/OpsBulletins.

payments, or is exposed to excessive legal, compliance, reputation or other risks through arrangements with third parties, we urge you to take swift action.

We thank you for protecting the integrity of the payment system, financial institutions, and consumers and look forward to your efforts to strengthen this important role going forward.

Respectfully submitted,

Americans for Financial Reform
Arkansans against Abusive Payday Lending
California Reinvestment Coalition
Center for Responsible Lending
Coalition of Religious Communities (UT)
Consumer Action
Consumers for Auto Reliabilty and Safety
Consumers Union
Economic Fairness Oregon
Georgia Watch
GRO Missouri
Jacksonville Area Legal Aid (FL)
Jesuit Social Research Institute at Loyola University
The Leadership Conference on Civil and Human Rights
Maryland Consumer Rights Coalition
NAACP
National Association of Consumer Advocates
National Community Reinvestment Coalition
National Consumer Law Center (on behalf of its low income clients)
New Economy Project (NY)
Policy Matters Ohio
Rhode Island State Council of Churches
Rhode Island Payday Lending Reform
South Carolina Appleseed Legal Justice Center
Southwest Center for Economic Integrity (AZ)
Texas Appleseed
US Public Interest Research Group
Virginia Poverty Law Center
Woodstock Institute (IL)

Third-party Payment Processors:

Consumer Fraud, Money Laundering, and Reputational Risks

Joel M. Sweet, Trial Attorney, Consumer Protection Branch, DOJ
(detailee from United States Attorney's Office for the Eastern District of Pennsylvania)

Disclaimer

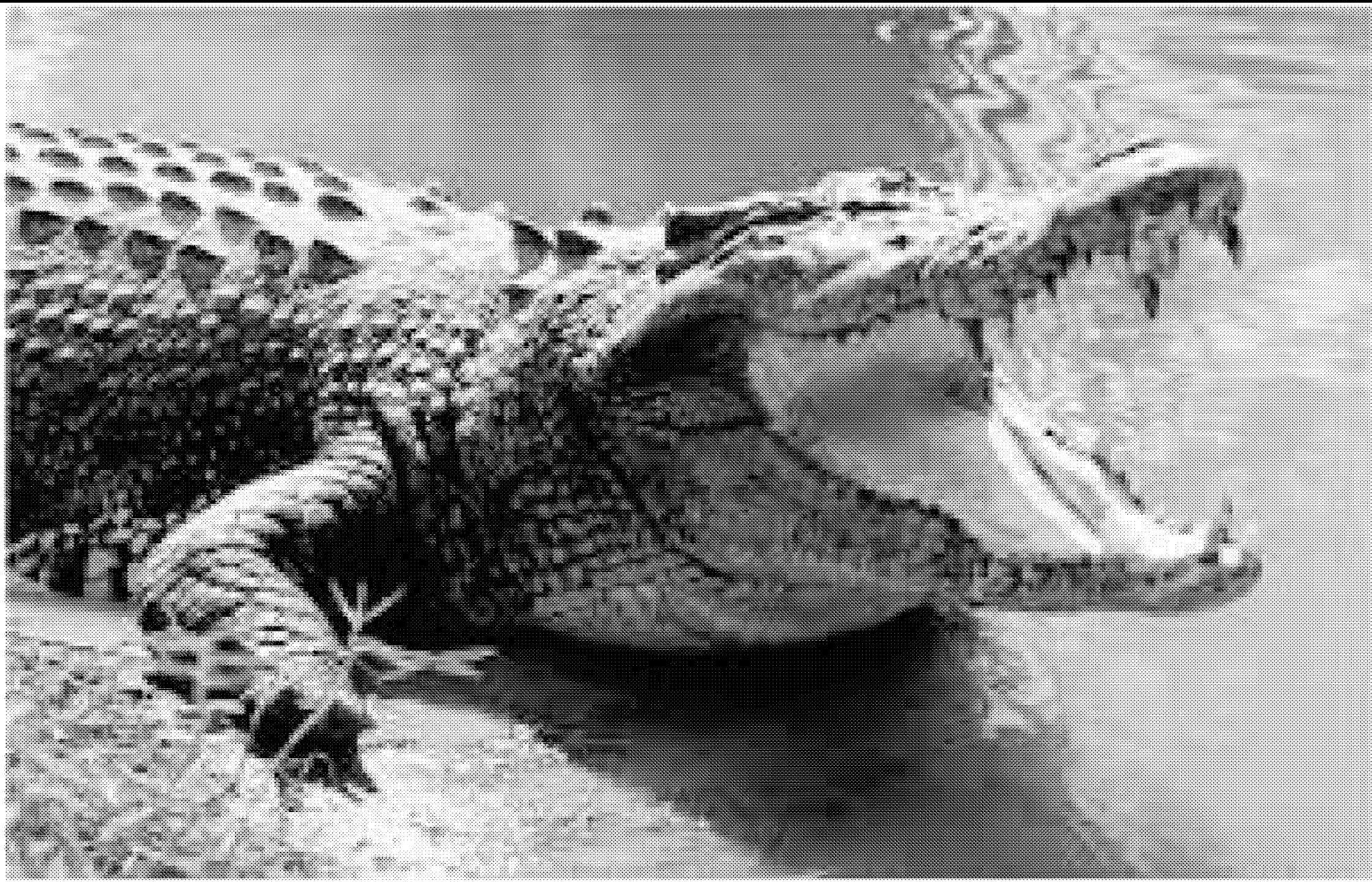
Any opinions reflected in this presentation are those of the presenter and are not necessarily those of the Department of Justice, or any government official, agency, department, or branch.

The information in this presentation is from public sources.

Risky Business

What are we talking about when we talk about *risk*?

How do we understand risk?



Mass-Market Consumer Fraud

- Internet and telemarketing
- Based upon purported authorizations
- Requires access to consumer bank accounts
- Billions annually in consumer losses
- Aggregation of small harm equivalent to big harm:
  - 1 X $200,000,000 = $200,000,000
  - 1,000,000 X $200 = $200,000,000

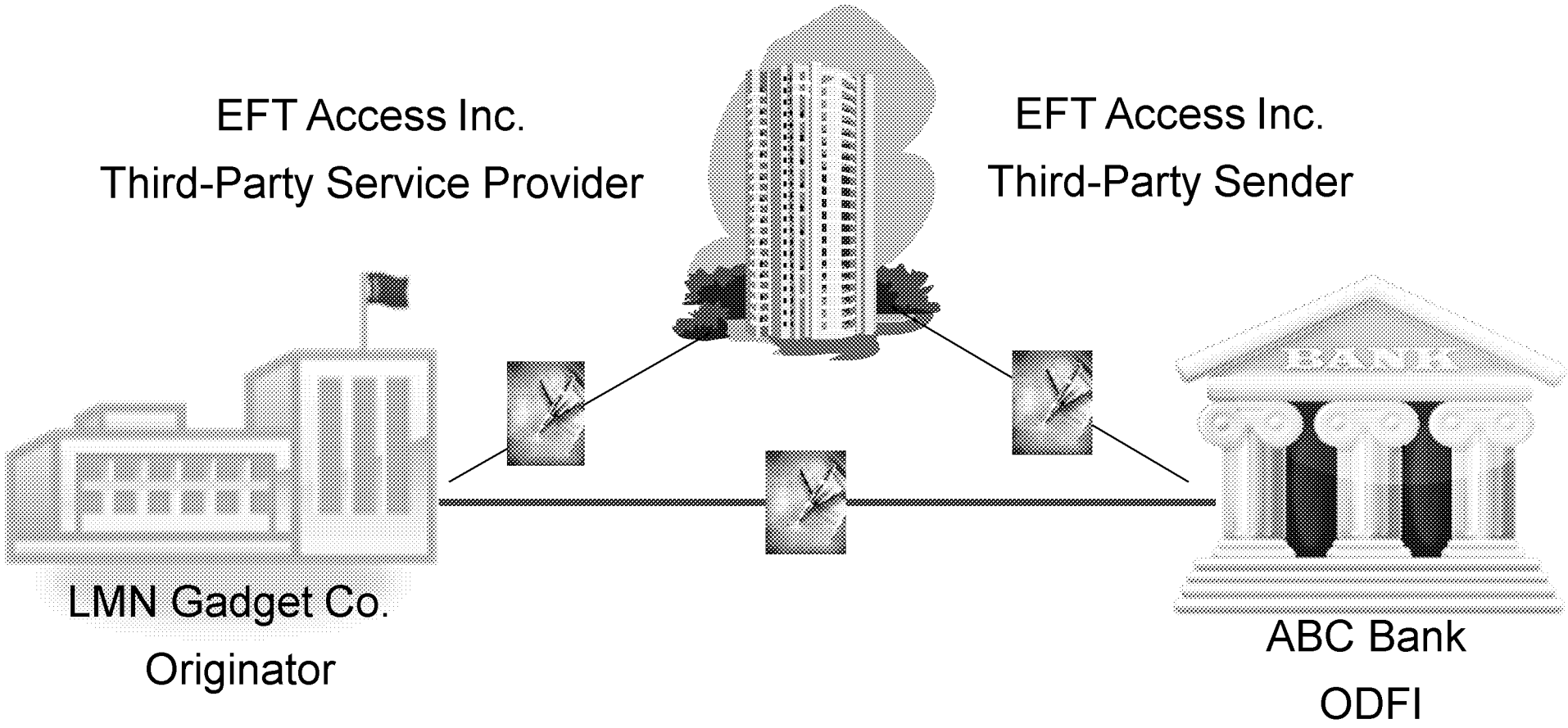
Law Enforcement Challenges to Prosecuting Telemarketing/Internet Fraud

- Jurisdictional limitations (state and international)
- Fraudsters change corporate identities and law enforcement plays "whack-a-mole"
- Victims are dispersed geographically
- Victims cannot identify fraudsters – no face-to-face contact
- Plausible deniability – cross-pointing among call centers, mail houses, fulfillment centers, payment processors, and banks
- Limited investigative and prosecutorial resources
- Limited reach of State Attorneys General and FTC

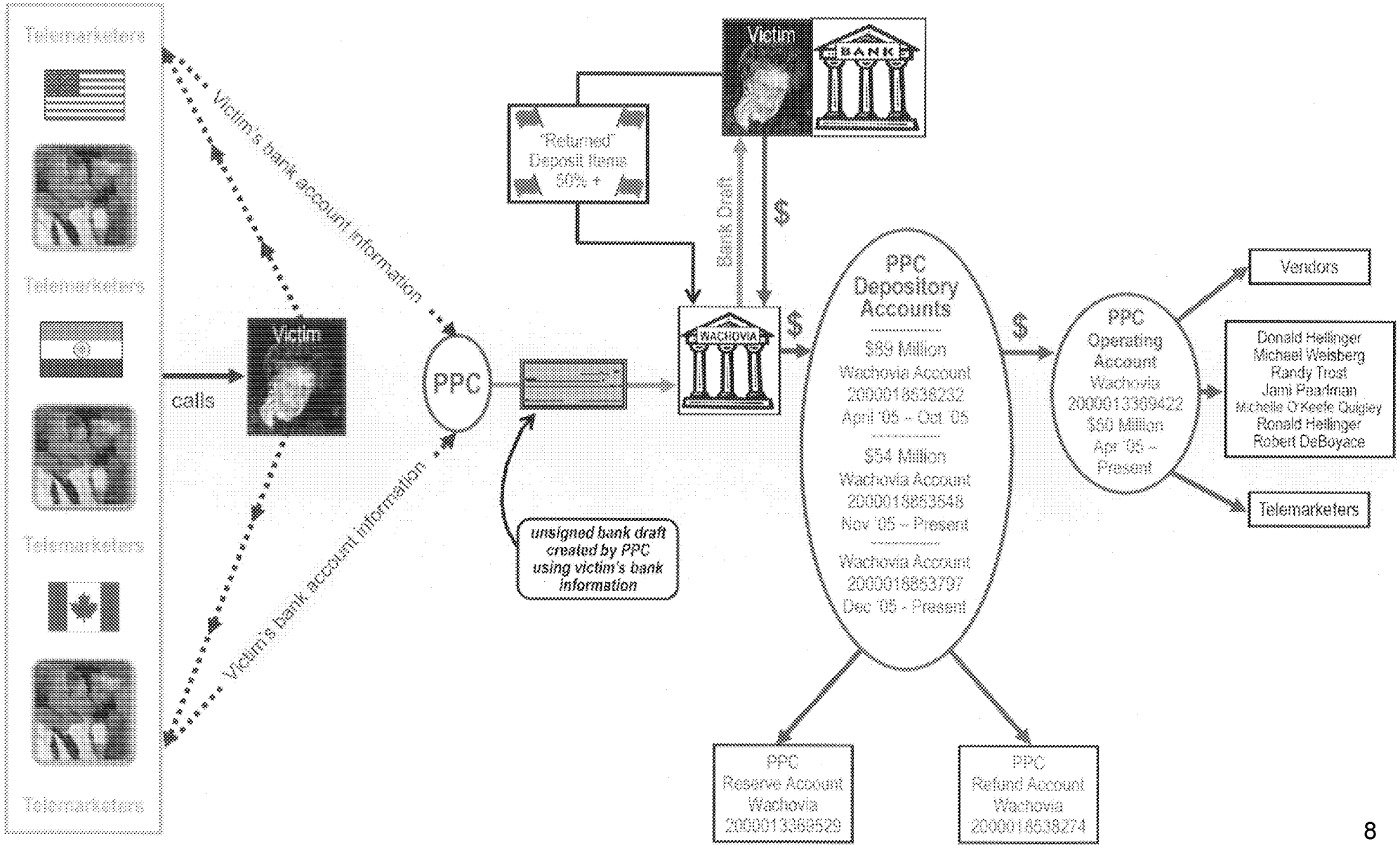
Third-Party Service Provider or Third-Party Sender?

So….what's the difference?

The difference is where the agreements exist (or *don't* exist)!



The Payment Process



: lmeojhlihcbbcapbcmliiebhcaaa.justin@paymentprocessingcenter.com
= 0000000353
: 00000000D8B3FD5A785EC54E87ADC17FEBD9131424232100
: To the fine people that made hellish phone abuse a little more bearable,
Thank you for making my summer a little less tedious and a little more

, I am glad to have shared the daily death-threats, hate-filled rants, and ignorance with all of you. I think sometime in the next couple weeks I may almost (in some kind of sick way) miss the sound of shit-kickers screamed obsenities over the verification playback.

bacon-speckled tomato soup, dealt with a phonebook's worth of customer callbacks, and a lot of soggy bread from the sandwich club.
When you come into work on Monday don't be sad that my cute little ass isn't around, be happy... because finally one of us will get to know what daylight looks like during a weekday. Just remember my smiling face and boyish good

I know the customer service number and I'm not afraid to call with my bank rep on the line)

Now, as I hang up my Steno Pad and descend back in to a world of relative normality I would like to say THANK YOU to everyone.

Side note to Michael: How much exactly do I owe you for the knowledge that it takes a total of 16 combined brain cells and teeth to provide your bank account information to a stranger on the phone to order something with as stupid a name as Washballs? or; the knowledge that old people are just plain easy to trick?

stay in touch,
Justin

Prime Time Checking

Account Number [redacted]
Statement Date: October 31, 2007
Page 1 of 3

[redacted]

- For Customer Service during business hours call 215.864.6730 or e-mail us at info@BeneficialSavingsBank.com
- For 24-hour account information call DirectLink at 215.864.1799 or 1.800.784.8490
- For other information visit us at www.BeneficialSavings.com

Account Summary

Previous Statement Balance As Of 09/30/07	1,864.08
Total Withdrawals/Charges	2,625.50
Total Deposits/Credits	2,560.02
Ending Balance	1,798.60

Annual Percentage Yield Earned: 0.50%

Check Summary

Checks Enclosed: 7

Date	Chk No.	Amount	Date	Chk No.	Amount	Date	Chk No.	Amount
10/01	2439	40.00	10/18	2462	438.50	10/30	2466	237.00
10/10	2463	13.86	10/19	2464	159.46	10/26	2470	9.95
10/24	2460*	10.00						

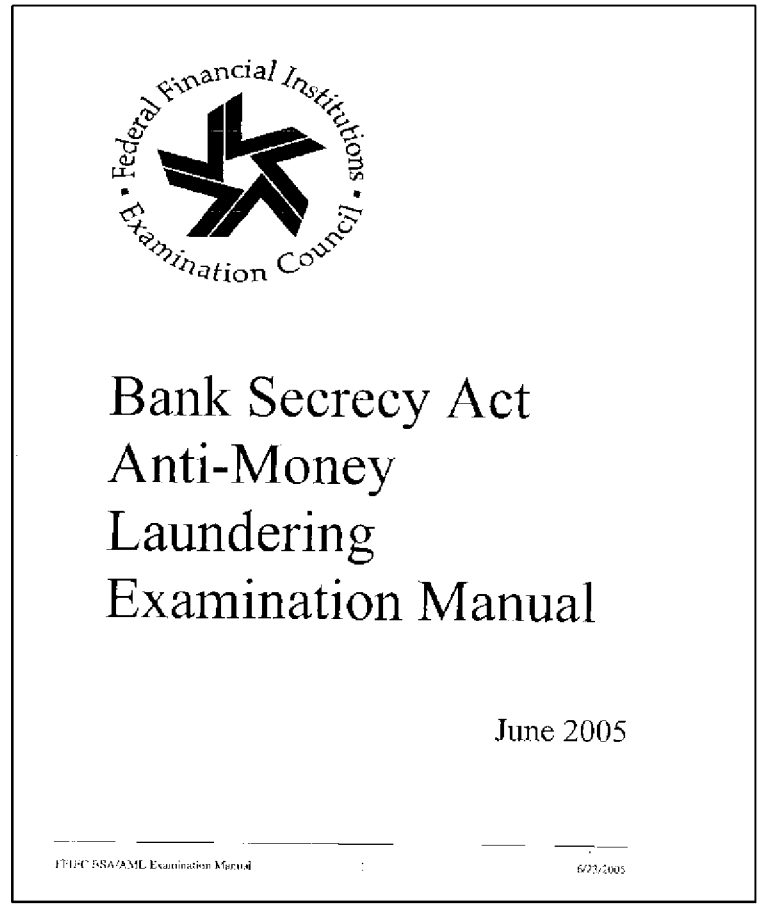
* Denotes Gap in Check Number Sequence

Other Transactions

Date	Description	Deposit(+) Withdrawal(-)
10/02	Ac-Us Treasury 303 -Soc Sec	565.00+
10/02	Ac-Us Treasury 303 -Soc Sec	1,194.00+
10/02	Ac-Car -Convcheck Ck-000000000002444	24.99-
10/02	Ac-Ppd -Convcheck Ck-000000000002446	27.99-
10/02	Ac-Pnd -Convcheck Ck-000000000002447	27.99-
10/02	Ac-App -Convcheck Ck-000000000002448	34.99-
10/03	Ac-Pm -Convcheck Ck-000000000002445	25.99-
10/05	Ac-Sdrd -Convcheck Ck-000000000002450	23.99-
10/05	Ac-Dcd Main Office -Convcheck Ck-000000000002449	24.99-
10/17	Ac-Ppa -Convcheck Ck-000000000002457	27.99-
10/17	Ac-Sbn -Convcheck Ck-000000000002458	39.99-
10/19	Ac-At&T Consumer -Checkpaymt Ck-00002461	77.46-
10/23	Ac-Rda -Convcheck Ck-000000000002467	31.99-
10/24	Ac-Adrd -Convcheck Ck-000000000002468	19.99-
10/24	Ac-Sr -Convcheck Ck-000000000002465	29.00-
10/25	Ac-Dpd Main Office -Convcheck Ck-000000000002469	31.99-
10/29	Ac-Reporting Data D-Convcheck Ck-000000000002471	24.99-

RCC Fraud: Well-Known to Bank Regulators

BSA/AML Examination Manual (FRB, FDIC, NCUA, OCC, and OTS)



Expanded Overview – Third-Party Payment Processors

OBJECTIVE

Assess the adequacy of the bank's systems to manage the risks associated with its relationships with third-party payment processors, and management's ability to implement effective monitoring and reporting systems.

OVERVIEW

Non-bank, or third-party, payment processors (processors) are bank customers that provide payment-processing services to merchants and other business entities.

Traditionally, processors contracted primarily with retailers that had physical locations in order to process the retailers' transactions. These merchant transactions primarily included credit card payments but also covered automated clearing house demand drafts[118] (also known as e-checks), and debit and stored value cards transactions. With the expansion of the Internet, retail borders have been eliminated. Processors may now service a variety of merchant accounts, including conventional retail and Internet-based establishments, prepaid travel, and Internet gaming enterprises.

RISK FACTORS

Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, and fraud schemes.

The bank's BSA/AML risks when dealing with a processor account are similar to risks from other activities in which the bank's customer conducts transactions through the bank on behalf of the customer's clients. When the bank is unable to identify and understand the nature and source of the transactions processed through an account, the risks to the bank and the likelihood of suspicious activity can increase. If a bank has not implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or sanctioned transactions.

[118] A demand draft is a substitute for a preprinted paper check. The draft is produced without a consumer signature but presumably with the consumer's authorization.

RISK MITIGATION

Banks offering account services to processors should develop and maintain adequate policies, procedures, and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. Verification and assessment of a processor can be completed by performing the following procedures:

- Reviewing the processor's promotional materials, including its web site, to determine the target clientele. (Businesses with elevated risk may include: offshore companies, online gambling-related operations, and online payday lenders). For example, a processor whose customers are primarily offshore would be inherently riskier than a processor whose customers are primarily restaurants.
- Determining whether the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization (ISO) opportunities" or "gateway" arrangements.[119]
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.
- Identifying the processor's major customers.
- Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.

Banks that provide account services should monitor their processor relationships for any significant changes in the processors' business strategies that may affect their risk profile. Banks should periodically re-verify and update the businesses' profiles to ensure the risk assessment is appropriate.

In addition to adequate and effective account opening and due diligence procedures for processor accounts, management should monitor these relationships for unusual and suspicious activities. To effectively monitor these accounts, the bank should have an understanding of the following processor information:

- Merchant base.
- Merchant activities.
- Average number of dollar volume and number of transactions.
- "Swiping" versus "keying" volume for credit card transactions.
- Charge-back history.

[119] Gateway arrangements are similar to an Internet service provider with excess computer storage capacity who sells its capacity to a third party, who would then distribute computer service to various other individuals unknown to the provider. The third party would be making decisions about who would be receiving the service, although the provider would be providing the ultimate storage capacity. Thus, the provider bears all of the risks while receiving a smaller profit.

Wachovia: Victim or Participant?

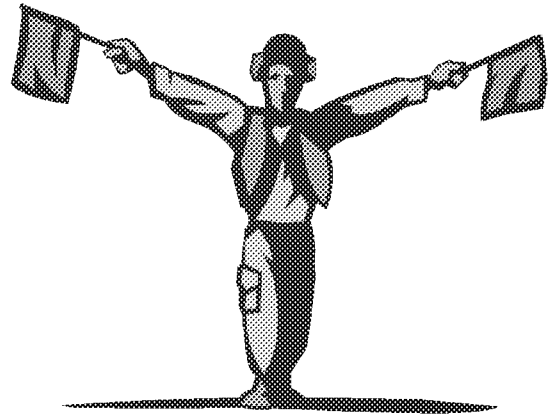
- Knew or remained willfully blind to fact that PPC serviced mass market fraudsters
- Ignored glaring red flags
- Suppressed internal concerns
- Ignored express warnings from other banks
- Entered agreements with PPC to protect its own interests at the expense of the interests of other banks and their customers

2012 ACH Return Rates

	Total	NSF	Invalid	Unauthorized
Network	.97%	.60%	.18%	.02%
Credits (All SECs)	.20%	.00%	.11%	.00%
Debits (All SECs)	1.51%	1.03%	.23%	.03%
ARC	.26%	.15%	.08%	.00%
BOC	1.45%	1.06%	.19%	.02%
IAT Credits	.66%	.00%	.39%	.00%
IAT Debits	1.57%	0.94%	.23%	.07%
POP	.84%	0.65%	.09%	.02%
PPD Credits	.23%	.00%	.14%	.00%
PPD Debits	2.07%	1.47%	.25%	.03%
RCK	60.48%	50.63%	1.69%	.08%
TEL	5.32%	3.56%	1.22%	.10%
WEB	1.43%	.97%	.23%	.03%

Returns – Charge Backs

- At inception, Wachovia **anticipated returns exceeding 35 percent** (compared to approximately 1/2 of 1 percent for all checks)
- Actual returns exceeded **50 percent**
- Wachovia charged PPC substantial fee for returns
- Wachovia offered PPC volume discounts on return fees



Return Reasons

- More than 50 percent of PPC's returns facially identified as:
  - UNAUTHORIZED
  - FRAUD
  - REFER TO MAKER

- Every month Wachovia received and hand-processed thousands of **sworn affidavits from consumers alleging that PPC debit transactions were not authorized**

Banknorth, N.A.

AFFIDAVIT OF UNAUTHORIZED CONSUMER DRAFT

(Type or Print Neatly)

Bank: Banknorth Massachusetts
Banking Center: SW Commons/39
RC: 3390
Telephone #: (508) 754 - 6745

Use this form for drafts with the following tran codes only:
184 POD Check
187 Check

[redacted] Customer's Name
[redacted] Account Number
[redacted] Street
Apt. #
P.O. Box
Worcester City
MA State
01604 Zip
[redacted] Daytime Telephone
Home Telephone

I declare, swearing under oath, that a draft charged to my account and appearing on my account statement is UNAUTHORIZED.

Check appropriate Section I OR Section II:

I. Draft Never Authorized:

☒ I have never authorized the company named above to debit my account

☐ I authorized the company named above to debit my account, but I revoked ** the authorization on _____ in the manner specified in said authorization.
Date of Revocation

** Customer must provide Bank with a copy of the written revocation

I further declare that the above transaction was not initiated by me or by any person acting on my behalf. In signing this form, I understand that the Bank will reverse any credit(s) to my account if it receives proof from the payee of the draft that I, in fact, authorized this draft.

[redacted] Customer Signature (required)
5-17-05 Date
Banking Center Representative

FOR USE ON PERSONAL ACCOUNTS ONLY

Instructions:

1. Fax to Adjustment Department 207-755-6315 OR Send a copy of the returned item (if available) and the signed affidavit through interoffice mail to: *Adjustment Department ME091-31*
2. Place a stop payment for the amount of the draft on the customer's account to prevent any future drafts from processing to the account. Have customer sign Stop Payment Order and remit form as usual.
3. Advise customer that provisional credit will NOT be granted on this transaction. Customer account will only be credited upon Bank receiving credit back from draft originator.

Affidavit of Unauthorized Consumer Draft Rev. 03/2004

Wachovia Ignored Internal Concerns

Return "volumes are tremendous" and "payment of these items is not our normal process"

Returns Operations Supervisor to VP of Loss Management

"Nothing [PPC] could ever do would make me comfortable . . ."

Bank Loss Management Official after learning about Bank relationship with PPC

After Loss Management official recommended closing PPC accounts, wrote "business line has assumed risk for the customer and decided to keep their accounts open"

Communication between Bank Loss Management Officials

Wachovia Ignored Explicit Fraud Warnings From Other Banks

"The purpose of this message is to **put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam . . .** instigate an investigation into whether [PPC is] conducting legitimate business and whether [Bank is] getting **a high volume of return items on those accounts (that should place your bank on notice of potential fraud).**"

E-Mail from Citizens Bank

What's a reputation worth?

CNNMoney.com News | Markets | Technology | Personal Finance | Small Business | CNN.com

FORTUNE

Yikes: Wachovia and the telemarketers

April 25, 2008

Wachovia Million

to Pay as Much as $144
arketing Case

Business Day

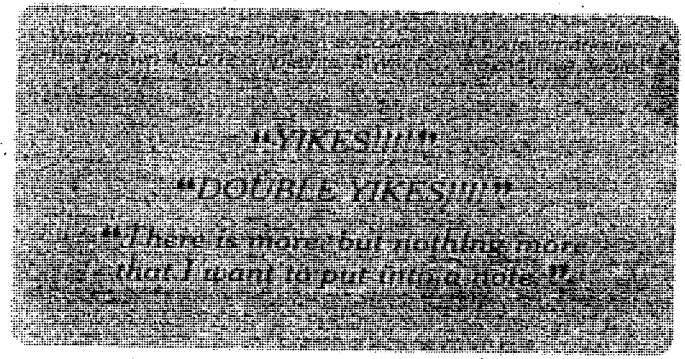
The New York Times

Papers Show Wachovia Knew of Thefts

By CHARLES DUHIGG

Last spring, **Wachovia** bank was accused in a lawsuit of allowing fraudulent telemarketers to use the bank's accounts to steal millions of dollars from unsuspecting victims. When asked about the suit, bank executives said they had been unaware of the thefts.

But newly released documents from that lawsuit now show that Wachovia had long known about allegations of fraud and that the bank, in fact, solicited business from companies it knew had been accused of telemarketing crimes.



e banking giant, has agreed to pay as
investigation accusing the bank of
ccounts to steal millions of dollars

HOGR-3PPP000436

Yes – it *is* a crime.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 10-20165 CR - LENARD
31 U.S.C. § 5318(h)
31 U.S.C. § 5322(a)

MAGISTRATE JUDGE
BRANNON

UNITED STATES OF AMERICA

v.

WACHOVIA BANK, N.A.,

Defendant.

FILED by D.C.
MAR 12 2010
STEVEN M. LARIMORE
CLERK U. S. DIST. CT.
S. D. of FLA. – MIAMI

INFORMATION

The United States Attorney charges that:

GENERAL ALLEGATIONS

At all times material to this Information

1. Defendant **WACHOVIA BANK, N.A.** was a national banking association based in Charlotte, North Carolina.

It's not over until it's over.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	CRIMINAL NO. 11-
	:	DATE FILED: February 10, 2011
v.		
	:	VIOLATIONS:
DONALD HELLINGER		18 U.S.C. § 371 (conspiracy – 1 count)
RONALD HELLINGER	:	18 U.S.C. § 1960 (operating an illegal money
MICHAEL WEISBERG		transmission business – 1 count)
RANDY TROST	:	18 U.S.C. § 1955 (operating an illegal gambling
JAMI PEARLMAN		business – 1 count)
MICHELE QUIGLEY	:	18 U.S.C. § 1084 (transmission of wagers and
		wagering information – 8 counts)
	:	18 U.S.C. § 1956(a)(2)(A) (international money
		laundering – 3 counts)
	:	Notice of forfeiture

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES THAT:

At all times relevant to this indictment:

BACKGROUND

1. Defendants DONALD HELLINGER, RONALD HELLINGER, MICHAEL WEISBERG, RANDY TROST, JAMI PEARLMAN, and MICHELE QUIGLEY

Important steps forward . . .

- Guidance to banks from FDIC, OCC and FinCEN
- U.S. v. Wachovia, U.S. v. First Bank of Delaware, anticipate additional civil and criminal actions by DOJ
- Reyes v. Zions Bank – class actions – RICO
- FTC and CFPB actions against payment processors
- Financial Fraud Enforcement Task Force/Consumer Protection Branch efforts to choke-off fraudsters' access to payment systems

Statutes -- civil

- FIRREA
  - Civil action
  - Civil money penalty
  - Violation of criminal fraud statutes affecting a FIFI
  - Civil legal standards (preponderance of evidence)
  - $5 million for continuing violations, or up to amount of consumer loss
  - Combined with injunctive statutes

Statute -- Criminal

- 18 U.S.C. § 1960 – Unlicensed Money Transmitting Businesses
- Whoever owns, manages, controls, manages . . . a money transmitting business:

(a) – without a state MT license

(b) – without registration with FinCEN

(c) – transmits funds known to be derived from or promoting unlawful activity

Enormous Regulatory Loophole

- Treasury Department regulation amended in 2011 arguably excludes third-party payment processors from the definition of "money transmitter" and thus all Money Services Business ("MSB") obligations.

- New rule:
  - "Whether a person is a money transmitter as described in this section is a matter of facts and circumstances."

- "**Read the new definition for yourself. Can *you* understand what it means and to whom it applies?**

Operation Choke Point

- Subpoenas issued to banks and TPPPs, including regulatory guidance.
- Several active criminal and civil investigations.
- Banks are scrutinizing TPPP and scammer relationships.
- Banks are self-disclosing problematic TPPP relationships.
- Internet Payday lending – fully dependent on TPPPs for ACH debits.

My nephew Lev's Bar Mitzvah

Thanks for your time and interest!

Questions?

Joel M. Sweet

[redacted]@usdoj.gov

Enforcement Strategies and Cases

Michael Blume
Director
Consumer Protection Branch
U.S. Department of Justice

Josh Burke
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice

The views expressed in this presentation are those of the presenters and do not necessarily reflect the views of the United States Department of Justice.

Law Enforcement Challenges to Prosecuting Telemarketing/Internet Fraud

- Limited reach of State Attorneys General and FTC
- Fraudsters change corporate identities and law enforcement plays "whack-a-mole"
- Victims are dispersed geographically
- Victims cannot identify fraudsters – no face-to-face contact
- Plausible deniability – cross-pointing among call centers, mail houses, fulfillment centers, payment processors, and banks
- Limited investigative and prosecutorial resources

Efforts to Combat Fraud by Focusing on Payment Processors and Banks

- Focused on banks and payment processors who are involved with or willfully blind to consumer fraud schemes that rely on payment systems to debit the accounts of consumer victims.
- Vertical investigations of high-risk, potentially fraudulent merchants, third-party payment processors, and banks.
- Concerned about all kinds of schemes that defraud consumers, primarily through telemarketing and internet-based companies.
- The schemes we are investigating have been identified in regulatory guidance and the BSA Manual as high-risk activity that warrants heightened due diligence and fraud controls.

Why Focus on Third-Party Payment Processors and Banks?

- Many high-risk and fraudulent merchants cannot obtain direct banking relationships because of risk factors.
- These merchants frequently use Third-Party Payment Processors to get the access to the banking system they cannot obtain directly.
- Focusing on one payment processor with dozens or even hundreds of fraudulent merchants is more efficient than pursuing each individual merchant.
- Focusing on a bank with multiple problematic third-party payment processors is even more efficient.

Red Flags and Indicia of Fraud in Our Investigations

- Return Rates - Both Unauthorized Returns and Total Returns
- Communications/ Complaints from RDFIs
- Contacts from law enforcement
- How does the TPPP market itself?
  - Does it offer to provide ACH processing for merchants who have been blacklisted from credit card processing?
  - Does it offer to process RCCs for merchants who cannot process credit cards or ACH?
- Internet complaints , lawsuits, and cease and desist orders against merchants
- Better Business Bureau Ratings and Warnings

Case Study: *United States v. Payment Processing Center, LLC*

- The government brought an injunction action to stop Payment Processing Center's operations
- PPC was a processor for merchants that included those that purported to offer government grants, prescription discount cards, travel programs, free gift cards, free computer
- PPC banked with Wachovia

Wachovia Bank: Victim or Participant?

- Processed hundreds of millions of dollars of RCCs for PPC and other payment processors
- PPC had a return rate over 40%
- Ignored red flags indicating that PPC serviced mass market fraudsters
- Ignored internal and external concerns about high return rates
- Wachovia failed to have an effective BSA/AML program in light of the high-risk nature of its third-party payment processor customers
  - Did not request detailed information about processors' merchant base
  - Did not have a detailed understanding of the processors' return rate history
  - Did not sufficiently scrutinize the processors' due diligence programs

Outcome

- Wachovia
  - Settled civil actions by DOJ, the OCC and a private class action by agreeing to pay more than $160 million in restitution to consumers, a $10 million fine to the U.S. Treasury, and $9 million to independent consumer protection education programs.
  - The government and Wachovia resolved a criminal investigation through a deferred prosecution agreement. United States v. Wachovia Bank, NA, (S.D. Fla.)
- Payment Processing Center, LLC
  - Company went out of business after government moved for an injunction under the Anti-Fraud Injunction Act. United States v. Payment Processing Center, LLC (E.D. Pa.)
  - Six individual owners of PPC convicted of federal felonies for operating an illegal money transmitting business. United States v. Donald Hellinger, et al. (E.D. Pa.).

Takeaways

- Processing ACH transactions and accepting RCC deposits on behalf of TPPPs and their high-risk merchants carries legal and reputational risks to your bank.
- Without significant due diligence and fraud controls, it also creates enormous potential risks to consumers by allowing fraudsters to have direct access to the consumer's bank accounts .
- RDFIs play an important role in combating fraud in the payment systems. What can you do?
  - Contact the ODFI with concerns of suspicious activity, allegations of fraud
  - Report problematic merchants and processors to NACHA
  - File SARs

From: Olin, Jonathan F. (CIV)
Sent: Monday, November 18, 2013 5:20 PM
To: Watson, Theresa (OAG)
Cc: Thompson, Karl (OAG)
Subject: RE: Civil Division Monthly Meeting

Tracking:

Recipient	Read
Watson, Theresa (OAG)	Read: 11/18/2013 5:20 PM
Thompson, Karl (OAG)	
Olin, Jonathan F. (CIV) [redacted]@civ.usdoj.gov)	
Olin, Jonathan F. (CIV)	Read: 11/18/2013 5:20 PM

Here you go – sorry for the delay. Item 2 is something Margaret asked us to add today.

Thanks,
Jon

Agenda for Civil Division Meet...

From: Watson, Theresa (OAG)
Sent: Monday, November 18, 2013 1:13 PM
To: Olin, Jonathan F. (CIV)
Cc: Thompson, Karl (OAG)
Subject: Civil Division Monthly Meeting

Hi Jonathan,

Can you forward me the agenda for the Civil meeting tomorrow with the AG. Karl is out today.

Thank you,

Theresa J. Watson
Acting Director of Scheduling
Office of the Attorney General
U.S. Department of Justice
[redacted]

" I will never quit. I persevere and thrive on adversity.
When knocked down I will get back up every time.
I am never out of the fight."

<< OLE Object: Picture (Device Independent Bitmap) >>

Civil Division Meeting with the Attorney General
November 19, 2013

AGENDA

[redacted]

2. Third Party Payment Processor Investigations

[redacted]

From: Olin, Jonathan F. (CIV)
Sent: Monday, November 18, 2013 8:51 PM
To: Delery, Stuart F. (CIV)
Subject: 3PPP TPs

Here are some TPs Maame sent along.

Brief TPs:

- We are after fraud on consumers. This includes fraudulent payday lending schemes or otherwise illegal payday lending schemes.
- Banks and processors are choke points for fraud on consumers.
- We are not targeting payday lending, and especially not tribally-owned payday lending businesses.
- The regulators are also taking action, and reinforcing their longstanding guidance on what are "high-risk merchants" and what due diligence banks should do on such merchants
- We have a number of pending investigations
- We have also learned from industry sources that many banks are taking note of our activity and that of the regulators and doing what they should have done all along - due diligence to know their customers. Some are also exiting "high-risk" lines of business.
- We understand that many of the players in these "high-risk" areas are forming alliances to lobby the Hill to slow our stop our various efforts. This includes the newly formed Online Lenders Alliance, and the newly formed Native American Financial Services Association.

Enforcement Strategies and Cases

Michael Blume
Director
Consumer Protection Branch
U.S. Department of Justice

[redacted]
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice

The views expressed in this presentation are those of the presenters and do not necessarily reflect the views of the United States Department of Justice.

Law Enforcement Challenges to Prosecuting Telemarketing/Internet Fraud

- Limited reach of State Attorneys General and FTC
- Fraudsters change corporate identities and law enforcement plays "whack-a-mole"
- Victims are dispersed geographically
- Victims cannot identify fraudsters – no face-to-face contact
- Plausible deniability – cross-pointing among call centers, mail houses, fulfillment centers, payment processors, and banks
- Limited investigative and prosecutorial resources

Efforts to Combat Fraud by Focusing on Payment Processors and Banks

- Focused on banks and payment processors who are involved with or willfully blind to consumer fraud schemes that rely on payment systems to debit the accounts of consumer victims.
- Vertical investigations of high-risk, potentially fraudulent merchants, third-party payment processors, and banks.
- Concerned about all kinds of schemes that defraud consumers, primarily through telemarketing and internet-based companies.
- The schemes we are investigating have been identified in regulatory guidance and the BSA Manual as high-risk activity that warrants heightened due diligence and fraud controls.

Why Focus on Third-Party Payment Processors and Banks?

- Many high-risk and fraudulent merchants cannot obtain direct banking relationships because of risk factors.
- These merchants frequently use Third-Party Payment Processors to get the access to the banking system they cannot obtain directly.
- Focusing on one payment processor with dozens or even hundreds of fraudulent merchants is more efficient than pursuing each individual merchant.
- Focusing on a bank with multiple problematic third-party payment processors is even more efficient.

Red Flags and Indicia of Fraud in Our Investigations

- Return Rates - Both Unauthorized Returns and Total Returns
- Communications/ Complaints from RDFIs
- Contacts from law enforcement
- How does the TPPP market itself?
  - Does it offer to provide ACH processing for merchants who have been blacklisted from credit card processing?
  - Does it offer to process RCCs for merchants who cannot process credit cards or ACH?
- Internet complaints , lawsuits, and cease and desist orders against merchants
- Better Business Bureau Ratings and Warnings

Case Study: *United States v. Payment Processing Center, LLC*

- The government brought an injunction action to stop Payment Processing Center's operations
- PPC was a processor for merchants that included those that purported to offer government grants, prescription discount cards, travel programs, free gift cards, free computer
- PPC banked with Wachovia

Wachovia Bank: Victim or Participant?

- Processed hundreds of millions of dollars of RCCs for PPC and other payment processors
- PPC had a return rate over 40%
- Ignored red flags indicating that PPC serviced mass market fraudsters
- Ignored internal and external concerns about high return rates
- Wachovia failed to have an effective BSA/AML program in light of the high-risk nature of its third-party payment processor customers
  - Did not request detailed information about processors' merchant base
  - Did not have a detailed understanding of the processors' return rate history
  - Did not sufficiently scrutinize the processors' due diligence programs

Outcome

- Wachovia
  - Settled civil actions by DOJ, the OCC and a private class action by agreeing to pay more than $160 million in restitution to consumers, a $10 million fine to the U.S. Treasury, and $9 million to independent consumer protection education programs.
  - The government and Wachovia resolved a criminal investigation through a deferred prosecution agreement. United States v. Wachovia Bank, NA, (S.D. Fla.)
- Payment Processing Center, LLC
  - Company went out of business after government moved for an injunction under the Anti-Fraud Injunction Act. United States v. Payment Processing Center, LLC (E.D. Pa.)
  - Six individual owners of PPC convicted of federal felonies for operating an illegal money transmitting business. United States v. Donald Hellinger, et al. (E.D. Pa.).

Takeaways

- Processing ACH transactions and accepting RCC deposits on behalf of TPPPs and their high-risk merchants carries legal and reputational risks to your bank.
- Without significant due diligence and fraud controls, it also creates enormous potential risks to consumers by allowing fraudsters to have direct access to the consumer's bank accounts .
- RDFIs play an important role in combating fraud in the payment systems. What can you do?
  - Contact the ODFI with concerns of suspicious activity, allegations of fraud
  - Report problematic merchants and processors to NACHA
  - File SARs

National Consumer Law Center 22nd Annual Consumer Rights Litigation Conference

Michael S. Blume, Director, Consumer Protection Branch, Civil Division, U.S. Department of Justice

Plenary delivered November 8, 2013

Good evening. Thank you for that kind introduction. It is a pleasure to be here. I am especially grateful to my good friend Irv Ackelsberg for arranging my appearance here today. Irv is a giant in the consumer protection bar, whose foresight, creativity, and doggedness, in decades of work as a legal services attorney and for a private, class action firm, has improved the lives of countless American consumers.

[And to Cary Flitter, I mention here a small world connection that we have. His office building is in Narberth, Pennsylvania, where I grew up. It's a several story brick building on a busy suburban road. It used to house doctor's offices. My pediatrician was in that building. There is a joke in there somewhere; I just don't know where.]

Before I begin, I do want to remind you that what I say here today represents my own views. They are not necessarily those of the Department of Justice.

With that, I welcome you to Washington. I hope that you had some time to enjoy the city in the fall. I see, however, that you might have little time to do that. Your agenda is packed, filled with substantive discussions of thorny consumer law issues. It amazes me how many legal issues confront lawyers seeking to protect consumers, and how difficult those issues are. Yours is not an easy job.

But, it is a vital job. Perhaps you know the sobering statistics, but I will highlight one of them for you. According to the FTC's report Consumer Fraud in the United States, 2011, 25 million Americans were victims of some kind of consumer fraud in 2011.

That statistic only tells a part of the story. You all know that. Because you represent the people who make up those statistics. They are real people, with real lives, and real stories of great loss. This loss is not just financial. It is loss that screams out for help. I will share with you two of the stories.

- Imagine a hard working woman with a good job. She owned her house, a modest one in a solid neighborhood of Philadelphia. She just wanted to upgrade her bathroom, the only one in her house. Unfortunately, she called the wrong home improvement contractor and fell prey to his fraud. He got her a mortgage loan, took her money, ripped out her bathroom, and then disappeared. What was she to do? She had to shower in her basement with a garden hose attached to the water line leading to her washing machine. At night, she had to urinate in a bucket. But, she soldiered on. She worked overtime to make enough extra money to fix the bathroom and pay off the loan.

- Imagine an elderly woman who learned that she won $5 million in the lottery. What would she do with the money? How could she help her family? All she had to do was pay certain taxes and fees. Yes, she had her doubts. But the documents looked so real – like they came from a federal agency. She sent thousands of dollars by wire, by direct transfer from her bank, and by cash. But, there was no lottery; there was no prize. Now, she is stuck with a home equity loan that she took out to pay these fees and taxes.

I could go on. I suspect that, right now, you are imagining some of your own clients, their stories, their struggles, and, hopefully, their triumphs.

Anyone who listens to these stories or who pays attention to these statistics should recognize the importance of consumer protection work. I am here to tell you that the Department of Justice does recognize it. The fact that there is a Consumer Protection Branch, with the explicit mission of protecting consumers, speaks volumes. So, too, do the kinds of cases that the prosecutors in the Branch bring. They are among the highest profile, widest impact cases in the entire Department of Justice. Consider just these few:

- This past Monday, the Department announced a $2.2 billion civil and criminal resolution with Johnson & Johnson. The investigations, three separate cases, largely involved the off-label promotion of powerful drugs. Our prosecutors were involved in the two criminal cases – worth $485 million – that were part of that resolution. The resolution is just one of the many that my office has done with U.S. Attorneys around the country in recent years, cases that have brought in over $6 billion in fines, forfeitures, and disgorgements since 2009.

- Prosecutors in my office, along with those from other components of the Department of Justice and the U.S. Attorney's Office in the Central District of California brought suit against Standard & Poor's, the credit rating agency. We have alleged that S&P misled investors about the credit risk associated with complex, mortgage backed securities. Our allegations stated that S&P issued inflated ratings given to those securities. The conduct alleged goes to the very heart of the recent financial crisis.

- Right now, in my office, prosecutors are investigating drugs, medical devices, food, and consumer products that have killed consumers, disabled them, or made them ill. We are looking into the actions of some of the largest companies in the world. Our cases are nationwide; many reach overseas.

Amidst all of that work, we have placed a special focus on payments systems fraud. We are looking at fraudulent merchants who use third parties to process their payments. We are looking at the payment processors themselves. And, we are looking at the banks that have payment processors as customers.

We want to know whether the banks or payment processors – because of their own actions or inactions – bear responsibility for fraud. Of the banks and payment processors, we are asking, "Are they aware of the fraud?" "Are they willfully blind to the fraud running through their banks?"

Given the critically important issues that my office investigates, some may ask, how did we get here? Why are we so concerned about fraud in the payment system?

The answer stems from our response to the unique and significant challenges that we who do consumer protection work face.

Start with the frauds that plague American consumers. The number and type of these frauds is limited only by the imagination of a person who wants to steal your money. That imagination is boundless. Telemarketing fraud, healthcare fraud, mortgage lending schemes, mortgage foreclosure schemes, government grant scams, vacation scams, credit repair scams, on-line lending scams. How do we address all of these different schemes?

We in the law enforcement community could do nothing but consumer fraud and we would be plenty busy. Obviously, we can't. There are too many other competing – and equally compelling – priorities. Choosing among these priorities is difficult enough. It is near impossible in today's budget environment. Federal prosecutors simply cannot do as many cases as we otherwise would do; there are fewer of us and we are supported with less investigative help. Now, ask yourself which types of cases a prosecutor's office are likely to prioritize. And, in answering that question, remember all of the things that we ask federal prosecutors to do, from anti-terrorism efforts, to gun violence prevention, to public corruption, to name a few. How can we make sure that consumer protection cases stay in the mix?

The cost to fraudulent merchants of opening and closing their operations – and stealing from consumers – is falling, and falling rapidly. Put another way, the barriers to setting up a fraudulent mass marketing operation are lower than they have ever been. According to the FTC, the internet is the most likely medium through which fraudsters promote their scams and by which they receive payment. Now compare the costs associated with a website and the reach of that website to a brick-and-mortar store or to the U.S. mails. Throw in voice-over-internet protocols. Fraudsters can pop up, shut down, and pop up somewhere else with ease, anywhere in the world, making it harder and harder for law enforcement to track them, let alone to stop them. I'm loath to use the metaphor, but I have yet to hear a better one; we are often playing "whack-a-mole." How can we take effective enforcement action in this environment?

Looking at the financial architecture of consumer fraud is helping us confront those challenges.

Mass marketing fraud schemes involve many thousands, if not millions, of individual financial transactions – debits to consumers' bank accounts. The people who run these schemes need to find a way to get the money from these transactions. The most effective

way of doing so is through the existing payment system. If a fraudster can work his way into the payment system, he can, literally at light speed, debit your bank account and credit his own.

The fraudster faces a big obstacle, however. The fraudulent merchant needs to gain access to the payment system. Banks would be an obvious choice. But, banks have "know your customer" responsibilities. They must conduct due diligence on their customers. They will ask uncomfortable questions of the fraudulent merchant, answers to which may deter a bank from working with the merchant.

To overcome this obstacle, a fraudulent merchant will use an intermediary, a third party payment processor. This entity is a kind of "middle man" in a financial transaction, and work on behalf of a wide variety of merchants, some legal and legitimate, and some fraudulent. The processor opens a bank account and uses it to gain access to the banking system on behalf of its merchants. At the merchants' direction, the processor will originate debit transactions against consumers' account, gather all that money together, and transmit it to the fraudulent merchant.

This structure offers several advantages to the fraudulent merchant. It allows him to hide behind the payment processor. The critical transactions will be carried out by the payment processor. Many banks are unwilling to conduct transactions for merchants that have been identified by their regulator as high-risk, but are willing to do so for payment processors. And, the structure obscures one of the major red flags of consumer fraud – return rates. Return rates measure the rate at which financial transactions are reversed because, for instance, the account to be debited has insufficient funds or the account holder claims the debit to be unauthorized. To the extent that a processor's transactions are returned, the rate of those returns will be measured not by a single merchant alone, but by many merchants in the aggregate. A fraudulent merchant's return rate, then, could be minimized by the fact that its rate is grouped together with the rates of other merchants, many if not all of whom could will be legitimate. Finally, because a payment processor is not a bank, it is exempt from many of the specific "know your customer" rules that govern banks. A processor may therefore be less likely to engage in the kind of due diligence of its customers that a bank would undertake.

This structure – in which a fraudulent merchant uses a payment processor as its entry point into the financial system – became clear to law enforcement and regulators only over time. And, only after many attorneys – private attorneys and government attorneys alike – often working independently and in different parts of the country, pressed forward with their investigations of fraudulent merchants.

To extend our earlier metaphor, as government played "whack-a-mole" with the merchants, it started to follow the moles' path through the financial system more closely. We noticed the payment processors. Following the path just a little further, we noticed the banks for the payment processors.

What emerged was our strategy. It is one that I believe to be creative and elegant. It is replicable and efficient. It is born of experimentation and based on collaboration. And, it is continually being refined and developed as we implement it.

The fraudulent merchants sent their fraudulent transactions through the payment processors. The payment processors, in turn, sent those transactions through their banks. The many merchants funneled their transactions to fewer processors; the processors funneled to even fewer banks. The banks were a "choke point" of sorts for fraudulent payments in the system, the narrow part of a funnel. If these relatively few banks were to take steps to prevent fraudulent transactions, then they would stop the flow of fraudulent transactions from the many merchants.

Focusing our efforts on the banks, then, could be highly efficient. One bank may have many processor customers, which in turn may have scores of merchant clients. One bank could affect hundreds of merchants. What is more, operating as they do in a highly regulated environment, banks have the infrastructure in place to engage in compliance efforts and to undertake internal due diligence. We are simply expecting the banks to do what they are already equipped and required to do.

What we are finding when we turn our attention to banks is illuminating. It turns out that some banks know a great deal about the processors who are their customers. Some also know a great deal about the merchants, who are not their customers, but their customers' customers. Much of that information is negative.

Here are some of the things that we are finding:

- Banks are acutely aware of the return rates for transactions associated with their customers. And, banks recognize that return rates can be a warning sign of an unlawful business. They will often seek more information about customers who have unusually high return rates.

- Banks will learn about a processor customer. They will learn about how the processor markets itself to merchants; how (or whether) it conducts its own due diligence on its merchants; and who its merchants are.

- Banks seek information about processors' merchant base, and get it. They can learn what the merchants' business is and how they operate.

- Banks communicate with each other and will tell one another when they see evidence of fraud. That is, a consumer's bank will tell a processor's bank that a transaction may be fraudulent.

This is significant information. Based on this type of evidence, we are identifying instances in which banks knew that they were processing payments for merchants engaged in unlawful activity or turned a blind eye to that fact.

What can we at DOJ do when we learn that banks are aware of or willfully blind to fraudulent transactions running through their operations? We can – and have – used traditional tools of law enforcement. They include, among other things, civil fraud statutes, like FIRREA and the Anti-Injunction Act. They can also include criminal statutes, if appropriate, whether they are bank fraud, wire or mail fraud, or Bank Secrecy Act provisions. Two examples of such enforcement, of which you are undoubtedly aware, can be seen in the Wachovia case and the First Bank of Delaware case. Because much of the investigative material in those cases is not public, I will not go into detail. Suffice it to say that, in both of those cases, the defendant banks admitted, in agreements resolving the regulatory, civil, and criminal actions against them, that they were either aware of or willfully blind to the suspicious transactions that went through their operations.

The success of the Wachovia and the First Bank of Delaware cases helped us to conclude that our strategy – of focusing on banks – made good sense. It was time to expand our efforts and to give it some focus. Earlier this year, with the full support of senior Department of Justice leadership – including Stuart Delery, the Assistant Attorney General for the Civil Division and Michael Bresnick, who is with us tonight, formerly the Executive Director of the Financial Fraud Enforcement Task Force – we in the Consumer Protection Branch did just that.

- We sent out subpoenas to banks that evidence suggested were doing business with payment processors that worked with high-risk merchants. We followed up with investigations when warranted. Those investigations continue, and, when they conclude, we will be in a position to make public announcements about how they have resolved.

- We built better channels of communication with other law enforcement agencies, like the FTC, the USPIS, and the FBI, and with banking regulators, like the CFPB and others, to share information and develop strategies about the payment system.

- We spread the word among U.S Attorney's Offices about the importance of this issue.

- We engaged with industry to make sure that the steps we took would not interfere with legitimate businesses or the efficient running of the payment system.

- We engaged with consumer advocates.

I believe that our efforts in dealing with fraud in the payment system exemplify the kind of law enforcement initiative that we at DOJ must undertake to be most effective.

- First, it is smart. By looking to the "choke point" in the flow of money in a fraudulent transaction, the effort focuses on cases and investigations that will

have the widest and most long-lasting impact. And, by focusing on objective, data-based red flags – most prominently abnormally high return rates – the effort can sharpen its aim only at the most likely fraud targets. We do not want to burden or deter lawful businesses from operating.

- Second, it leverages government expertise. We share information with other government agencies; they share information with us. We use every tool in our tool box. Some problems are best handled by regulators, some by law enforcement, some criminally, some civilly. Every agency is doing its part, and doing it based on its own authority.

- Third, it engages industry. Ultimately, all we are asking is that banks undertake the due diligence efforts that we believe they are already required to undertake and, when they do, to stop doing business with entities that are engaged in unlawful activity. In other words, banks are well positioned to handle this problem on their own. They can distinguish between the lawful and the unlawful businesses that seek their services, using guidance from regulators. And, they can avoid processing payments for fraudsters without interfering with legitimate businesses.

- Fourth, the initiative grew out of the creativity of prosecutors on the ground. We face daunting law enforcement problems. We need innovative solutions. We must encourage everyone to think differently, to experiment. We must give them the room to try new things. And, if these new things don't work, to try something else.

    - Here, I must recognize Joel Sweet. He is an Assistant U.S. Attorney, from Philadelphia, who is working in my office. Much of what I have discussed today, can be traced to his insight and to his foresight. He was the driving force in the Wachovia and First Bank of Delaware cases, but didn't stop there. He recognized this issue and stayed with it, pushing others to do more.

Before closing, I have things to ask of you. Law enforcement is only effective if it makes people's lives better. We can only do that if we know what is happening in the communities we serve and how our efforts affect those communities. Here is what I would like from you:

- We take the role of private attorneys general seriously. You litigate consumer protection cases. Share your findings with us. Let us know what you learn about fraudulent practices and the entities that engage in them. Don't assume we know.

- Reach out to local prosecutors. Reach out to regulators. Reach out to me and my office. Even beyond the litigation that you do, you are simply closer to the community than we are. We want to know – we need to know – what is

happening as it is happening. Recognize that we cannot always address the issues that you would like us to address. Our authority, our resources limit us. But, we certainly cannot address those issues if we don't know what they are.

- Work with industry. I will say that again. Work with industry. I think we can all agree that the best solutions to problems arise when all of the stakeholders work together. The banking industry has an interest in keeping fraudsters out of the payment system. Engage with it.

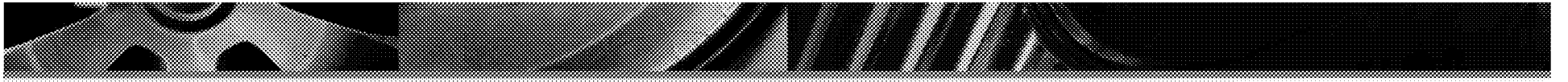
- Continue to dialogue with us. Criticize us; thank us. We need feedback to make sure that what we are doing is the right thing.

Thank you again for having me. It has been a pleasure. I look forward to continuing to work with you on important consumer protection issues.

Stopping Consumer Fraud Access to Payment Systems

Richard Goldberg
Assistant Director
Consumer Protection Branch
U.S. Department of Justice

The views expressed in this presentation are those of the presenter and do not necessarily reflect the views of the United States Department of Justice.



25 million Americans were victims of consumer fraud in 2011.

Consumer Fraud in the United States, 2011 FTC Staff Report of the Bureau of Economics, published April 2013, p. i.

Federal Trade Commission
PROTECTING AMERICA'S CONSUMERS

[redacted]
Tulsa, OK
74136[redacted]

Claim Number: GAO-751-23

January 13th, 2012

Lydia Parnes
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, D.C. 20580

Notification

The **Federal Trade Commission** has been established to monitor the sweepstakes companies operating inside of the United States. We are a **Consumer Protection Agency** that assists the recipients of sweepstakes awards such as you.

An agent from the **Federal Trade Commission** will direct you in receiving your award and inform you of security issues that you should be aware of. Please keep these suggestions in mind and if you have any concerns feel free to contact us at **877-907-2646 or 202-618-9119**

conditions of the policy payment.

When the courier arrives within 24 hours you will need 2 forms of ID and proof of deposit. The courier will then hand you an envelope with your award check from Bank of America, along with a 1099 Tax Exemption Form and a reimbursement check for your safe delivery insurance payment. This delivery will take place once you have posted the required deposit for the activation of the temporary insurance policy.
Sincerely,

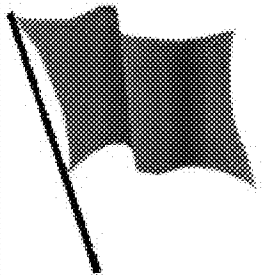
Lydia Parnes

Lydia Parnes
F.T.C. Chief of Staff
Fraud Prevention and Security Guidelines Dtp.

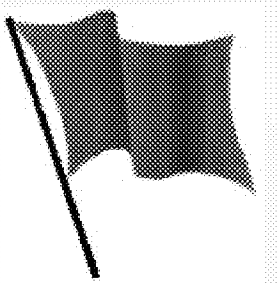
Fraud Facilitator Liability

- Do they know they are helping a merchant engage in consumer fraud?
- Are they turning a blind eye to clear signs that they are helping a merchant commit consumer fraud?

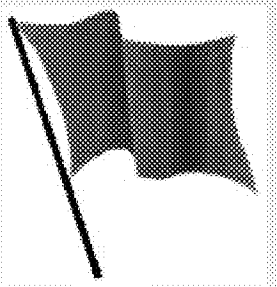
Where does the Third-Party Payment Processor fit in?



Regulator Warnings

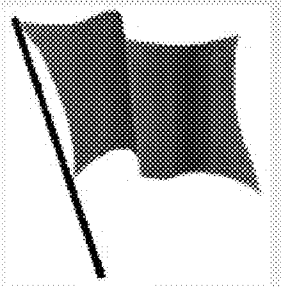


- FINCEN Advisory 2012-A010, "Risks Associated with Third-Party Payment Processors."
- Federal Financial Institutions Examination Counsel Bank Secrecy Act Anti-Money Laundering Examination Manual, Section on Third-Party Payment Processors.
- Guidance on Payment Processor Relationships, FDIC FIL-127-2008, November 7, 2008.
- Risk Management Guidance: Payment Processors, OCC Bulletin 2008-12, April 24, 2008.



Red Flags - Indicia of Fraud

- Return Rates - Both Unauthorized Returns and Total Returns
- Communications / Complaints from RDFIs (consumers' banks)
- Contacts from law enforcement



Red Flags - Indicia of Fraud

...continued

- How does the TPPP market itself?
  - Does it offer to provide ACH processing for merchants who have been blacklisted from credit card processing?
  - Does it offer to process RCCs for merchants who cannot process credit cards or ACH?
- Internet complaints, lawsuits, and cease and desist orders against merchants, Better Business Bureau Ratings and Warnings

Case Study: *United States v. Payment Processing Center, LLC*

- The government brought an injunction action to stop Payment Processing Center's operations
- PPC was a processor for merchants that included those that purported to offer government grants, prescription discount cards, travel programs, free gift cards, free computer
- PPC banked with Wachovia

Wachovia Bank - Court documents alleged:

- Processed hundreds of millions of dollars of RCCs for PPC and other payment processors
- PPC had a return rate over 40%
- Ignored red flags indicating that PPC serviced mass market fraudsters
- Ignored internal and external concerns about high return rates
- Wachovia failed to have an effective BSA/AML program in light of the high-risk nature of its third-party payment processor customers
  - Did not request detailed information about processors' merchant base
  - Did not have a detailed understanding of the processors' return rate history
  - Did not sufficiently scrutinize the processors' due diligence programs

Outcome

- Wachovia
  - Settled civil actions by DOJ, the OCC and a private class action by agreeing to pay more than $160 million in restitution to consumers, a $10 million fine to the U.S. Treasury, and $9 million to independent consumer protection education programs.
  - The government and Wachovia resolved a criminal investigation through a deferred prosecution agreement. United States v. Wachovia Bank, NA, (S.D. Fla.)
- Payment Processing Center, LLC
  - Company went out of business after government moved for an injunction under the Anti-Fraud Injunction Act. United States v. Payment Processing Center, LLC (E.D. Pa.)
  - Six individual owners of PPC convicted of federal felonies for operating an illegal money transmitting business. United States v. Donald Hellinger, et al. (E.D. Pa.).

Takeaways

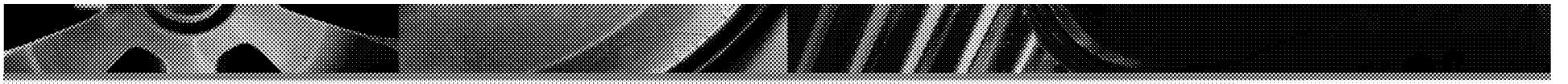
- Without significant due diligence and fraud controls, banks create enormous potential risks to consumers and, ultimately, themselves by allowing fraudsters to have direct access to the consumer's bank accounts .

Takeaways

- RDFIs (consumers' banks) play an important role in combating fraud in the payment systems by contacting ODFIs with concerns of suspicious activity and allegations of fraud.

Takeaways

- All banks should
  - report problematic merchants and processors to NACHA and law enforcement
  - File SARs
  - Help us do our jobs better
  - Stop processing for fraudsters



TARGET: [W]hen I was first at AmeriP.O.S., and I took a woman that lived in a trailer, her last whatever, $12,980, I went home and I thought about that, I was going, "God, I'm a bad guy, I'm a bad guy, I'm a bad guy." Right? Then, I thought about it, she's calling three other companies, if I didn't take the money, one of the other three companies is going to take the money. Now I've come to terms with that, and I realize this is what I've done, this is what I'm doing.

CI: You have no problem, right?

TARGET: I have no problem whatsoever.

CI: Okay.

TARGET: Done. That's all. Give me my, my check for $70,000 this month and I'm a happy guy.

U. S. Department of Justice

Civil Division

Assistant Attorney General *Washington, D.C. 20530*

November 21, 2013

TO: Staff of the Office of the Attorney General
Staff of the Office of the Deputy Attorney General
Staff of the Office of the Associate Attorney General

FROM: Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General
Civil Division

SUBJECT: Operation Choke Point

I. Introduction

In 2011 alone, approximately 25.6 million people —10.8 percent of American adults— were victims of consumer fraud. *See Consumer Fraud in the United States, 2011* (FTC Staff Report of the Bureau of Economics, published April 2013), p. i. Government authorities traditionally attack consumer fraud schemes through civil and criminal prosecutions against the principals who design and operate the schemes and the salespeople that misrepresent themselves to consumer victims. These cases play a critical role in achieving specific and general deterrence. Nevertheless, law enforcement recognizes that this traditional approach often results in "whack-a-mole" results: We shut down a fraudulent scheme and another pops up, often involving the same perpetrators.

In early 2013, the Civil Division, through the Consumer Protection Branch, launched Operation Choke Point as an initiative to fight consumer fraud more effectively, by attacking it at a broader and deeper level. The initiative represents a shift in enforcement strategy. Rather than attempting to stop fraud by prosecuting only fraudulent merchants, we seek to expand our focus to include that which is common to all consumer fraud schemes – the payment infrastructure used by fraudulent merchants to take money from victims' bank accounts.

Mass-market consumer frauds frequently draw funds from consumers' bank accounts based upon fraud-induced authorizations, and sometimes without even the pretext of authorization. Fraudulent merchants ideally want a direct relationship with a bank through which they can access the national payment systems, and, thus, consumers' bank accounts. Unfortunately for many merchants engaged in fraud, banks generally are reluctant to establish a direct relationship with them because of financial, legal, regulatory, and reputational risks associated with their businesses. To overcome this obstacle, fraudulent merchants work with third-party payment processors that serve as intermediaries to banks.

Third-party payment processors establish bank accounts in their own names to gain access to the payment systems. For a per-transaction or dollar-volume fee, third-party payment processors provide fraudulent merchants with access to the payment systems and consumers' bank accounts. Banks, in turn, charge the processors a fee for each transaction. The bank typically charges the processor a higher fee if the transaction is rejected or "returned."

Because banks are the sole entry point to the payment systems, banks can play a critical role in facilitating or thwarting consumer fraud. Banks are obligated under the Bank Secrecy Act and other laws and regulations to prevent illicit use of the payment systems in part by knowing their customers, monitoring transactions, and reporting suspicious activity. Based upon our experience and that of our law enforcement partners, as well as witnesses in our investigations and even bank counsel, we know that banks often delegate these duties to third-party payment processors that arguably are not subject to regulatory anti-fraud or anti-money laundering requirements. Where banks are confronted with obvious red flags of consumer fraud, they often take precautions to protect their own financial interests while callously ignoring ongoing harm to consumers.

This memo addresses the Civil Division's efforts, through the Consumer Protection Branch, during the past nine months to combat mass-market consumer fraud by focusing on payment system vulnerabilities, and particularly the roles banks and third-party payment processors play in facilitating the offenses. Our goal is to hold accountable those banks and third-party payment processors that turn a blind eye to, and profit from, taking and transmitting victims' money on behalf of fraudulent merchants. We hope that this will, in turn, deter other banks and third-party payment processors from engaging in this conduct and make the payment system safer for consumers.

II. Prior Efforts to Address Those Who Facilitate Fraud Through the Payment System

The critical role of third-party payment processors in mass-market consumer fraud schemes is not new to federal authorities. Federal Trade Commission ("FTC") staff report that virtually all of the mass marketing fraud schemes they investigate involve a third-party payment processor acting as an intermediary between the fraudulent merchant and a bank. For more than 10 years, the FTC has targeted processors based on evidence that the processors knew consumers were harmed by large numbers of fraudulent debit transactions. The FTC's efforts, however, are tempered by its limited civil remedies and a jurisdictional bar to it bringing actions against banks.

The Department of Justice also has recognized that fraudulent merchants use processors and other intermediaries to facilitate fraud, and has brought civil and criminal actions to address the problem. For example, in 2006, the United States Attorney's Office for the Eastern District of Pennsylvania obtained an injunction under 18 U.S.C. § 1345 against a payment processor that in less than 12 months had taken more than $60 million from consumers accounts without authorization. See United States v. Payment Processing Center, LLC, Civil Action 06-0725 (E.D. Pa.), dkt. 71. This matter implicated Wachovia Bank and eventually resulted in a criminal investigation, an Office of the Comptroller of the Currency ("OCC") investigation, and a private civil class action against the bank. Wachovia Bank processed unauthorized or otherwise fraud-

tainted debits against consumers' accounts on behalf of Payment Processing Center and three other payment processors. Wachovia agreed to pay more than $160 million in restitution to consumers, a $10 million fine to the U.S. Treasury, and a $9 million payment to independent consumer protection education programs. The government and Wachovia resolved the criminal investigation into Wachovia via a deferred prosecution agreement. See United States v. Wachovia Bank, NA, Criminal No. 10-10265 (S.D. Fla.). In 2012, the six owners of Payment Processing Center were convicted for operating an illegal money transmitting business. See United States v. Donald Hellinger, et al., Criminal No. 11-0083 (E.D. Pa.).

More recently, in United States v. Moneygram International, Inc., Criminal Action No. 12-291 (M.D. Pa.), prosecutors followed a similar strategy of combatting fraud by attacking the fraudulent merchants' payment infrastructure. Prosecutors discovered that Moneygram, a private money transmitter, had actual knowledge of a massive number of consumer complaints of fraud perpetrated by associated payment outlets. Rather than terminate the fraudulent outlets, Moneygram profited from them. The matter resolved with a deferred prosecution agreement and forfeiture and restitution of $100 million.

Similarly, in United States v. First Bank of Delaware, Civil Action No. 12-6500 (E.D. Pa.), prosecutors alleged that a bank violated the Financial Institutions Reform, Recovery and Enforcement Act, 12 U.S.C. § 1833a, by knowingly processing debit transactions against consumers' accounts on behalf of a large group of fraudulent Internet and telemarketing merchants – despite obvious signs of fraud. That case was resolved by the bank paying a civil money penalty of $15 million (half its shareholder equity) before surrendering its charter.

The Consumer Protection Branch and the U.S. Attorney's Office for the Eastern District of Pennsylvania recognized that these cases amounted to a breakthrough in law enforcement efforts to combat consumer fraud and initiated Operation Choke Point to apply the lessons learned from these cases nationwide.

III. Initiating Operation Choke Point

A. Initial Composition and Staffing

Operation Choke Point is dedicated to targeting banks and payment processors that facilitate consumer fraud by providing the means for fraudulent merchants to take and transmit consumer funds. The initiative brings together the Assistant U.S. Attorney who prosecuted the PPC, Wachovia, Hellinger, and First Bank of Delaware cases described above, and prosecutors from the Consumer Protection Branch ("CPB"), who have extensive experience prosecuting criminal and civil consumer fraud cases.

Choke Point is supported primarily by United States Postal Inspection Service ("USPIS") personnel embedded within CPB. USPIS has dedicated a full-time postal inspector and two analysts to the effort, along with a fraud team leader to facilitate further USPIS assistance. The FBI has assigned agents to one of our criminal investigations, and is providing administrative support. Agents from the FDIC-OIG and U.S. Secret Service also are assigned to specific cases.

[redacted]

[redacted]

B. Statutes and Legal Theories

We have initiated each Choke Point investigation as a civil investigation under the Financial Institutions Reform, Recovery and Enforcement Act, 12 U.S.C. § 1833a ("FIRREA"), and the Anti-Fraud Injunction Act, 18 U.S.C. § 1345 ("Section 1345"). As described below, these statutes provide both a mechanism for investigating potentially fraudulent behavior as well as remedies to hold wrongdoers accountable.

Our investigations are opened as *civil* FIRREA matters to leave open our options for pursuing wrongdoing. A preponderance of the evidence standard applies to each element of a civil FIRREA claim. A higher, "beyond a reasonable doubt" standard will apply to any criminal prosecutions we bring. Because the elements of civil and criminal claims coincide in this context, our civil investigations pursue the same types of evidence as we would seek in a criminal investigation. To the extent that our civil efforts unearth evidence of egregious, readily-provable criminal conduct, we have opened criminal investigations.

1. FIRREA

FIRREA provides a civil cause of action for violations of certain enumerated criminal offenses, one of which is wire fraud "affecting a federally-insured financial institution."

a. FIRREA Elements

i. Wire Fraud

We contemplate that any FIRREA case we bring will be predicated on wire fraud violations. If so, we will need to satisfy wire fraud's *mens rea* requirement – proving that the defendant acted with intent to defraud.

In some of our cases, proving that a bank or processor acted with intent to defraud will not be a challenge because employees expressly admitted in emails, memos, or other written documents that they believed or suspected that the merchant was engaged in fraud against consumers, but nonetheless continued to process payments in return for significant fees. Most of our cases, however, will be based upon bank officials' or processors' willful blindness to obvious red flags of fraud. Under federal mail and wire fraud statutes, "knowing" participation in unlawful conduct may be based upon evidence that a defendant "purposely closed his eyes to avoid knowing what was taking place around him." United States v. Schnabel, 939 F.2d 197, 203 (4th Cir. 1991), cited favorably in Global-Tech Appliances, Inc. v. SEB S.A., 131 S. Ct. 2060, n. 9 (2011).

Several targets have received large numbers of affidavits from consumers swearing that transactions were unauthorized. Many banks conducted some level of research or due diligence

on merchants and discovered – but nonetheless ignored –substantial evidence of fraud. Others disregarded evidence of fraud and conducted no due diligence at all, despite regulatory requirements. Among the most compelling evidence are letters from other banks demanding that the target bank stop taking money from consumers' accounts without authorization.

Bank regulators have clearly communicated to the industry the red flags that suggest that a merchant may be engaged in illicit conduct. For example, the Financial Crimes Enforcement Network issued guidance to financial institutions on the "Risk Associated with Third-Party Payment Processors in October 2012. The advisory stated that "Payment Processors providing consumer transactions on behalf of telemarketing and Internet merchants may present a higher risk profile to a financial institution than would other businesses." See FINCEN Advisory 2012-A010, "Risks Associated with Third-Party Payment Processors."). The first red flag listed in the advisory stated:

> *Fraud*: High numbers of consumer complaints about Payment Processors and/or merchant clients, and particularly high numbers of returns or charge backs (aggregate or otherwise), suggest that the originating merchant may be engaged in unfair or deceptive practices or fraud, including using consumers' account information to create unauthorized RCCs or ACH debits. Consumer complaints are often lodged with financial institutions, Payment Processors, merchant clients, consumer advocacy groups, online complaint Web sites or blogs, and governmental entities such as the Federal Trade Commission and state Attorneys General.

The "returns" described in the advisory mean financial transactions that are reversed and the funds returned to the account from which they were debited. In other words, returns are a bank's way of "undoing" a debit transaction against an account, in this case the account of a consumer. Returns may be processed for a number of reasons, including if the transaction was unauthorized or there were insufficient funds in the account.

Transactions returned because they were unauthorized are particularly suspicious. NACHA, the industry self-regulating body that governs electronic fund transfers (automated clearing house or "ACH" transactions), sets limits on the number of transactions that can be unauthorized for a given merchant as 1 percent (and has recently proposed lowering the threshold to one-half of one percent). The 1 percent threshold is 33 times the 2012 unauthorized return rate for all ACH debits.

Consistently high total return rates also indicate that a bank and processor have abdicated their responsibility to ensure that their accounts are being used to process legitimate business transactions. NACHA has stated that the national average total return rate is 1.38 percent. A number of our targets have seen merchant total return rates reach 30 to 70 percent. These rates falling far outside the norm occur when merchants attempt to debit the accounts of consumers without an adequate basis.

Despite seeing these clear red flags and other evidence of fraud, however, many of our targets continued business as usual without stopping the consumer harm. By continuing to

process transactions for these fraudulent merchants while turning a blind eye to the fraudulent proceeds passing through their hands, banks and payment processors aid and abet the fraudulent schemes under Title 18, United States Code, Section 2.

ii. "Affecting a Federally Insured Financial Institution"

The fraud schemes we are investigating affect financial institutions in several ways. First, consumers' banks suffer loss, or risk of loss, when consumers demand to be reimbursed for debits procured through fraud. See United States v. The Bank of New York Mellon, - F. Supp. 2d - , 2013 WL 1749418, *12 (S.D.N.Y. April 24, 2013) (stating that "a bank can be 'affected' when a scheme exposes the bank to 'a new or increased risk of loss,' even without a showing of actual loss.") (citations omitted).

Second, our target banks—which provide fraudulent merchants with bank accounts—suffer loss, or risk of loss, when consumers' banks seek to be reimbursed for transactions procured by fraud. This creates FIRREA liability even though the "affected financial institution" was the perpetrator of the offense. Id. at *14-15 (stating that FIRREA liability may be imposed when a financial institution commits a wire fraud scheme that affects itself).

Third, our target banks are at great risk of reputational harm from becoming known as institutions that help fraud schemes to victimize consumers. This too creates FIRREA liability. Id. at 11-12 (finding allegation of adverse reputational effect, among other effects, sufficient for a FIRREA case).

b. FIRREA Investigative Tools

FIRREA also provides the primary tools we use to investigate Operation Choke Point cases. The statute authorizes issuance of subpoenas and taking of testimony under oath to gather evidence of potential violations. See 12 U.S.C. § 1833a(f)(1). We can share the material we obtain through these tools with criminal investigators and with other federal agencies.

c. FIRREA Penalties

FIRREA's penalty provisions provide that the United States may recover civil money penalties of up to $1 million per violation, or for a continuing violation, up to $1 million per day or $5 million, whichever is less. See 12 U.S.C. § 1833a(b)(1)-(2). The statute further provides that the penalty can exceed these limits to permit the United States to recover the amount of any gain to the person committing the violation, or the amount of the loss to a person other than the violator stemming from such conduct, up to the amount of the gain or loss. See 12 U.S.C. § 1833a(b)(3).

2. Section 1345

Section 1345 authorizes the government to bring a civil action to enjoin ongoing mail, wire and bank fraud offenses. As with FIRREA, any Section 1345 case we bring will be predicated on wire fraud violations, and we will need to satisfy the *mens rea* requirement for wire fraud—proving that the defendant acted with intent to defraud. Depending on the circuit in which we bring the case, we would either need to satisfy a preponderance standard or a probable

cause standard. In either event, the analysis described above with respect to wire fraud for FIRREA purposes would apply.

The statute explicitly authorizes asset restraints to prevent dissipation of bank fraud proceeds, 18 U.S.C. § 1345(a)(2), and case law has interpreted the provision to authorize asset freezes in mail and wire fraud cases as well. See, e.g., United States v. DBB, Inc., 180 F.3d 1277, 1283 (11th Cir. 1999); United States v. Payment Processing Center, LLC, 435 F. Supp. 2d 462 (E.D. Pa 2006); United States v. Fang, 937 F. Supp. 1186, 1192 (D. Md. 1996).

C. Investigative Methods and Case Development

We have served FIRREA subpoenas on approximately fifty banks and six payment processors. We picked these banks and processors based upon evidence that they had facilitated, or had been solicited to facilitate, fraud schemes. The evidence included statements of cooperating witnesses, tips and referrals from defrauded consumers found on the FTC's Consumer Sentinel database, FTC staff conducting merchant and processor investigations, NACHA (the self-regulating electronic payment network), private class action lawyers, and banks whose consumer customers have been victimized.

Our initial subpoenas have sought general information sufficient to identify third-party payment processors and merchants with high levels of returns, documents relating to complaints about fraud and unauthorized debits, and other specific information to allow us to determine whether further investigation is warranted. To avoid over-breadth and remain focused only on the entities that pose the highest risk to consumers, we have defined the term "merchant" to include only telemarketing, Internet, and mail merchants – thereby excluding broad categories of merchants with low fraud risks. We have served the subpoenas along with copies of the most recent third-party payment processor guidance and advisory material from the FDIC, OCC, and FinCEN. This assists the banks to understand the nature of our investigation and the basis of our concerns. We have sometimes also requested that the bank's federal regulator provide recent examination reports and exam work papers relating to third-party payment processors, excessive return rates, and related issues.

Upon receipt of subpoena returns, CPB and Postal Inspection Service staff have reviewed the records to determine whether they contain evidence of fraud by merchants, processors and the bank. We often also have engaged in a constructive dialogue with the bank and its counsel to further explore whether the bank may unwittingly be processing fraudulent transactions, and we have given banks examples of conduct we are aware of that may pose fraud risks to consumers. Depending upon the nature of the evidence we have found, we have made a decision in each case to either open a civil and/or criminal investigation, or close the file.

IV. Progress and Impact

In the nine months since Operation Choke Point commenced, we have laid the groundwork to achieve significant progress in two areas: (1) investigations leading to civil and criminal actions; and (2) engagement with other government components, regulators, and industry, to identify and address weaknesses in the payment systems that lead to consumer fraud. With respect to investigations and actions, we have opened criminal investigations of four payment processors and their principals, as well as a bank and responsible bank officials. We also have opened civil FIRREA investigations into more than ten banks and processors, and we are attempting to negotiate consent decrees with at least three of these entities. Several banks and payment processors — after receiving our subpoenas and understanding our concerns — have stopped processing payments for entities they believe or suspect are fraudulent merchants, thereby providing immediate and enduring relief to millions of consumer fraud victims and would-be victims.

We measure success primarily by civil and criminal actions filed and resolved. In this circumstance, however, success also must be measured by the number of fraud schemes that have been stymied due to a cut-off of access to the payment system, and the innumerable consumers who will not become victims. We have a long way to go and a substantial amount of work before us. Nevertheless, all signs indicate that Operation Choke Point is beginning to have a material effect on the behavior of banks doing business with illicit third-party payment processors and fraudulent merchants. We believe we already have denied fraudulent merchants access to tens, if not hundreds, of millions of dollars from consumers' bank accounts, and that amount will increase daily and indefinitely. This substantial level of deterrence is corroborated by payment processors and banks that have informed us that they have stopped providing services to merchants that they believe or suspect are fraudulent; by undercover recordings of fraudulent operators; and by FTC attorneys describing increased cooperation by banks and processors in FTC investigations.

Most importantly, we have learned directly from many sources that banks that have received our subpoenas, and others aware of our efforts, are scrutinizing their relationships with high risk third-party payment processors. In several cases, after receiving a subpoena, banks and processors have self-disclosed potentially problematic relationships and have informed us that they have taken corrective action. We have encouraged this type of positive conduct. As a consequence, we have several matters in which the bank or processor has agreed to stop bad conduct and has indicated an interest in attempting to negotiate an agreed resolution. We currently are attempting to negotiate settlements with these entities.

Our efforts also are being noticed in the public interest and banking communities. Front page articles in the Wall Street Journal on August 7, 2013,[1] the New York Times on June 10, 2013,[2] and the American Banker on September 25, 2013,[3] have educated the public and, more

[1] "Probe Turns Up Heat On Banks," available at http://online.wsj.com/article/SB10001424127887323838204578654411043000772.html

[2] "Banks Seen as Aid in Fraud Against Older Consumers," available at http://www.nytimes.com/2013/06/11/business/fraud-against-seniors-often-is-routed-through-banks.html?pagewanted=all&_r=0

[3] "Banks Pressured to Settle in Online Lending Probe," available at

importantly, the banking and payment processor industries, about our initiative and objectives. The articles are a "deterrence multiplier" because, as we have learned from many sources, the articles have alerted banks to the risks of implication in consumer fraud schemes and have been the catalysts to encourage banks to take proactive steps to ferret out fraud from the payment systems. More recently, our efforts to bring together various government components to address payment system fraud was recognized in a laudatory letter to DOJ and regulatory agencies signed by 30 national and local consumer protection organizations.[4]

V. Choke Point In Action: Our Ongoing Investigation of [redacted]

[redacted]

http://www.americanbanker.com/issues/178_186/banks-pressured-to-settle-in-online-lending-probe-1062408-1.html

[4] Letter to Attorney General Holder and others from Consumer Protection Organizations, dated October 24, 2013.

VI. Strategy for Resolutions

We intend to try to reach consent agreements with as many targets as possible as quickly as possible. If we obtain and announce consent decrees with meaningful injunctive and civil penalty relief, we hope this will inspire other banks and processors to look closely at their merchant relationships and deter them from processing payments for suspected fraudulent merchants. As mentioned above, where we have developed evidence of particularly egregious criminal conduct, we have opened criminal investigations, and will continue to do so as new evidence of criminal conduct arises.

VII. Our Effects on the Pay-Day Lending Industry

After serving our FIRREA subpoenas, a handful of lawyers representing subpoena-recipient banks contacted us and stated that their clients acknowledged having potentially problematic payment processor relationships. Several of these problematic relationships stemmed from merchants involved in Internet payday lending. According to the banks' lawyers, the payday lenders experienced astronomically high return rates and engaged in suspicious business relationships that should have, and in some cases did, raise red flags for the banks' employees.

Self-disclosure from these banks was not the first that we had heard of widespread consumer fraud and abuse in the Internet payday lending industry. Consumer advocacy groups, state attorneys general, and public interest and research organizations such as the Pew Foundation, have decried Internet payday lending as a leading source of harm to the public,

particularly the working poor. In particular, they have pointed out that many of the complaints they receive "allege fraud – including companies initiating loans or withdrawing money without permission, or calling to collect a debt that the consumer claims was never owed." BBB online warning, "Fast Cash May End Up Costing Consumers."

Enforcement efforts by state attorneys general have been frustrated by online payday lenders purporting to operate offshore. For example, several states have laws prohibited payday lending or placing limits on the interest rates these lenders can charge. The efforts by these states' attorneys generals to enforce these laws have been stymied either because these allegedly offshore entities either claim not to be subject to state jurisdiction or because these states lack the jurisdiction or power to pursue them overseas. Other lenders have affiliated with federally-recognized Indian tribes that claim sovereign immunity as a defense against state and federal actions.[5]

As word began to spread through the financial industry about Operation Choke Point, banks began scrutinizing their merchant relationships in a much more focused way than ever before. Like the banks that received our subpoenas, many of these other banks have determined that fraudulent online payday lenders, with their extraordinarily high return rates and suspicious efforts to conceal their true identities, present an unacceptable risk to the bank. We have received word from multiple sources, corroborated by undercover recordings of those in the fraudulent payday lending industry, that banks are terminating large swaths of deceptive payday lending businesses from their account portfolios. Some of these banks have ceased doing business with all Internet payday lenders, but we are unaware of any terminated merchants that operated in a wholly legitimate fashion with terms that are transparent to consumers.

Those profiting from the Internet payday loan industry are unhappy about the decisions of many banks to stop processing debits against consumer banks account on behalf of payday lenders. Some blame Operation Choke Point and other efforts by law enforcement and regulators for their loss of business. Recent editorials in the American Banker, and a letter to both DOJ and the FDIC from several members of the U.S. House of Representatives,[6] accuse us of targeting the entire Internet payday lending industry and of sweeping too broadly with our

[5] Internet payday lenders affiliated with tribes, and the tribes themselves, take the position that state lending laws and many federal lending and consumer protection laws do not apply to their lending activities. They claim that tribal sovereignty shields them from state usury and consumer protection laws. Although many tribal-affiliated lenders claim to follow some federal laws voluntarily, such as the Truth in Lending Act, they claim federal laws do not apply to them absent an express Congressional statement to that effect. There is considerable disagreement in the courts about the applicability of laws of general applicability to Indian tribes. The Office of Tribal Justice has also advised us that this issue affects numerous areas of the Department's work, and there is no clear Department position on it. In the most recent case on the matter, a magistrate judge held that the FTC Act, the Truth in Lending Act, and the Electronic Funds Transfer Act – all laws of general applicability – applied to tribal business entities. *See FTC v. AMG Services, Inc.*, 12–cv–00536 (D. NV July 16, 2013).

[6] Information obtained from a cooperator suggests that both of these efforts were directed and funded primarily by the owner of a particular payment processor presently under investigation.

enforcement brush. These interests incorrectly contend that our efforts are directed at the entire Internet payday lending industry, including purported lawful lenders.[7]

Our initiative is focused exclusively on fraud. Because of our efforts, many banks have realized that they have opened the payment systems to potentially fraudulent merchants without sufficient due diligence and monitoring. Some banks have recalibrated their risk analyses and refined their "know your customer" processes. As a result, processors and merchants face additional scrutiny from banks, which are now more focused on the legal, systemic, and reputational risks associated with these relationships. We recognize the possibility that some banks may decide to exit relationships with payday lenders that claim to be operating lawfully. We do not, however, believe that this possibility should alter our investigative activities. Addressing that situation – if it exists – should be left to the individual payday lenders who presumably can present sufficient information to a bank to convince the bank that its lending operation is lawful and a worthy risk.

IX. Collaboration In Support of Our Consumer Protection Objectives

We recognize that exploitation of the payment systems by mass market fraudsters cannot be stopped by the efforts of CPB attorneys, paralegals, agents, and analysts working on our initiative alone. To maximize our reach, and to share the knowledge and experience we are gaining, we actively solicit the participation of U.S. Attorney Offices. Presently we are working jointly or conferring with AUSAs in the District of Nevada, the Middle District of Florida, the Eastern District of Virginia, the Northern District of Georgia, the Eastern District of North Carolina, the District of North Dakota, the Southern District of New York, and the Eastern District of Pennsylvania. We are contemplating cases with the Central District of California, and the Western District of Texas.

Equally important, we recognize that litigation alone cannot solve this problem. Consistent with the objectives of the Financial Fraud Enforcement Task Force, we are making significant efforts to engage other agencies -- including bank regulators and private entities with an interest in the security of the payment systems -- to support our efforts. We are deeply engaged in discussions about how to best address payment systems fraud, and we are providing information and ideas to support efforts to address these problems using each agency's own authority and tools. We also are attempting to address common concerns by creating a platform for communication with disparate elements of the payment systems to address vulnerabilities.

Our engagement and collaboration efforts include in part:

Federal Trade Commission: The FTC's efforts in this area predate our own, and not surprisingly our agencies work closely. Through information gleaned from the FTC's

[7] On September 20, 2013, Civil Division Deputy Assistant Attorney General Maame Ewusi-Mensah Frimpong briefed House of Representatives Majority staff on Operation Choke Point. In light of concerns that had been raised by letter, Ms. Frimpong informed the staff members that the initiative pursues only those banks and processors that have engaged in unlawful conduct. House staff members later requested that Stuart Delery, Assistant Attorney General for the Civil Division, provide a similar briefing, but it was determined that Ms. Frimpong's briefing had been extremely thorough and that there was no further public information that could be provided in a second briefing. On November 21, 2013, Ms. Frimpong provided a similar briefing to House Minority staff.

many actions against fraudulent merchants, we have identified several bank and processor investigatory targets. The FTC has assigned its principal payment processor expert to work as a SAUSA on one of our criminal cases.

Other bank regulators: The FDIC, OCC, and Federal Reserve Board all regulate the banks that we are investigating. We are in communications with these regulators with respect to specific banks. We also are engaged with these agencies about broader issues, such as the potential regulation of remotely-created checks (payment devices frequently used to commit fraud), proposed guidance to banks, and their own enforcement matters.

Treasury Department: The Department of Treasury's Office of Terrorist Financing and Financial Crimes has taken a special interest in Operation Choke Point. The Office, which is charged with combatting illicit use of the banking system and money laundering, has requested information and data from our initiative to develop legislative and/or regulatory cures to prevent payment systems fraud. We have tried to focus Treasury on significant regulatory gaps relating to third-party payment systems that implicate our ability to prosecute criminals under 18 U.S.C. § 1960, which prohibits the operation of illegal money transmitting businesses.

Federal Reserve Bank of Atlanta: This bank serves as a primary clearing house for ACH and check transactions. We have developed a strong working relationship with several officials at the bank who are concerned about payment systems fraud risks and who have committed to working with us on these matters. We also receive information from the bank that assists us in identifying potential targets.

NACHA: The entity created by the banking industry to set rules and supervise the ACH payment system has become an ally in our efforts to protect consumers. At our request, NACHA's General Counsel, Jane Larimer, provided a detailed presentation at DOJ to more than 100 government attorneys and investigators concerning the operation of the ACH payment system. NACHA has provided information that has assisted us to identify potential investigatory targets. Most importantly, following in-depth discussions concerning the significance of return rates, NACHA recently issued proposed rule changes that would lower the return threshold requiring banks to take action against merchants – a significant step in consumer protection.

In addition to these efforts, through DOJ's Payment Systems Fraud Working Group, we are working with the Federal Reserve Board and the Federal Reserve Bank of Atlanta to address the misuse of remotely-created checks or ("RCCs") a payment instrument used frequently to

perpetrate consumer fraud. RCCs are unsigned check instruments created by third-parties that pass through the payment systems based upon purported authorizations by consumers. RCCs are the fraudulent merchant's payment device of choice because, unlike credit cards and ACH debits, they are unmonitored as they move through the payment system. Support is growing among a variety of interested parties to further restrict or eliminate the use of RCCs from the payment systems.

Finally, our public education outreach is increasing. We recently addressed more than 300 public interest attorneys at the annual conference of the National Consumer Law Center. We also recently addressed more than 100 bank executives on the subject of payment systems fraud at an event hosted by the Federal Reserve Bank in Atlanta. We also presented before the New York External Fraud Committee, a New York City association of dozens of bank officials, regulators and law enforcement devoted to ferreting out fraud from the banking system. And we regularly conduct trainings and presentations for federal and state bank examiners through the Federal Financial Institutions Examination Council, which is the interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. We estimate that more than 1,000 bank examiners have attended our presentations concerning third-party payment processors and consumer fraud.

From: Taylor, Elizabeth G. (OAAG)
Sent: Thursday, November 21, 2013 5:30 PM
To: Frimpong, Maame Ewusi-Mensah (CIV)
Cc: Martinez, Brian (OAAG)
Subject: RE: Third-Party Payment Processors Initiative (Operation Chokepoint)

This is great Maame. Thanks for this memo and for this great work.

From: Frimpong, Maame Ewusi-Mensah (CIV)
Sent: Thursday, November 21, 2013 11:42 AM
To: Thompson, Karl (OAG); Jacobsohn, Robin (ODAG); Starks, Geoffrey (ODAG); Taylor, Elizabeth G. (OAAG); Martinez, Brian (OAAG)
Cc: Olin, Jonathan F. (CIV); Wilkenfeld, Joshua (CIV)
Subject: Third-Party Payment Processors Initiative (Operation Chokepoint)

Hi –

Please see attached a memo giving an overview of our 3PPP Initiative (also known as Operation Chokepoint). I am also attaching a speech the Branch Director recently gave on this topic, and two (virtually identical) Powerpoint presentations our attorneys have given to regulators and bank compliance executives on this topic.

Happy to discuss or answer any questions you may have. Thank you for your interest.

Regards,
Maame

Maame Ewusi-Mensah Frimpong
Deputy Assistant Attorney General, Consumer Protection Branch
Civil Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Room No. 3129
Washington, DC 20530
[redacted]

To: Bresnick, Michael J (ODAG)[redacted]@usdoj.gov]
From: Benardo, Michael B.
Sent: Wed 1/18/2012 9:17:51 PM
Subject: Re: meeting

OK, thanks!

From: Bresnick, Michael J (ODAG) [mailto:[redacted]@usdoj.gov]
Sent: Wednesday, January 18, 2012 01:30 PM
To: Benardo, Michael B.; Sherrill, Gary L.; Davidovich, John A.; Alessandrino, Matthew **T.**
Subject: RE: meeting

Thanks a lot, Mike. The meeting time is still being worked out—that's why I haven't sent out a formal invitation yet—but it's currently looking like we'll start around 11:30. Sorry I can't be more specific, but that's the most current information I have. I will get back to you when I know more about timing, and when the agenda is set.

From: Benardo, Michael B. [mailto:[redacted]@FDIC.gov]
Sent: Wednesday, January 18, 2012 12:08 PM
To: Bresnick, Michael J (ODAG); Sherrill, Gary L.; Davidovich, John A.; Alessandrino, Matthew **T.**
Subject: Re: meeting

I'd be happy to. What time?

From: Bresnick, Michael J (ODAG) [mailto:[redacted]@usdoj.gov]
Sent: Wednesday, January 18, 2012 11:55 AM
To: Benardo, Michael B.; Sherrill, Gary L.; Davidovich, John A.; Alessandrino, Matthew **T.**
Subject: meeting

Hello gentlemen: I just wanted to give you a heads up that the Financial Fraud Enforcement Task Force is about to start a new working group focusing on consumer protection issues. We are currently planning to have our inaugural meeting next Wednesday, January 25. I have not been able to send out a formal invitation yet because we are still working out the details. The current plan is to have the new group formally announced to the public at a press conference immediately preceding the actual meeting. One of the issues I'd like to discuss at the meeting is third party payment processors. Mike, would you be interested in spending about 15 minutes with Joel Sweet talking about the dangers that tppps pose to banks, citing examples such as SunFirst, Wachovia, First Bank of Delaware as examples?

Thanks,

Mike

To: Goldberg, Richard ([redacted]@usdoj.gov]; Bresnick, Michael J (ODAG[redacted]@usdoj.gov]; Frimpong, Maame Ewusi-Mensah ([redacted]@usdoj.gov]; Blume, Michael S. (CIV[redacted]@usdoj.gov]
From: Soneji, Sabita J. (CIV)
Sent: Wed 5/30/2012 2:09:17 PM
Subject: RE: CPWG Update

Thanks, everyone. Rich, I think your anticipated payment processor discussion sounds great…and adding FBI and FINCEN makes a lot of sense, if feasible.

Lois is a great fit, too.

From: Goldberg, Richard
Sent: Wednesday, May 23, 2012 3:58 PM
To: Bresnick, Michael J (ODAG) (JMD); Soneji, Sabita J. (CIV); Frimpong, Maame Ewusi-Mensah (CIV); Blume, Michael S.
Subject: RE: CPWG Update

Great.

Lois Greisman said that she or someone from her shop can handle the part we had in mind for Harris. In looking at the agenda, I think she would be more appropriate to address the issue for the NGOs than Harris anyway.

From: Bresnick, Michael J (ODAG) (JMD)
Sent: Wednesday, May 23, 2012 2:06 PM
To: Goldberg, Richard; Soneji, Sabita J. (CIV); Frimpong, Maame Ewusi-Mensah (CIV); Blume, Michael S.
Subject: RE: CPWG Update

Thanks, Rich. I think adding FBI (Tim Gallagher?), which is currently mining data from the FIC for TPPP cases, and FinCEN (Kevin Whalen) to this discussion would be helpful as well.

Mike

From: Goldberg, Richard (CIV)
Sent: Wednesday, May 23, 2012 12:49 PM
To: Soneji, Sabita J. (CIV); Bresnick, Michael J (ODAG); Frimpong, Maame Ewusi-Mensah (CIV); Blume, Michael S. (CIV)
Subject: RE: CPWG Update

Good afternoon. I spoke with Harris, who is checking into whether he can attend. He does not know whether FTC will pay for him to travel for the meeting and, in the alternative, he is checking to see if a past CLU chief or someone else can address his topic.

Re: my payment processor piece, I was anticipating a discussion of:

1) Cramming

a. Progress on the cramming front re: voluntary compliance,

b. FTC's case against BSG,

2) Targeting of third party payment processors,

a. Reminder: these entities process victim payments through ACH, third party checks, credit cards, etc., despite notice of fraud,

b. We are collecting a critical mass of agents and prosecutors to work cases,

c. We are collecting cases with meat on the bones to handle/refer,

3) Money Service Businesses ("MSBs")

a. Western Union, MoneyGram, Green Dot, and others are facilitating fraud by transmitting victim funds to offenders,

b. MoneyGram is now under FTC order,

c. There are isolated incidences of corrupt outlets set up to process payments,

d. MSBs have information that may be helpful to law enforcement, including ID of

recipient,

e. MSB complaint data coming into Sentinel,

f. MSBs may be willing to limit funds transmitted to certain countries based upon fraud emanating therefrom.

I have a call into Lois and will ask her if she'd like to put someone up to discuss any one of these topics, including FTC's BSG case or MSBs. Please let me know if these topics are what everyone has in mind. Thanks.

From: Soneji, Sabita J. (CIV)
Sent: Wednesday, May 23, 2012 12:17 PM
To: Bresnick, Michael J (ODAG) (JMD); Frimpong, Maame Ewusi-Mensah (CIV); Blume, Michael S.; Goldberg, Richard
Subject: CPWG Update

Hello CPWG Team –

Just wanted to let you know where things stand on the agenda. I think we are in good shape, but we may need a little more prodding in the coming days to make this come together.

Here are the leads for each part of the meeting:

1:00-1:05pm: Welcome and Introductory Remarks [Mike Bresnick or the Co-Chairs]

1:05-1:50pm: Short Term Priorities and Deliverables Discussion

•□□□□□□□ Third-Party Payment Processors [Rich Goldberg will take the lead. Joel Sweet is unavailable. Anyone else?]

•□□□□□□□ Payday Lending [I asked FTC to take the lead on this. Have not heard back yet.]

•□□□□□□□□ Fraud on Servicemembers [Civil and CFPB can take the lead.]

1:50-2:10pm: Outreach Initiatives

•□□□□□□□□ Co-Chair Andre Birotte to discuss recent consumer protection summit in Los Angeles

•□□□□□□□□ FTC to discuss upcoming Common Ground Conference in Chicago [David Vladeck]

•□□□□□□□□ USTP to discuss upcoming consumer protection event in Chicago [Mike Bresnick, Did you confirm Sandra Rasnak will join?]

2:10-2:20pm: Open Discussion/Next Steps

Meeting with Consumer Advocates

-

2:30-3:00pm: Consumer Advocate Presentation: Payday Lending [Ira Rheingold of NACA will take the lead.]

3:00-3:30pm: Appropriate Matters for Referral to Federal Law Enforcement [Mike Blume and Rich, Can you confirm Harris Senturia of the FTC and someone from Consumer Protection Branch will take the lead?]

Let me know if we have the right point people on these and if you have any additional suggestions.

Thanks!

Sabita

To: Bresnick, Michael J (ODAG)[redacted]@usdoj.gov]
From: Fishman, Paul (USANJ)
Sent: Thur 5/31/2012 9:06:36 PM
Subject: FW: RSVP: Consumer Protection Working Group Meeting---June 1, 2012
CPWG June 1 Meeting Draft Agenda.docx

Mike –

Can't make it tomorrow I'm afraid. Can I get a back brief on Monday?

Thanks

PF

From: Soneji, Sabita J. (CIV) [mailto[redacted]@usdoj.gov]
Sent: Thursday, May 31, 2012 5:03 PM
To: Alessandrino, Matthew; Arterberry, John (CRM); Benardo, Michael; Birotte Jr., Andre (USACAC); Blume, Michael S. (CIV); Braunstein, Sandra; Bresnick, Michael J (ODAG) (JMD); Breuer, Lanny A. (CRM); Buretta, John (CRM); Bylsma, Michael; Chua, Michelle; Colucci, Nicholas; Davidovich, John; Delery, Stuart F. (CIV); Dukes, Susan; Dunleavy, Hugh; Evans, Carol; Fishman, Paul (USANJ); Freis, James; Frimpong, Maame Ewusi-Mensah (CIV); Gallagher, Timothy A. (FBI); Garcia, Sandra; Goldberg, Richard (CIV); Graber, Geoffrey (CIV); Greisman, Lois; Hagan, Deborah; Halperin, Eric (CRT); Hamel, William; Harwood, Charles; Haynes, Patricia; Kelly, Thomas; Knox, Jeffrey (CRM); Kreisher, Todd; Leon, Glenn (CRM); Markus, Kent; Martinez, Brian (OAAG) (JMD); McGovern, Kathleen (CRM); McInerney, Denis (CRM); McPherson, James; Merritt, Cynthia; Miller, Steven; Monica Vaca; Morris, Lucy; Olin, Jonathan F. (CIV); Patterson, Jodi; Perez, Thomas E (CRT); Raman, Mythili (CRM); Raper, Troy; Rasnak, Sandra (USTP); Rebein, Scott; Riordan, Bruce (USACAC); Rivera, Mike; Rosen, Paul (CRM); Rusch, Jonathan (CRM); Schultz, Vicki (CRT); Senturia, Harris; Sherrill, Gary; Smith, Mary L. (CIV); Smith, Tyler; Soneji, Sabita J. (CIV); Stegman, Matthew (OAAG) (JMD); Stipano, Dan; Suleiman, Daniel (CRM); Susan Stocks; Sweet, Joel (USAPAE); Tighe, Kathleen; Vanderburg, Pamela J. (FBI); Vladeck, David; Washington, Rachel; West, Tony (OAAG) (JMD); Whalen, Kevin; White, Clifford (USTP); [redacted]@usss.dhs.gov; [redacted]@frb.gov; [redacted]@fincen.gov; Susan Stocks; [redacted]@fincen.gov; [redacted]@fincen.gov; [redacted]@atg.in.gov; Josephs, Mark (CIV)
Subject: FW: RSVP: Consumer Protection Working Group Meeting---June 1, 2012

Working Group Members –

Attached is the updated draft agenda for tomorrow's CPWG meeting. We recommend arriving at the FTC between 10 and 15 minutes early to allow time for security and to ensure we start on time.

See you all then!

From: Soneji, Sabita J. (CIV)
Sent: Wednesday, May 23, 2012 11:50 AM
To: Alessandrino, Matthew; Arterberry, John (CRM); Benardo, Michael; Birotte Jr., Andre (USACAC); Blume, Michael S.; Braunstein, Sandra; Breuer, Lanny A. (CRM); Buretta, John (CRM); Bylsma, Michael; Chua, Michelle; Colucci, Nicholas; Davidovich, John; Delery, Stuart F. (CIV); Dukes, Susan; Dunleavy, Hugh; Evans, Carol; Fishman, Paul (USANJ); Freis, James; Frimpong, Maame Ewusi-Mensah (CIV); Gallagher, Timothy A. (FBI); Garcia, Sandra; Goldberg, Richard; Graber, Geoffrey (CIV); Greisman, Lois; Hagan, Deborah; Halperin, Eric (CRT); Hamel, William; Harwood, Charles; Knox, Jeffrey (CRM); Kreisher, Todd; Leon, Glenn (CRM); Markus, Kent; Martinez, Brian (OAAG) (JMD); McGovern, Kathleen (CRM); McInerney, Denis (CRM); McPherson, James; Merritt, Cynthia; Miller, Steven; Morris, Lucy; Patterson, Jodi; Perez, Thomas E (CRT); Raman, Mythili (CRM); Raper, Troy; Rasnak, Sandra (USTP); Riordan, Bruce (USACAC); Rosen, Paul (CRM); Rusch, Jonathan (CRM); Schultz, Vicki (CRT); Senturia, Harris; Sherrill, Gary; Smith, Tyler; Stegman, Matthew (OAAG) (JMD); Stipano, Dan; Suleiman, Daniel (CRM); Sweet, Joel (USAPAE); Tighe, Kathleen; Vanderburg, Pamela J. (FBI); Vladeck, David; West, Tony (OAAG) (JMD); Whalen, Kevin; White, Clifford (USTP); Wiggins, Hunter; [redacted]@frb.gov; [redacted]@ftc.gov; Lennon, Kenneth; [redacted]@usss.dhs.gov
Cc: Bresnick, Michael J (ODAG) (JMD)
Subject: RSVP: Consumer Protection Working Group Meeting---June 1, 2012

Just a reminder to **RSVP** for our upcoming CPWG meeting next Friday, June 1, from 1:00-3:30pm. Thanks to the many of you who have already done so.

We will be meeting in the FTC Commissioners Conference Room in the FTC Building (**600 Pennsylvania Avenue NW**). Visitors should enter the building on the Pennsylvania Avenue side of the building at the 6th Street end.

Attached is a draft agenda for the meeting.

See you then.

Sabita Soneji

Counsel

Office of the Assistant Attorney General, Civil Division

United States Department of Justice

202.307.1697

FFETF Consumer Protection Working Group
June 1, 2012 Meeting
Agenda

1:00-1:05pm: Welcome and Introductory Remarks

1:05-1:50pm: Short Term Priorities and Deliverables Discussion

- Third-Party Payment Processors
- Payday Lending
- Fraud on Servicemembers

1:50-2:10pm: Outreach Initiatives

- Co-Chair Andre Birotte to discuss recent consumer protection summit in Los Angeles
- FTC to discuss upcoming Common Ground Conference in Chicago

2:10-2:20pm: Open Discussion/Next Steps

Meeting with Consumer Advocates

2:30-3:00pm: Consumer Advocate Presentation: Payday Lending

3:00-3:30pm: Appropriate Matters for Referral to Federal Law Enforcement

- DOJ, FTC, and others will discuss factors that might indicate a good matter for referral to law enforcement.

FFETF Consumer Protection Working Group
June 1, 2012 Meeting
Draft Agenda

1:00-1:05pm: Welcome and Introductory Remarks

1:05-1:50pm: Short Term Priorities and Deliverables Discussion

- Third-Party Payment Processors
- Payday Lending
- Fraud on Servicemembers

1:50-2:10pm: Outreach Initiatives

- Co-Chair Andre Birotte to discuss recent consumer protection summit in Los Angeles
- FTC to discuss upcoming Common Ground Conference in Chicago
- USTP to discuss upcoming consumer protection event in Chicago

2:10-2:20pm: Open Discussion/Next Steps

Meeting with Consumer Advocates

2:30-3:00pm: Consumer Advocate Presentation: Payday Lending

3:00-3:30pm: Appropriate Matters for Referral to Federal Law Enforcement

- DOJ, FTC, and others will discuss factors that might indicate a good matter for referral to law enforcement.

To: Bresnick, Michael J (ODAG)[redacted]@usdoj.gov]
From: Goldberg, Richard (CIV)
Sent: Mon 11/5/2012 6:41:15 PM
Subject: Presentation.docx
Presentation.docx

Mike – Here it is. Enjoy London.

Rich

Good afternoon. I'm Rich Goldberg, assistant director of the Department of Justice, Consumer Protection Branch. The Consumer Protection Branch handles various criminal and civil cases in an effort to protect individuals from fraudulent and deceptive business practices.

At this point, we're going to take a step back to a broader level to make sure everyone is up to speed on exactly what we're talking about here.

Third party payment processors are being used to facilitate various sorts of offenses. I'm going to talk about frauds being committed using third party payment processors. Other sections of the Department of Justice are paying attention to other sorts of offenses, such as internet gambling, being facilitated using processors. But today, I'll be focusing on frauds, and a specific type of frauds – consumer frauds.

Let's look at why the Department of Justice and other agencies are looking at payment processors in the context of consumer frauds.

SLIDE 6

Why the interest in payment processors?

Federal, state, and local governments have finite resources. But, fraudulent

actors are blessed, or cursed, with unlimited ingenuity and manpower. We do our best to keep up, but there is no way we can take down every fraudulent firm out there. There are many firms out there in the U.S. that are devoting substantial energies to defrauding U.S. citizens. Debt relief firms, loan modification companies, bogus sweepstakes companies, these are just some of the many companies trying to take advantage of our consumers. Frequently, it's the consumers in the most desperate financial straits that pay money to these firms in hope of a brighter future. In a few minutes, Monica Vaca of the FTC will talk a little bit more about some of these schemes.

Sometimes, the firms tell outright lies to consumers about the goods or services they supply.

Sometimes, the firms don't supply the product or service they promise at all.

Sometimes, they have had no contact with the victim at all; they simply debit the consumers' bank account while claiming to have authorization to do so.

We will always attack the fraudulent actors themselves, but we are also paying attention to those firms and individuals who are facilitating the fraud.

There may be a facilitator who is helping many fraudulent firms. If we can take out that one facilitator, then we have a larger overall impact on half a dozen fraudulent merchants.

At times, third party payment processors stand in the role of a fraud facilitator. And they may be helping a number of fraudulent merchants to do business at the same time. So, targeting a processor who knows of the fraud, or is turning a blind eye to the fraud, may be a more effective use of our resources.

SLIDE 7

Let's diagram how this payment processor relationship works. This is, of course, an oversimplification. But, again, I want to make sure everyone understands what we're talking about here.

We'll begin at the upper right corner of this diagram. Fraudulent actors, here labeled "offenders," market to consumers. As I said before, at times, there is no marketing and the consumer does not even know that their accounts are being debited. But, for simplicity sake, let's say that in this case, the firm is soliciting the consumer to purchase a good or service.

The solicitation is directed to the consumer. When a third party payment

processor is used, the consumers' money is transmitted from the consumer's bank account, to a payment processor bank account. The money is then sent from the payment processor's bank account to the offender or fraudster's bank account, and from there on to the offender. Of course, this same transaction may be used for legitimate actors when dealing with a payment processor. But, this is also how it often happens with a fraudulent actor.

What are the mechanisms used for this money to be transmitted.

SLIDE 8.

It may be automated clearing house, or ACH transactions.

It may be what is know as Remotely Created Checks or Remotely Created Payment orders.

These payment mechanisms are created by entering a consumer's name and bank account information into an electronic form and are processed like an ordinary paper check. When printed, remotely created payment orders look like regular bank checks, but instead of having the account holder's signature, they bear a statement such as "Authorized by Account Holder" or "Signature on File." These payment mechanisms are prone to abuse and have become a particularly

attractive payment method for merchants and processors engaged in fraud and unauthorized debiting.

Why are these payment forms more prone to abuse than traditional payment forms like checks and wire transfers?

Of course, there are the completely unauthorized charges that some fraudsters are taking out of consumer bank accounts using these payment methods. But, even putting those aside, offenders like these payment types for other reasons as well.

-Offenders committing consumer frauds have realized that they can take money from a whole lot more people at a time using ACH and remotely created checks.

-It takes less effort on the part of the fraudster, especially when it's happening through a processor.

-ACH payments and remotely created checks are quick and give the consumer less time to think about their payment than traditional checks or wire transfers. When writing a paper check or wiring money, it's a much more deliberate act for the consumers. Consumers have more time to consider the

decision, to research the merchant online, and take other types of due diligence steps to ensure that a) the person at the other end of the phone is who they say they are and, b) they will deliver what they say they're going to deliver.

These are just some of the reasons why fraudsters like to use these payment methods up on the board.

So, back to our chart. The account held by the Payment processor is used to process consumer payments and send them on to the offender's bank account.

SLIDE 9

This is the account where you come in.

If your financial institution is the one that holds this account -- the payment processor account, then you are in a position to see what is happening in this account.

Typically, all of the adjustments, credits, chargebacks, and other actions are taken and applied out of the payment processor account, rather than the offender's bank account. It is this account in the middle here – the payment processor account, that is the most telling.

If the payment processor is dirty, or is turning a blind eye to the fraud that is being committed, then you and your financial institution are the only ones who stand between the public's money and the fraudster's bank account.

Sometimes, these payment processor bank accounts are held in large banks and credit unions. Sometimes, they're small banks and credit unions. We in law enforcement have seen them in both places. They've ALL been used to facilitate consumer fraud through tppps.

You need to be able to see all transactions, broken down by merchant, not just broken down by processor. If you can't, a bad merchant may be hidden in the transactions of many merchants.

So, when you're reviewing the bank accounts, you have got to be able to see credits, debits, chargebacks, and other account activity broken down by merchant, not by the payment processor as a whole.

When you are reviewing transactions dealing with ACH, and remotely created checks and payment orders, ask what proof there is that the consumer authorized the transaction. And push. Don't give up when you get a seemingly stock answer of "it's there."

But, it's not only transactions with literally no authorization that may be problematic. Are you getting consumer complaints? How is the product being marketed online?

Even when there are authorizations for a debit, they may be authorizations for a single transaction, not for the recurring payments that the processor is taking out of their accounts.

And even when fully authorized, the authorization may have come based on fraudulent statements about what was being offered or provided.

Watch for all of the red flags discussed in the FINCEN advisory, and that the other webinar participants will be discussing after me.

There is more you need to look out for as well.

SLIDE 10

This what one payment processor relationship looks like.

SLIDE 11

This is what another payment processor relationship looks like. In other words,

there are occasions in which multiple processors are being used to process payments for a merchant. A consumer's money may go from one payment processor account, to another payment processor account.

SLIDE 12

And it can get even more complicated. There may be several payment processors nesting together. Why is this done? It may be done in order to hide the chargebacks of one merchant in the transactions of others.

This is why I say, and others may reiterate, that if you don't see the transactions broken down by merchant, you may not be seeing the whole picture of that merchant.

That's why we're all hear. To talk about what's going on. What may be going on in your financial institution as we speak.

We're looking at the payment processors. Some of us will be looking to make sure that financial institutions are not turning a blind eye to consumer fraud.

As many of you know, pressure is also coming from the class action plaintiff's bar. It is likely that, when a fraudster hits the road and a processor closes down, the financial institution closest to the processor will be the one that class actions look

to to collect. If you haven't seen it, take a look at the case of Reyes v. Zion First National Bank from the Eastern District of Pennsylvania. It will show you that regulators are not the only ones watching what is going on. Class action lawyers are as well.

Look, you and your colleagues did not go into the banking industry to help a bunch of skumbag fraudsters to leach off the American public. You're there to do banking for legitimate customers. In the process, you can do a valuable public service and, at the same time, fulfill a legal obligation. Notify us of suspicious activity and be proud that you have helped weed out consumer fraud against your friends and neighbors, maybe your family. We hope that you will work with us. The FINCEN advisory discusses exactly how you can do that.

I want to thank FINCEN very much for providing this venue to speak with all the attendees out there, and I want to thank all of the financial institutions out there for your time and attention.

To: Bresnick, Michael J (ODAG)[[redacted]@usdoj.gov]; Sweet, Joel (USAPAE)[/O=GSD/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Joel.Sweet-USA]; Blume, Michael S.[miblume@CIV.USDOJ.GOV]
From: Goldberg, Richard
Sent: Sat 11/17/2012 2:39:24 PM
Subject: RE: NAC Fraud Survey

To me, the most important thing is to find AUSAs with an interest in the subject. I don't think it's necessary to announce the "initiative," especially since AUSAs tend to be wary of initiatives, especially deriving from Main. Consider getting 15 minutes on the agenda to briefly describe the problem of TPPP and banks that help. Maybe ask for a show of hands how many AUSAs have done cases in which a TPPP was used. Ask how many have investigated the TPPP and bank that was used. And urge folks to do so in the future.

Of course a full lecture on the subject would be great, but even 15 minutes would be a good start at flagging the issue, gauging interest from the field, and letting folks know that there is a source of expertise when they need it.

-----Original Message-----
From: Bresnick, Michael J (ODAG) (JMD)
Sent: Saturday, November 17, 2012 8:16 AM
To: Sweet, Joel (USAPAE); Blume, Michael S.; Goldberg, Richard
Subject: Re: NAC Fraud Survey

I think it's ok to describe the increased focus on this area, but I'm not sure we should announce specific strategy. Let me think about it some more.

----- Original Message -----
From: Sweet, Joel (USAPAE)
Sent: Saturday, November 17, 2012 07:56 AM
To: Bresnick, Michael J (ODAG); Blume, Michael S. (CIV); Goldberg, Richard (CIV)
Subject: Re: NAC Fraud Survey

In fact, it doesn't matter if I am out of the closet by Dec 4. We can still announce/describe the initiative at the conference, no?

Joel M. Sweet
T: [redacted]
C: [redacted]

----- Original Message -----
From: Sweet, Joel (USAPAE)
Sent: Saturday, November 17, 2012 06:51 AM
To: Bresnick, Michael J (ODAG) (JMD); Blume, Michael S. (CIV); Goldberg, Richard (CIV)
Subject: NAC Fraud Survey

Guys- week of dec 4 is the Fraud Survey course at the nac. I will attend as a participant. If Operation Choke Point is public by then, perhaps we can get an opening on the program to announce, describe, enlist

interested ausas, etc. According to the registration material, it will be a full house.

Joel M. Sweet
T: [redacted]
C: [redacted]

To: Goldberg, Richard[[redacted]@CIV.USDOJ.GOV]; Bresnick, Michael J (ODAG)[[redacted]@usdoj.gov]; Blume, Michael S.[[redacted]@CIV.USDOJ.GOV]
From: Sweet, Joel (USAPAE)
Sent: Sun 11/18/2012 11:34:45 PM
Subject: RE: NAC Fraud Survey

Rich -- I agree with you on objectives. I'll try to find out who the course planner is and if I can get on the agenda. At the least, I can try to steal 10 minutes of Harris Senturia's time. JMS

-----Original Message-----
From: Goldberg, Richard [mailto:[redacted]@usdoj.gov]
Sent: Saturday, November 17, 2012 9:39 AM
To: Bresnick, Michael J (ODAG) (JMD); Sweet, Joel (USAPAE); Blume, Michael S. (CIV)
Subject: RE: NAC Fraud Survey

To me, the most important thing is to find AUSAs with an interest in the subject. I don't think it's necessary to announce the "initiative,"
especially since AUSAs tend to be wary of initiatives, especially
deriving from Main. Consider getting 15 minutes on the agenda to
briefly describe the problem of TPPP and banks that help. Maybe ask for a show of hands how many AUSAs have done cases in which a TPPP was used.
Ask how many have investigated the TPPP and bank that was used. And urge folks to do so in the future.

Of course a full lecture on the subject would be great, but even 15 minutes would be a good start at flagging the issue, gauging interest from the field, and letting folks know that there is a source of expertise when they need it.

-----Original Message-----
From: Bresnick, Michael J (ODAG) (JMD)
Sent: Saturday, November 17, 2012 8:16 AM
To: Sweet, Joel (USAPAE); Blume, Michael S.; Goldberg, Richard
Subject: Re: NAC Fraud Survey

I think it's ok to describe the increased focus on this area, but I'm not sure we should announce specific strategy. Let me think about it some more.

----- Original Message -----
From: Sweet, Joel (USAPAE)
Sent: Saturday, November 17, 2012 07:56 AM
To: Bresnick, Michael J (ODAG); Blume, Michael S. (CIV); Goldberg, Richard (CIV)
Subject: Re: NAC Fraud Survey

In fact, it doesn't matter if I am out of the closet by Dec 4. We can still announce/describe the initiative at the conference, no?

Joel M. Sweet
T:[redacted]
C:[redacted]

----- Original Message -----
From: Sweet, Joel (USAPAE)
Sent: Saturday, November 17, 2012 06:51 AM
To: Bresnick, Michael J (ODAG) (JMD); Blume, Michael S. (CIV); Goldberg, Richard (CIV)
Subject: NAC Fraud Survey

Guys- week of dec 4 is the Fraud Survey course at the nac. I will attend as a participant. If Operation Choke Point is public by then, perhaps we can get an opening on the program to announce, describe, enlist interested ausas, etc. According to the registration material, it will be a full house.

Joel M. Sweet
T:
C: [redacted]

To: Bresnick, Michael J (ODAG)[redacted]@usdoj.gov]
From: Michael Bresnick
Sent: Thur 12/6/2012 12:10:05 PM
Subject: remarks
Remarks to CSBS--Dec. 2012.docx
ATT00001.txt

Good afternoon, and thank you all for having me here today. It is a privilege to be able to address this distinguished group directly, particularly since you are on the front lines in the states on so many issues that I deal with every day at the U.S. Department of Justice.

As you heard, I am the Executive Director of President Obama's Financial Fraud Enforcement Task Force, which is chaired by the United States Attorney General, and counts as its members the highest leaders throughout the Department of Justice, including the FBI, and more than 25 other federal law enforcement offices and regulatory agencies (such as the OCC, FDIC, Federal Reserve, and CFPB), state attorneys general, inspectors general, Tribal leaders, and more. In short, when President Obama created the Task Force in November 2009, he formed the largest federal, state, and local coalition ever assembled to investigate and prosecute financial fraud. Now, while the Task Force's goals may seem ambitious at first glance, its foundation is really quite simple: Those charged with protecting the public in all levels of government cannot work in isolated and compartmentalized silos; instead, if the government is unified in its approach and execution it can achieve more by working together than it ever could achieve by working separately. So, as Executive Director, and working with leaders throughout government agencies, I have identified priorities for the various Task Force's working groups and committees and fraud trends occurring throughout the country, developed national fraud enforcement strategies, created and coordinated national initiatives, and established training events and guidance for our nation's prosecutors and civil attorneys.

Currently, the Task Force has eight different working groups, each one focused on a particular type of financial fraud. They include: (1) Mortgage Fraud, (2) Securities and Commodities Fraud, (3) Rescue Fraud (focused on the TARP program), (4) Oil and Gas Price Fraud, (5) Recovery Act, Grant, and Procurement Fraud, (6) Fair Lending, and, most recently (6) RMBS fraud, and (7) Consumer Protection. While our efforts focused on RMBS fraud – which the President announced during his State of the Union speech in January -- has received the most public attention, it's actually the last working group I mentioned -- that focused on consumer protection -- that I'd like to focus on initially.

The Consumer Protection Working Group of the Task Force, which I created soon after taking over this position, is led by David Vladeck, the Director of the Bureau of Consumer Protection for the FTC, Stuart Delery and Lanny Breuer, the heads of the Department's Civil and Criminal Divisions, Kent Markus, the Director of Enforcement for the CFPB, and Andre Birotte, the U.S. Attorney in Los Angeles. Other members of the Group include FinCEN, the OCC, FDIC, NCUA, IRS-CI, Postal Inspection Service, and others. Together, we have made investigating mass-marketing fraud schemes a priority, and especially the use of businesses that process payments for their fraudulent merchant clients, thereby facilitating the scheme and providing the fraudsters access to the U.S. banking system.

Recently there has been increased focus and attention by federal regulators, as well as the Department of Justice, in holding financial institutions, including Money Services Businesses, accountable to their BSA obligations and making sure they have robust and vibrant Anti-Money Laundering policies and procedures in place. Of course, these policies and procedures must include, at a minimum:

--internal policies, procedures, and controls designed to guard against money laundering;
--an individual to coordinate and monitor day to day compliance with the BSA and AML requirements;
--ongoing employee training; and
--independent testing for compliance conducted by bank personnel or an outside party.

Given the complexities of some relationships between financial institutions and their account holders, however, a number of financial institutions have run into trouble of late.

In particular, financial institutions maintaining client accounts for **third-party payment processors** have found themselves "underneath the v," so-to-speak, in a number of actions brought by government agencies. Third-party payment processors are non-bank processors that process payments for their merchant clients, many of which are online companies offering **consumer-based services**, such as payday loans, debt relief, and government grants, among other things. Unfortunately, many of these services are simply scams that use the payment processors to gain access to the U.S. financial system, victimize consumers, and launder their illegal proceeds. Senior citizens are the most common victims of mass market fraud schemes. According to the AARP, the National Association of Attorneys General, and the Federal Trade Commission, the majority of fraudulent telemarketing victims are age sixty-five or older. Accordingly, these scams, and the processors and financial institutions that facilitate them, have been the subject of increased focus throughout the federal government, and, specifically, the Consumer Protection Working Group of the Financial Fraud Enforcement Task Force.

For those of you who may not know, here is how the scam operates: Mass market consumer fraud generally involves a scheme that uses deceptive and misleading offers for products and services to induce unsuspecting consumers to provide personal payment information, such as a credit card number or a bank account number. Once in possession of consumers' personal payment information, the fraudulent merchant must access the banking system to gain access to the consumer's money. Fraudulent merchants, however, cannot directly access the national banking payment system. To take consumers' money, a fraudulent merchant must establish a relationship with a bank. The bank must agree to originate debit transactions through the national banking system by which money will be withdrawn from consumers' bank accounts and transferred to the fraudulent merchant's bank account. In order to gain access to the national banking system and consumers' accounts, fraudulent merchants often engage third-party payment processors to establish a relationship with a bank. A third-party payment processor, therefore, serves as an intermediary between the fraudulent merchant and the bank. Through this relationship, a bank can profit from the fees it receives from the third-party payment processor and the fraudulent merchant, while avoiding a direct relationship with the fraudulent merchant and the scrutiny that such a relationship would draw to the bank.

When a third-party payment processor is used, the consumers' money is transmitted from the consumer's bank account to a payment processor's bank account. The money is then sent from the payment processor's bank account to the fraudster's bank account, and from there on to the offender. Of course, this same transaction may be used for legitimate actors when dealing with a payment processor. But, this is also how it often happens with a fraudulent actor.

What are the mechanisms used for this money to be transmitted? It may be automated clearing house, or ACH transactions. It may also be what is known as **Remotely Created Checks** or Remotely Created Payment orders. These payment mechanisms are created by entering a consumer's name and bank account information into an electronic form and are processed like an ordinary paper check. When printed, remotely created payment orders **look like regular bank checks**, but instead of having the account holder's signature, they bear a statement such as "Authorized by Account Holder" or "Signature on File." These payment mechanisms, however, are prone to abuse and have become a particularly attractive payment method for merchants and processors engaged in fraud and unauthorized debiting. In fact, they are not regulated like ACH transactions (which are monitored by NACHA). In fact, in a 2005 letter to the Board of Governors of the Federal Reserve System, the Attorneys General of 35 states jointly urged that RCCs be eliminated from the banking system altogether. The Attorneys General explained that RCCs are "used to perpetrate fraud on consumers" by causing the withdrawal of money from consumers' bank accounts without authorization.

Now, it is also unfortunate, but true, that we have seen a number of financial institutions that have knowingly assisted, or willfully turned a blind eye to, fraudulent payment processors and their involvement in mass marketing fraud scams. Of course, proof of such knowledge or willful blindness can be tricky, but there are certain indicators of fraud –and knowing participation in the fraud—that we have identified. For instance, a return or chargeback reflects a transaction that was rejected by the consumer or the consumer's bank and was thus not successful in taking funds from the account of the consumer. A return "rate" refers to number of returned items compared to the number of originated transactions during a particular time period. High return rates are not absolute proof of fraud; rather, they are a red flag that a merchant's practices may be deceptive or otherwise dishonest. High return rates trigger a duty by the bank and the third-party payment processor to inquire into the reasons for the high rate of returns, and specifically whether the merchant is engaged in fraud.

We have actually seen instances where the **return rates** on processors' accounts (particularly where the processors have used RCCs) have exceeded 30%, 40%, 50%, and, even **85%.** Just to put this in perspective, the industry **average return rate for ACH transactions is 1.5%,** and the industry average for **all bank checks processed through the check clearing system is less than .5%.** This is more than a red flag—that, to me, is an ambulance siren, screaming out for attention.

So, where are we finding these troubling accounts? Sometimes, in large banks and credit unions. Sometimes, they're in small banks and credit unions. **(Third-party payment processors often promise large deposits and smaller banks may like the idea of additional fees**, including return fees). We in law enforcement have seen them in both places.

Given all these problems, the Consumer Protection Working Group recently worked with FinCEN to issue a new **financial advisory** for the more than 20,000 financial institutions it regulates regarding the red flags associated with third-party payment processor accounts. And after the advisory, **I subsequently moderated a panel –on a webinar, in fact, graciously hosted by FinCEN -- with leaders from FTC, CFPB, FDIC, OCC, FBI, and DOJ for more than 700 financial institutions.**

The message to financial institutions was this: Knowing Your Customer is not enough. They need to endeavor to Know Your Customer's Customer. Who is the merchant that the processor is processing payments for? What is the nature of its business? Who owns and operates it? Where is it located? What product are they selling? Do they have a sales script? What do their advertisements say? What's their history of chargebacks? Do they maintain a database of customer complaints? Are there other complaints out there that they should know about, such as prior FTC actions, Better Business Bureau complaints, and so on. And, once they accept a processor as a client, financial institutions need to be able to **see all transactions**, **broken down by merchant**, not just broken down by processor. If they can't, a bad merchant may be hidden in the transactions of many merchants. Also, if a payment processor maintains accounts at several banks, or switches accounts from one bank to another quickly, ask why—that processor may be trying to lower the total return rates to avoid detection.

As I mentioned earlier, for the past several years there has been an increase in criminal and civil enforcement and regulatory actions against businesses that process payments on behalf of their client-merchants, as well as against the financial institutions doing business with them. For example, in **United States v. Wachovia Bank, N.A.**, No. 10-20165-CR, SDFL, the United States, working in conjunction with FinCEN and the Office of the Comptroller of the Currency ("OCC"), entered into a deferred prosecution agreement with the bank. This agreement resulted in part from the bank's failure to maintain robust Anti-Money Laundering policies and procedures that would have guarded against the dangers posed by certain third-party payment processors that maintained accounts at the bank in order to process payments for their telemarketing merchant clients.

Wachovia agreed to forfeit $110,000,000 to resolve the charges.

In 2011 the United States Attorney's Office for the Eastern District of Pennsylvania announced the indictment of six individuals who owned and operated Payment Processing Center, Inc., a company that processed payments to individuals in the United States on behalf of internet gambling businesses located outside the United States. The indictment made clear that one of the objects of the conspiracy was to "launder funds internationally to promote illegal gambling . . . ." And just a couple of weeks ago, the same U.S. Attorney's Office, in conjunction with FDIC and FinCEN, obtained a $15 million civil money penalty under the Financial Institutions Reform, Recovery, and Enforcement Act against the First Bank of Delaware for engaging in a scheme to defraud, resulting from its origination of more than $138 million in transactions on behalf of fraudulent merchants and third-party payment processors.

The Federal Trade Commission also has filed several civil complaints against third-party payment processors -- including Landmark Clearing, Inc. (which, incidentally, marketed its willingness to process payments using RCCs (which are unregulated), rather than the regulated ACH transactions, to potential clients), and Your Money Access, LLC, among others, demonstrating in detail the risks these processors pose to consumers as well as the U.S. banking system.

Other banking regulators such as the FDIC and the OCC also have filed enforcement actions

against financial institutions for failing to maintain proper AML policies and procedures safeguarding against the money laundering risks posed by businesses that process payments for creditors or sellers. For example, the FDIC filed consent orders against the First Bank of Delaware and SunFirst Bank. Similarly, the OCC filed an enforcement action against T Bank, N.A., in addition to Wachovia, discussed above.

These actions led both the FDIC and the OCC to issue guidance to the financial institutions they supervise about the money laundering and other risks associated with payment processor relationships, as well as the Federal Financial Institutions Examination Council Exam Manual (April 29, 2010). The overwhelming conclusion expressed by these regulators is that businesses that process payments on behalf of other businesses acting as creditors or sellers can pose significant money laundering risks. The criminal indictments, civil enforcement actions, regulatory supervision, and guidance offered by every federal office and agency to have addressed this issue are unanimous in this regard.

Yet, despite this consensus, currently third-party payment processors are not defined as money transmitters under many states' money transmitter laws, allowing many of them to fly under the radar, avoid attention and detection by law enforcement, and make it more difficult for financial institutions to recognize them as facilitators of fraud. Since it is plain that these processors do, indeed, pose significant money laundering risks, I ask you to take a look at your particular state's money transmitter laws to see if it covers third-party payment processors. If it simply mirrors FinCEN's MSB rule, then it may not, since payment processors currently are excluded from there as well. If your law does not cover them, please consider whether it might be wise to seek a change to the law.

As we have seen, despite the banks' own BSA/AML obligations and despite the abundance of guidance on this issue from various regulators, unscrupulous and clever payment processors have made it extremely difficult for even the most vigilant of banks to identify and eliminate the risky behavior. For example, certain processors have undertaken a variety of measures for the sole purpose of deceiving the banks at which they maintain accounts. This deceptive conduct includes (1) opening accounts at several different banks in order to reduce the total return rate at any single bank, (2) quickly switching banks at which they maintain accounts so the return rate never gets too high, (3) processing payments for another payment processor (a so-called "nesting" arrangement that, according to the FDIC Guidance FIL-3-2012, poses "additional challenges as they may be extremely difficult to monitor and control"), and (4) using so-called "returned check-consolidation accounts," separate deposit accounts either at the same or separate banks that make it difficult for financial institutions to identify and evaluate return rates and which "severely inhibits a financial institution's ability to monitor and report suspicious activity," as recognized in the recent FinCEN advisory.

Yet, if a bank knew at the outset that a processor were required to register with a particular state but had not done so, the bank would be less likely to do business with that processor in the first instance.

In addition, requiring payment processors to register as a money transmitter with a state has significant law enforcement implications, since 18 U.S.C. § 1960 makes it a crime punishable by

up to 5 years in prison for a money transmitting business to operate in a state requiring a money transmitter license without such a license. If more states were to require payment processors to register as money transmitters, prosecutors would have a powerful weapon with which to pursue unlawful payment processors under § 1960 and, we expect, severely curtail the risky and unlawful conduct described above.

As I said at the outset, the Consumer Protection Working Group of the Task Force is dedicating a significant amount of attention to this issue, and we are approaching it in a smart, systematic, and coordinated way. The principle behind this new enforcement initiative is this: If we can eliminate the mass-marketing fraudsters' access to the U.S. financial system—that is, if we can stop them from getting paid—then we can significantly reduce the harm caused by this type of fraud. Third-party payment processors are what we call the bottleneck in this problem. Most mass-marketing fraudsters need them in order for their scams to work. We hope to close that access to the banking system—effectively putting a chokehold on it—and put a stop to this billion dollar problem that has harmed so many American consumers.

Before I go, I also want to make sure I tell you about another issue that I thought would be of particular interest to this group, and that we're increasingly focused on, and that is payday lending. I know this is something the states have grappled with for years. And recently, of particular concern, has been fraudulent payday lenders' efforts to avoid state regulation by affiliating themselves with Indian Tribes. This, of course, is a sensitive issue—one involving Tribes' Sovereign Immunity—but we are looking into it to see if there is something that can be done. In addition, the Department of Justice's Civil Rights Division, as part of the Non-Discrimination Working Group of the Task Force, has made payday lending a priority and is considering the fair lending implications associated with these lenders.

The Task Force also continues to be steadfastly focused on all aspects of housing issues—whether is be RMBS fraud, fair lending, foreclosure public auction bid rigging, systemic mortgage loan origination abuses, or more traditional mortgage fraud cases, such as foreclosure rescue or loan modification schemes.

In short, there is plenty of work to do, but, as I said at the beginning, we all share a unity of purpose, and if we are unified in our approach and execution, we can accomplish great things together. I look forward to working with you in the future, and thank you, again, for the opportunity to speak to you today.

To: Blume, Michael S.[redacted]@CIV.USDOJ.GOV]; Bresnick, Michael J (ODAG)[redacted]@usdoj.gov]; Benardo, Michael B.[redacted]@FDIC.gov]; Sweet, Joel (USAPAE)[/O=GSD/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Joel.Sweet-USA]
From: Goldberg, Richard
Sent: Thur 12/13/2012 6:01:14 PM
Subject: RE: cybersecurity

I agree with Mike. I think unauthorized charges by a firm made to appear as legitimate charges for a product or service they purport to provide are within our scope; e.g., when done through RCC. But outright theft via hacking is a cybersecurity issue beyond our reach.

From: Blume, Michael S.
Sent: Thursday, December 13, 2012 12:55 PM
To: Bresnick, Michael J (ODAG) (JMD); Benardo, Michael B.; Sweet, Joel (USAPAE); Goldberg, Richard
Subject: RE: cybersecurity

My two cents – this is beyond the scope and capabilities of that group. I think this is for a different set of folks with different expertise.

From: Bresnick, Michael J (ODAG) (JMD)
Sent: Thursday, December 13, 2012 11:49 AM
To: Benardo, Michael B.; Sweet, Joel (USAPAE); Blume, Michael S.; Goldberg, Richard
Subject: cybersecurity

Is this something that the Consumer Protection WG can work on?

http://www.washingtonpost.com/business/technology/cybersecurity-firm-identifies-credible-threat-to-30-us-banks/2012/12/12/b0ec226a-3e3b-11e2-ae43-cf491b837f7b_story.html

To: Bresnick, Michael J (ODAG)[redacted]@usdoj.gov]
From: Michael Bresnick
Sent: Tue 2/12/2013 6:20:18 PM
Subject: updated notes
Notes for American University Lecture 2-13-13.docx

Michael Bresnick
[redacted]

Introduction

--great to be here
--when Lee and Jerry asked me to lecture here I was very excited about the opportunity
--For me law school was a great time to learn the law, but also to think about the different paths I could take. So I'm really glad I can be here with you today to talk about what I've done, and where the law might take you.
--There will be time at the end for questions, but if I say something that you want to talk about please don't hesitate to ask me.
--I'd like this to be a discussion, not a speech.

--So I'd like to start by introducing myself and talking about my career, and, more specifically, about what I'm doing now, and then we'll talk about some things DOJ and other government agencies are doing with consumer fraud that we hope will make a difference.

--I graduated from UMaine Law School in 1996
--clerked for a couple of federal judges (and, if you're at all considering this path, I highly encourage it-great experience to see how judges react to various arguments, how trials are conducted, and how to hone your research and writing skills)
--after that I went to work at a law firm in NY for 5 years—also a great experience (learned how big firms operate and how they think and react; worked a lot in criminal defense, particularly securities fraud matters), but soon felt the call of public service and went to USAO in EDPA
--As an AUSA I tried 16 cases—all different kinds—and investigated every type of crime—violent, RICO, financial fraud, heath care, tax, mortgage, public corruption
--after 7 years I went to the CRM Division of USDOJ, supervising FF cases
--and soon after that I was asked by the DAG to start in my current position, Exec. Dir of FFETF

--TF created in Nov. 2009 by executive order of the president, chaired by AG, and consists of leading officials throughout DOJ and other government agencies
--8 different WGs
--Soon after I started, I consulted with the AG to start a Consumer Protection WG, since it was an area that had not previously been addressed but was extremely important

How Identify Priorities

--For each of these WGs, I work with the leaders of the respective groups to identify fraud trends and priorities, create national initiatives, and training events for the nation's prosecutors and civil attorneys.
--In terms of identifying priorities, there are several ways we do this
--Identify problems by discussing issues openly with TF members, sharing information, and agreeing on a coordinated course of action best designed to fix the problem (purpose of the task force is to bring together all the different stakeholders to share ideas and work together; unity of purpose; accomplish more by working together than by working in compartmentalized silos)
--Or, a problem is brought to my attention by an outside group—maybe a consumer

advocacy group –that I hadn't been aware of (a good reason why we actively and regularly speak with organizations, and, even, private industry, outside government—outreach is a critical piece of what we do)
--Or, as simple as my thinking about a particular issue (maybe something raised in a private lawsuit, or an article, or an IG report) and coming up with a variety of ideas and bouncing them off others for their input
--As you can imagine, in the area of consumer fraud, there's no shortage of opinions.

So, What are the Priorities of the Consumer Protection Working Group
--Third-party payment processors and financial institutions doing business with them, as well as other types of payment fraud involving mobile payments, prepaid access devices, and other emerging payment mechanisms
--fraud on servicemembers (working with many state AGs, USAOs, and JAG officers)
--and payday lending (short-term, low dollar, high interest rate), including their recent strategy of seeking out Tribal Nations to get incorporated by them in order to avoid state usury laws (work with Tribal leaders, state financial regulators, consumer advocacy groups, and federal and state government officials)
--I'm here today primarily to talk about TPPPs and the FIs who do business with them, and their role in the business of mass marketing fraud, which accounts of billions of dollars of losses to consumers

Third Party Payment Processors
--Before I even started the group last year, I had been looking at this industry called third-party payment processors and the financial institutions that do business with them
--The reason that we've identified them is based on their position as so-called bottlenecks, or choke-points, in the fraud committed by so many merchants (such as internet payday lenders, providers of government grants, lottery schemes, grandparent schemes, credit repair services, internet gambling, and so on, that victimize consumers and launder their illegal proceeds)
-- Senior citizens are the most common victims of mass market fraud schemes. According to the AARP, the National Association of Attorneys General, and the Federal Trade Commission, the **majority of fraudulent telemarketing victims are age sixty-five or older.**
--TPPPs are, in short, the means by which the bad guy merchants are able to get paid—they provide the fraudsters with access to the national banking system and facilitate the movement of money from the victim of the fraud to the bad guy.
-Of course, we'll continue to investigate and prosecute the originators of the fraudulent schemes, but we realized that if we can also cut off their ability to get paid, then we hope we can have a much greater affect.

--In addition to the TPPPs, we also observed that FIs are also complicit in the scheme—either knowingly or willfully blind to what was happening at their institutions.
-- As a result, several financial institutions maintaining client accounts for **third-party payment processors** have found themselves "underneath the v," so-to-speak, in a number of actions brought by government agencies.
-- Accordingly, these scams, and the processors and financial institutions that facilitate

them, have been the subject of increased focus throughout the federal government, and, specifically, the Consumer Protection Working Group of the Financial Fraud Enforcement Task Force.

Here's How It Works

--For those of you who may not know, here is how the scam operates: Mass market consumer fraud generally involves a scheme that uses deceptive and misleading offers for products and services to induce unsuspecting consumers to provide personal payment information, such as a credit card number or a bank account number. (E.g., Jamaican lottery scam).

--Once in possession of consumers' personal payment information, the fraudulent merchant must access the banking system to gain access to the consumer's money. Fraudulent merchants, however, cannot directly access the national banking payment system.

--To take consumers' money, a fraudulent merchant must establish a relationship with a bank. The bank must agree to originate debit transactions through the national banking system by which money will be withdrawn from consumers' bank accounts and transferred to the fraudulent merchant's bank account.

--In order to gain access to the national banking system and consumers' accounts, fraudulent merchants often engage third-party payment processors to establish a relationship with a bank. A third-party payment processor, therefore, serves as an intermediary between the fraudulent merchant and the bank. Through this relationship, a bank can profit from the fees it receives from the third-party payment processor and the fraudulent merchant, while avoiding a direct relationship with the fraudulent merchant and the scrutiny that such a relationship would draw to the bank.

--When a third-party payment processor is used, the consumers' money is transmitted from the consumer's bank account to a payment processor's bank account. The money is then sent from the payment processor's bank account to the fraudster's bank account, and from there on to the offender. Of course, this same transaction may be used for legitimate actors when dealing with a payment processor. But, this is also how it often happens with a fraudulent actor.

--What are the mechanisms used for this money to be transmitted? It may be automated clearing house, or ACH transactions. It may also be what is known as **Remotely Created Checks** or Remotely Created Payment orders. These payment mechanisms are created by entering a consumer's name and bank account information into an electronic form and are processed like an ordinary paper check. When printed, remotely created payment orders **look like regular bank checks**, but instead of having the account holder's signature, they bear a statement such as "Authorized by Account Holder" or "Signature on File." These payment mechanisms, however, are prone to abuse and have become a particularly attractive payment method for merchants and processors engaged in fraud and unauthorized debiting. In fact, they are not regulated like ACH transactions (which are monitored by NACHA). In fact, in a 2005 letter to the Board of Governors of the Federal Reserve System, the Attorneys General of 35 states jointly urged that RCCs be eliminated from the banking system altogether. The Attorneys General explained that

RCCs are "used to perpetrate fraud on consumers" by causing the withdrawal of money from consumers' bank accounts without authorization.

Red Flags

-- Now, it is also unfortunate, but true, that we have seen a number of financial institutions that have knowingly assisted, or willfully turned a blind eye to, fraudulent payment processors and their involvement in mass marketing fraud scams. Of course, proof of such knowledge or willful blindness can be tricky, but there are certain indicators of fraud –and knowing participation in the fraud—that we have identified.

--For instance, a **return or chargeback** reflects a transaction that was rejected by the consumer or the consumer's bank and was thus not successful in taking funds from the account of the consumer. A return "rate" refers to number of returned items compared to the number of originated transactions during a particular time period. High return rates are not absolute proof of fraud; rather, they are a red flag that a merchant's practices may be deceptive or otherwise dishonest. High return rates trigger a duty by the bank and the third-party payment processor to inquire into the reasons for the high rate of returns, and specifically whether the merchant is engaged in fraud.

--We have actually seen instances where the **return rates** on processors' accounts (particularly where the processors have used RCCs) have exceeded 30%, 40%, 50%, and, even **85%.** Just to put this in perspective, the industry **average return rate for ACH transactions is 1.5%,** and the industry average for **all bank checks processed through the check clearing system is less than .5%.** This is more than a red flag—that, to me, is an ambulance siren, screaming out for attention.

--So, where are we finding these troubling accounts? Sometimes, in large banks and credit unions. Sometimes, they're in small banks and credit unions. **(Third-party payment processors often promise large deposits and smaller banks may like the idea of additional fees**, including return fees). We in law enforcement have seen them in both places.

Life cycle of a case (FBD)

--Here's an example of a bank that got caught up in this problem: The First Bank of Delaware

--We were informed by the FTC that a number of fraudulent telemarketing merchants were processing their payments through the First Bank of Delaware

--Rather than issue a GJ subpoena, or even a civil investigative demand, the USAO simply requested by letter that the bank voluntarily produce documents concerning its electronic payments program.

--The bank cooperated immediately (value to the bank in doing this—under the USSG the bank can get credit for cooperating with an investigation immediately upon being notified that there is a problem)

--After evaluating its records, the bank admitted a serious problem arising from its relations with a number of TPPPS and telemarketing and internet merchants.

--The bank's own investigation resulted in the termination of the bank's CEO and virtually all of its senior management

--We worked closely with the FDIC, the bank's regulator, to review its examination reports and determine the depth and scope of the bank's involvement in the fraud
--Also obtained information from FTC, which had been investigating the processors and the fraudulent merchants.
--Realized that the bank was deeply involved in the scheme. Here's what we found:

--One TPPP, Landmark Clearing, initiated more than 950,000 RCC transactions for an aggregate dollar amount of more than $57.2M from April 2010 to March 2011. The return rate for those transactions was more than 53 percent on a transaction basis.
--Another TPPP, Check Site, initiated more than 1.2 million RCC transactions worth more than $46M. Return rate was more than 55 percent.
--Another TPPP, Check 21, initiated more than 353,000 RCC transactions worth more than $15.4M with a return rate of more than 55 percent.

--Again, the bank did not dispute the evidence or our theory of liability.

--On the contrary, it fired all of the bank's officers, including its president, chief compliance officer, chief operations officer, and director of its electronic payments program.
--FBD also terminated its relationship with all of its TPPPs

--Estimate of consumer loss was about $150M
--From 2009-2011, FBD attempted to process approximately $359M in ACH and RCC transactions from 4 notorious TPPPs and their merchants.
--Of this $359M, approximately $205M – or 57 % -- were returned and therefore did not result in a consumer loss.
--Ultimately, the government brought FIRREA charges against the bank (allowing for civil money penalties when proof of predicate criminal acts by a preponderance of evidence)
--FIRREA permits the government to recover the amount of loss.
--In this case, during the investigation, FBD announced that intended to sell its assets to another FI and cease its banking operations by the end of 2012.
--Based on the amount of assets on hand, and working with FDIC and FinCEN, we worked out a $15M CMP

What We're Doing
-- Holding financial institutions, including Money Services Businesses, accountable to their BSA/AML obligations and making sure they have robust and vibrant Anti-Money Laundering policies and procedures in place. Of course, these policies and procedures must include, at a minimum:

--internal policies, procedures, and controls designed to guard against money laundering;
--an individual to coordinate and monitor day to day compliance with the BSA and AML requirements;
--ongoing employee training; and

--independent testing for compliance conducted by bank personnel or an outside party.

--FinCEN financial advisory
--FinCEN webinar (FTC, FDIC, OCC, DOJ, FBI, and CFPB) (KYC is not enough; must know your customer's customer)
--new initiative focused on banks and TPPPs; recently took someone on a detail to work exclusively on these cases; we created a strategic plan and are pursuing it
--Also, I spoke to CSBS about having the states consider amending their money transmitting rules to include TPPPs as money transmitters
-- In addition, requiring payment processors to register as a money transmitter with a state has significant law enforcement implications, since 18 U.S.C. § 1960 makes it a crime punishable by up to 5 years in prison for a money transmitting business to operate in a state requiring a money transmitter license without such a license. If more states were to require payment processors to register as money transmitters, prosecutors would have a powerful weapon with which to pursue unlawful payment processors under § 1960 and, we expect, severely curtail the risky and unlawful conduct described above.

Conclusion
-- As I said at the outset, the Consumer Protection Working Group of the Task Force is dedicating a significant amount of attention to this issue, and we are approaching it in a smart, systematic, and coordinated way. The principle behind this new enforcement initiative is this: If we can eliminate the mass-marketing fraudsters' access to the U.S. financial system—that is, if we can stop them from getting paid—then we can significantly reduce the harm caused by this type of fraud. Third-party payment processors are what we call the bottleneck in this problem. Most mass-marketing fraudsters need them in order for their scams to work. We hope to close that access to the banking system—effectively putting a chokehold on it—and put a stop to this billion dollar problem that has harmed so many American consumers.

2013

Financial Fraud Enforcement Task Force Consumer Protection Working Group

Servicemember Subgroup

UNITED STATES ATTORNEY TOOLKIT FOR MILITARY CONSUMER FRAUD ENFORCEMENT