
From: [REDACTED]
Sent: Wednesday, May 15, 2013 2:21 PM
To: Sweet, Joel; [REDACTED]
Subject: RE: Pay Day Lending

Either day works for me-just let me know.

Thanks

From: Sweet, Joel
Sent: Wednesday, May 15, 2013 2:20 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Pay Day Lending

Monday could work for me.

From: [REDACTED]
Sent: Wednesday, May 15, 2013 2:09 PM
To: Sweet, Joel; [REDACTED]
Cc: [REDACTED]
Subject: RE: Pay Day Lending

I have something scheduled tomorrow that I might be able to move. Can you do lunch on Monday? If not, I will move my other thing.

From: Sweet, Joe [REDACTED]
Sent: Wednesday, May 15, 2013 2:04 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Pay Day Lending

How about lunch on Thursday? Josh is not available, but I'd like to bring [REDACTED] who is detailed to our office from Treasury.

From: [REDACTED]
Sent: Thursday, May 09, 2013 10:44 AM
To: Sweet, Joel; Cassak, Lance D.
Cc: Burke, Josh; Dunn, Charles B. (CIV)
Subject: RE: Pay Day Lending

Joel ~

As [REDACTED] mentioned, we've been looking closely at the EFTA - and the liability of both the originating banks and any of the processors to whom they give their routing number for access to the ACH system. NACHA (the FINRA like group over the ACH system) holds the bank liable if it lets a 3d party use its number for processing ACH debits/credits that are returned. And the rules require a system of oversight, but... Disincentives still abound.

Monday's tough next week. Tues, wed, thurs - either lunch or otherwise? Let us know what works.

Thanks.
Dana

From: Sweet, Joel [REDACTED]
Sent: Tuesday, May 07, 2013 12:23 PM
To: [REDACTED]; [REDACTED]
Cc: [REDACTED] Dunn, Charles B. (CIV)
Subject: Pay Day Lending

[REDACTED] and [REDACTED] –

We have an idea for a joint project that we want to jump on ASAP. A provision of the Electronic Funds Transfer Act, 15 U.S.C. Sec. 1693k, states:

This material has been redacted.

[REDACTED] We need your expertise and
experience. Can we do this together?

And in response to your question below – yes -- let's have lunch (Thursday?) and discuss further.

Best,

Joel

Joel M. Sweet, Trial Attorney
Consumer Protection Branch
United States Department of Justice
450 5th Street, NW
Washington, DC 20530 (20001 for Fedex/UPS)

T: [REDACTED]
[REDACTED]

From: [REDACTED] [REDACTED] [REDACTED]

Sent: Monday, May 06, 2013 6:05 PM

To: Sweet, Joel

Cc: [REDACTED]

Subject: Re: Combining efforts

Joel,

Lance and are in a workshop in Va on negotiation strategies on tues and wed. Do you think we shd set up a time to talk or have lunch or what? (I, for one, am always game for lunch.)

[REDACTED]

[REDACTED] [REDACTED]
Counsel

Legal Division, Consumer Enforcement Unit

Federal Deposit Insurance Corporation

550 17th Street, N.W., F-2034

Washington, D.C. 20429

[REDACTED]
[REDACTED] [REDACTED]

From: Sweet, Joel [REDACTED]

Sent: Wednesday, May 01, 2013 05:49 PM

To: [REDACTED]

Cc: [REDACTED]

Subject: RE: Combining efforts

Guys –

I am out tomorrow and Friday. Let's talk early next week. I've got a plan.

JMS

From: [REDACTED]
Sent: Monday, April 29, 2013 6:35 PM
To: Sweet, Joel
Cc: [REDACTED]
Subject: Re: Combining efforts

At your pleasure.

[REDACTED]
Counsel
Legal Division, Consumer Enforcement Unit
Federal Deposit Insurance Corporation
550 17th Street, N.W., F-2034
Washington, D.C. 20429

From: Sweet, Joel [REDACTED]
Sent: Monday, April 29, 2013 06:33 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Combining efforts

Let's discuss further.

From: [REDACTED]
Sent: Monday, April 29, 2013 1:12 PM
To: Sweet, Joel
Cc: [REDACTED]
Subject: Combining efforts

Joel

Thanks again for taking the time for walking Marguerite through everything last week. When you get a chance, Lance and I would like to talk to you about whether or not there is a possibility of a detail to your project in which we could combine forces. We don't have nearly the manpower you do here but there's a very great interest in the same goal.

We haven't yet talked to our higher powers; we want to talk to you about a) whether it's feasible and b) how we could go about getting it done. Lance has had decades in banking and private sector litigation; I've been a litigator at both DOJ and the FTC as well as with a cyber-forensics firm, and was detailed from the FTC to the USAO for the SDFIa as a SAUSA. I worked at the FTC for a long time with [REDACTED] who I think is one of your colleagues in Consumer Lit.

Give us a buzz when you get a chance.

Thanks much.

[REDACTED]

[REDACTED]
Counsel, Consumer Enforcement Unit
Legal Division, FDIC
[REDACTED]
[REDACTED]

From: [REDACTED]
Sent: Monday, March 11, 2013 1:36 PM
To: Sweet, Joel (CIV)
Cc: [REDACTED]
Subject: RE: Pay Day Lending and third party processors

Joel

We can do 10 ish tomorrow if that would work but I have a short day. We would be happy to come to you.

Is that ok?

Thanks.

[REDACTED]

From: Sweet, Joel (CIV) [REDACTED]
Sent: Monday, March 11, 2013 1:10 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Pay Day Lending and third party processors

How about tomorrow, Tuesday? Can you guys come here (450 Fifth St, NW)?

From: [REDACTED] [REDACTED]
Sent: Thursday, March 07, 2013 6:37 PM
To: Sweet, Joel (CIV)
Cc: Cassak, Lance D.
Subject: RE: Pay Day Lending and third party processors

Joel --

Is there a day next week that would be good for lunch? We would really like to pick your brain on some issues that have come up.

I'm going to be traveling a bit of the week of the 18th, then it's Spring Break and LegoLand for me the week of the 25th.

Thanks.

[REDACTED]

From: Sweet, Joel (CIV) [REDACTED]
Sent: Thursday, February 28, 2013 6:12 PM
To: [REDACTED]
Subject: Pay Day Lending

Dana --

Sorry it's taken a couple of days for me to get back to you. Just got my email and phone up and running today. Please call me if you and your colleagues want to discuss PDL. I'll be travelling tomorrow best to send an email.

Best,
Joel

Joel M. Sweet
Consumer Protection Branch, DOJ

T [REDACTED]

From: [REDACTED]
Sent: Tuesday, April 23, 2013 12:15 PM
To: Sweet, Joel
Subject: RE: Meeting

Thanks. Look forward to seeing you.

[REDACTED]

From: Sweet, Joel [REDACTED]
Sent: Tuesday, April 23, 2013 11:31 AM
To: [REDACTED]
Subject: RE: Meeting

450 5th Street, NW

From: [REDACTED]
Sent: Tuesday, April 23, 2013 10:08 AM
To: Sweet, Joel
Subject: RE: Meeting

Joel,

Can you give me your street address again so I know where we are going? It's the old SEC bldg., right?

Thanks.

[REDACTED]

From: Sweet, Joel [REDACTED]
Sent: Monday, April 22, 2013 5:46 PM
To: [REDACTED]
Subject: RE: Meeting

Let's meet here, as there is a greater likelihood that others in my group will be able to join us. Thanks for the accommodation of the start time.

From: [REDACTED]
Sent: Monday, April 22, 2013 5:44 PM
To: Sweet, Joel; [REDACTED]
Subject: RE: Meeting

3 pm this Wednesday looks fine by everyone's calendar here (if I am reading the calendar wrong, I will let you know tomorrow). As to where we meet, it is your call. If you would like us to come to you, that's fine. If you don't mind a trip to this side of town (we are a short distance from the White House), we can do it here. Please let me know your preference. Thanks.

From: Sweet, Joel [REDACTED]
Sent: Monday, April 22, 2013 5:38 PM
To: [REDACTED]
Subject: RE: Meeting

[REDACTED] and [REDACTED] -- Are we set for this day/time? Is there any chance we can push back until 3 pm (I will be in Phila at a school event in the morning and I want to be sure that I'm not late to our meeting.) Where should we meet? Thanks, Joel

From: [REDACTED]
[REDACTED], April 15, 2013 3:21 PM
To: Sweet, Joel
Cc: [REDACTED]
Subject: RE: Meeting

Why don't we set 2:00 on Wednesday April 24th for the meeting. Thanks again.

From: [REDACTED]
Sent: Monday, April 15, 2013 10:12 AM
To: 'Sweet, Joel'
Cc: [REDACTED]
Subject: RE: Meeting

Thanks. I will talk to Marguerite and [REDACTED] and get back to you with a time to meet.

As for FDIC's internal structure, FDIC has nine different Divisions. One of them is the Division of Depositor and Consumer Protection ("DCP"), which handles consumer protection. That is headed up by Mark Pearce. He is trained as a lawyer but it is not a legal position. He is what might be called "the client".

In banking agencies, the primary focus is on supervision and regulation of insured institutions, which is basically done by examiners and others who track what is happening on a regular basis in the banks. Lawyers play a secondary role, helping out supervision (as opposed to DOJ, which it appears to an outsider is predominantly staffed by lawyers and lawyers run the show). Mark has a number of lawyers doing his work, all in the Legal Division (another of the nine Divisions). The head of DCP's legal team is Assistant General Counsel Jim Anderson. Jim has two Units reporting to him: Compliance and Enforcement. Marguerite is the supervisor, reporting directly to Jim, of all of the attorneys in Consumer Enforcement. [REDACTED] and I are in the Consumer Enforcement Unit and Marguerite is our immediate boss.

I hope this helps. If you have further questions, please let us know.

From: Sweet, Joel [REDACTED]
Sent: Friday, April 12, 2013 5:54 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Meeting

Sure thing. Next week I am available only Tuesday morning or after 3 pm. The following week, open except for Monday 9-1, Tuesday 1-4.

Please help me out a bit. What is your branch called officialy? And who is the head of it, Sagatelian or Pierce?

Thanks,

Joel

From: [REDACTED]
Sent: Friday, April 12, 2013 3:34 PM
To: Sweet, Joel
Cc: [REDACTED]
Subject: Meeting

Marguerite Sagatelian, the head of Consumer Enforcement here at the FDIC and [REDACTED]'s and my immediate boss, has asked us to see if you would be willing to meet with her [REDACTED] and I would be there as well). I think [REDACTED] wants to meet to discuss pretty much what we talked about in our meeting. Do you have any time next week or in the near future to get together? Thanks.

From: [REDACTED]
Sent: Friday, April 26, 2013 8:47 AM
To: Sweet, Joel (CIV) [REDACTED]
Cc: [REDACTED]
Subject: Devices under 18 USC 1029

Joel,

I was referring to 18 USC 1029 the other day, trafficking in devices, since checks sent through the ACH system with routing and numbers are arguably "devices" under 1029(e)(1), and they are received by wire.

And if, just if you want to go that way, that's a predicate for criminal RICO.

[REDACTED]

From: [REDACTED]
Sent: Monday, May 20, 2013 10:26 AM
To: Sweet, Joel
Cc: [REDACTED]; [REDACTED]
Subject: RE: Thoughts for lunch?

No -- shouldn't need a reservation. We'll see you at the Exchange at 12:30.

From: Sweet, Joel [REDACTED]
Sent: Monday, May 20, 2013 10:23 AM
To: [REDACTED]
Cc: [REDACTED]; [REDACTED]
Subject: RE: Thoughts for lunch?

The Exchange sounds good. While we certainly can discuss our details, I'm far more interested in discussing detailed strategies to address legal initiative re: FPPPs and PD lenders. Do we need a reservation?

From: [REDACTED]
Sent: Monday, May 20, 2013 10:19 AM
To: Sweet, Joel
Cc: [REDACTED]; [REDACTED]
Subject: RE: Thoughts for lunch?

Oooh. The caf. How about The Exchange, a block away at 1719 G St NW. Almost as cheap, and more easily digested. Also, better acoustics. Happy to have [REDACTED]. We want to hear details about details! Also happy to be joined by [REDACTED] if she's available.

From: Sweet, Joel [REDACTED]
Sent: Monday, May 20, 2013 10:12 AM
To: Lesemann, Dana J.
Cc: [REDACTED]; [REDACTED]
Subject: RE: Thoughts for lunch?

How about 12:30 at the FDIC cafeteria (fits my budget). I'll be joined by [REDACTED] a Treasury detailee working with me at CPB. Should I invite [REDACTED] from FTC?

From: [REDACTED]
Sent: Monday, May 20, 2013 9:17 AM
To: Sweet, Joel
Cc: [REDACTED]
Subject: Thoughts for lunch?

We're flexible.

[REDACTED]
Counsel, Consumer Enforcement Unit
Legal Division, FDIC

[REDACTED]

From: [REDACTED]
Sent: Monday, May 20, 2013 4:25 PM
To: Sweet, Joel; [REDACTED]
Cc: Bresnick, Michael J (ODAG); Goldberg, Richard; Burke, Josh
Subject: RE: FDIC DOJ Cooperation

Thanks. It was great talking to you and Ross as well. We have started our efforts here to find the right vehicle to work together and will be in touch soon.

From: Sweet, Joel [REDACTED]
Sent: Monday, May 20, 2013 4:23 PM
To: [REDACTED]
Cc: Bresnick, Michael J (ODAG); Goldberg, Richard; Burke, Josh
Subject: FDIC-DOJ Cooperation

Dana and Lance

It was good speaking with you guys today about the common interests of our agencies. I have worked closely with FDIC regional folks in the past with excellent results for both agencies. We all are working in the same space and have consumer protection agendas, so it makes sense to explore ways to work together for example by sharing investigative material to further our respective legal/enforcement actions. As I mentioned, we would welcome your assistance in evaluating anticipated subpoena responses from a large number of banks (many of them regulated by the FDIC). And we would like to continue our discussions about approaches to the payday lending industry.

I am bringing Mike Bresnick into the discussion. Mike is the Executive Director of the Financial Fraud Enforcement Task Force (stopfraud.gov), which includes both DOJ and FDIC. He may have insight and ideas about how we can better collaborate. Please feel free to speak with Mike directly.

Joel M. Sweet, Trial Attorney
Consumer Protection Branch
United States Department of Justice

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

From: Benardo, Michael B.
Sent: Tuesday, April 05, 2011 3:32 PM
To: Hartigan, Frank A.
Subject: FW: Supervisory Insights Article on Third Party Payment Processor Relationships

Importance: High

FYI.

From: Benardo, Michael B.
Sent: Tuesday, April 05, 2011 3:30 PM
To: Wirtz, Robert J.
Subject: RE: Supervisory Insights Article on Third Party Payment Processor Relationships
Importance: High

Bob---

Here is the latest version of the TPPP SI journal article, in case you want to review it again.



TPPP Article v4 -
clean.docx

Frank and I were talking that to make sure this gets attention by both RM and DCP examiners that it would be good if a DCP person were a co-author. Would you like to be that person?

Mike

From: Wirtz, Robert J.
Sent: Thursday, March 31, 2011 1:25 PM
To: Benardo, Michael B.
Cc: Geiger, Jennifer M.; Cornell Pape, Anna C.
Subject: FW: Supervisory Insights Article on Third Party Payment Processor Relationships

Mike,

Very nice job on this. My suggested edits are in the attached document. I used track changes. On page 9, where you discuss consumer complaints in the top paragraph, I'm wondering if we should provide examples of the blogs or Web sites, for example, ripoffreport.com. I know we need to be careful about not providing an endorsement and we don't want banks to think they only need to research sites that we mention. Just a thought.

Bob

From: Benardo, Michael B.
Sent: Wednesday, March 30, 2011 7:53 PM
To: Wirtz, Robert J.; Geiger, Jennifer M.; Cornell-Pape, Anna C.
Subject: Supervisory Insights Article on Third Party Payment Processor Relationships

If you have time...

Attached is the first draft of a Supervisory Insights article on Third Party Payment Processor Relationships. If you have time, I would appreciate it if you (or a designee) could review it and provide comments to me, especially from each of your unique perspectives.

<< File: TPPP Article.docx >>

Unfortunately, I am a bit behind in comparison to the production schedule for the next issue of Supervisory Insights, so I ask that you provide comments soon.

Thank you,

Mike

Managing Risks in Third-Party Payment Processor Relationships

During the past few years, the Federal Deposit Insurance Corporation (FDIC) has observed an increase in the number of deposit relationships between financial institutions and third-party payment processors and a corresponding increase in the risks associated with these relationships. Deposit relationships with payment processors can expose financial institutions to risks not present in typical commercial customer relationships, including greater strategic, credit, compliance, transaction, legal, and reputation risk. It was for this reason in 2008 that the FDIC issued *Guidance on Payment Processor Relationships* which outlines risk mitigation principles for this type of higher-risk activity.¹

Although many payment processors effect legitimate payment transactions for a variety of reputable merchants, an increasing number of processors have been initiating payments for abusive telemarketers; deceptive online merchants; and organizations that engage in high risk or illegal activities. In the absence of adequate monitoring systems and controls, a financial institution could be facilitating unauthorized transactions and, ultimately, unfair and deceptive practices resulting in financial harm to the consumer. Therefore, it is essential that financial institutions and examiners recognize and understand the risks associated with these relationships.

This article explains the role of third-party payment processors and the risks they can present to financial institutions, identifies warning signs that may indicate heightened risk in a payment processor relationship, and discusses the risk mitigation controls that should be in place

¹Financial Institution Letter (FIL) 127-2008. *Guidance on Payment Processor Relationships*, dated November 7, 2008. See: <http://www.fdic.gov/news/news/financial/2008/fil08127.html>

to manage this risk. The article concludes with an overview of supervisory remedies that may be used when it is determined that a financial institution does not have an adequate program in place for monitoring and addressing the risks associated with third-party payment processor relationships.

Background

The core elements of managing third-party risk are present in payment processor relationships (e.g., risk assessment, policies and procedures, due diligence, and oversight). However, managing these risks can be particularly challenging as the financial institution does not have a direct customer relationship with the payment processor's merchant clients. Furthermore, the risks associated with this type of activity are heightened when neither the payment processor nor the financial institution performs adequate due diligence, such as verifying the identities and business practices of the merchants for which payments are originated and implementing a program of ongoing monitoring for suspicious activity.

For example, in a typical third-party payment processor relationship, the payment processor is a deposit customer of the financial institution which uses its deposit account to process payments for its merchant clients. The payment processor receives lists of payments to be generated by the merchant clients for the payment of goods or services and initiates the payments by creating and depositing them into a transaction account at a financial institution. In some cases, the payment processor may establish individual accounts at the financial institution in the name of each merchant client and deposit the appropriate payments into these accounts. The merchant may then be a co-owner of the deposit account and make withdrawals from the

account to receive its sales proceeds, or the payment processor may periodically forward the sales proceeds from the account to the merchant. Alternatively, the payment processor may commingle payments originated by the merchant clients into a single deposit account in the name of the payment processor. In this case, the payment processor should maintain records to allocate the deposit account balance among the merchant clients.

Payment Types Used by Third-Party Payment Processors

Payment processors may offer merchants a variety of alternatives for accepting payments including credit and debit card transactions, traditional check acceptance, Automated Clearing House (ACH) debits and other alternative payment channels. The potential for misuse or fraud exists in all payment channels. However, the FDIC has observed that some of the most problematic activity occurs when originating ACH debits or creating and depositing remotely created checks.

Automated Clearing House Debits

The Automated Clearing House (ACH network) is a nationwide electronic payment network which enables participating financial transactions to distribute electronic credit and debit entries to bank accounts and settle these entries.

Common ACH credit transfers include the direct deposit of payroll and certain benefits payments. Direct debit transfers also may be made through the ACH network and include consumer payments for insurance premiums, mortgage loans, and other types of bills. Rules and regulations governing the ACH networks are established by NACHA - The Electronic Payments

Association (formerly National Automated Clearing House Association)² and the Board of Governors of the Federal Reserve.

Third-party payment processors initiate ACH debit transfers as payments for merchant clients by submitting these transfers, which contain the consumer's financial institution routing number and account number (found at the bottom of a check) to their financial institution to enter into the ACH networks. Telemarketers and online merchants obtain this information from the consumer and transmit it to the payment processor to initiate the ACH debit transfers. The risk of fraud arises when an illicit telemarketer or online merchant obtains the consumer's account information through coercion or deception and initiates an ACH debit transfer that may not be fully understood or authorized by the consumer.

As with all payment systems and mechanisms, the financial institution bears the responsibility of implementing an effective system of internal controls and ongoing account monitoring for the detection and resolution of fraudulent ACH transfers. If an unauthorized ACH debit is posted to a consumer's account, the procedures for resolving errors contained in the Federal Reserve Board's Regulation E, which governs electronic funds transfers,³ provide the consumer 60 days after the financial institution sends an account statement to report the unauthorized ACH debit.⁴ Regulation E requires the consumer's financial institution to investigate the matter and report to the consumer the results of the investigation within a

² NACHA establishes the rules and procedures governing the exchange of automated clearinghouse payments. See http://www.nacha.org/c_achrules.cfm.

³ Provisions of the Federal Reserve Board's Regulation E establish the rights, liabilities, and responsibilities of participants in electronic fund transfer systems, such as automated teller machine transfers, telephone bill-payment services, point-of-sale terminal transfers, and preauthorized transfers from or to a consumer's account.

⁴ 12 CFR Section 205.11.

prescribed time frame. In the case of an ACH debit, when a consumer receives a refund for an unauthorized debit, ACH rules permit the consumer's financial institution to recover the amount of the unauthorized payment by returning the debit item to the originating financial institution.

Remotely Created Checks

Remotely Created Checks (RCCs), often referred to as “demand drafts,” are payment instruments that do not bear the signature of a person on whose account it is drawn. In place of the signature, the RCC bears the account holder's printed or typed name, or a statement that the account holder's signature is not required or the account holder has authorized the issuance of the check. Similar to the initiation of an ACH debit transfer, an account holder authorizes the creation of an RCC by providing his financial institution's routing number and his account number. Examples of RCCs are those created by a credit card or utility company to make a payment on an account, or those initiated by telemarketers or online merchants to purchase goods or services.

The risk of fraud associated with RCCs is often greater than the risk associated with other kinds of debits that post to transaction accounts. For example, a fraudster might obtain a consumer's account information by copying it from an authorized check or tricking the consumer into providing the information over the telephone or the Internet. Once the necessary information is obtained, the fraudster can generate unauthorized RCCs and forward them for processing. Similar to the responsibilities associated with the ACH network, the financial institution should implement an effective system of internal controls and account monitoring to identify and resolve the unauthorized RCC. However, because RCCs are cleared in the same

manner as traditional checks, there is no way to differentiate between the two and, therefore, no efficient way to measure the volume or use of RCCs.

RCCs may be processed as a paper item through the customary clearing networks or converted to and processed as an ACH debit. However, check clearing and ACH rules differ as to the re-crediting of an accountholder for an unauthorized RCC and how losses are allocated by and between the participating financial institutions. RCCs processed as checks are governed by provisions of the Uniform Commercial Code (UCC) and the Expedited Funds Availability Act,⁵ as implemented by Regulation CC. RCCs converted to ACH debits are governed by applicable ACH rules, the Electronic Fund Transfer Act, and Regulation E.

In response to heightened concern about the risk of fraud, in 2005 the Board of Governors of the Federal Reserve amended Regulation CC to transfer the liability for losses resulting from unauthorized RCCs.⁶ At the same time, the Board also amended Regulation J (the Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire) to clarify that certain warranties, similar to those provided under the UCC, apply to RCCs collected through the Reserve Banks. In conjunction with Regulation CC, the amendments to Regulation J shifted the liability for losses attributed to unauthorized RCCs to the financial institution where the check is first deposited as this institution is in the best position to know its customer (the creator of the RCC) and determine the legitimacy of the deposits. The liability also creates an economic incentive for depository institutions to perform enhanced due

⁵ The Expedited Funds Availability Act (EFAA) enacted in 1987, addresses the issue of delayed availability of funds by banks. The EFAA requires banks to (1) make funds deposited in transaction accounts available to customers within specified time frames, (2) pay interest on interest-bearing transaction accounts not later than the day the bank receives credit, and (3) disclose funds-availability policies to customers.

⁶ Effective July 1, 2006 [70 Fed. Reg. 71218-71226 (November 28, 2005)]

diligence on those customers depositing RCCs. Furthermore, by providing the paying financial institution with the ability to recover against the financial institution presenting the unauthorized RCC, it should make it easier for customers to obtain re-credits.⁷

Types of High Risk Payments

Although some clients of payment processors are reputable merchants, an increasing number are not and should be considered “high risk.” These disreputable merchants use payment processors to charge consumers for questionable or fraudulent goods and services. Often a disreputable merchant will engage in high pressure and deceptive sales tactics, such as aggressive telemarketing or enticing and misleading pop-up advertisements on Web sites. Still other disreputable merchants will use processors to initiate payments for the sale of products and services, including, but not limited to, unlawful Internet gambling and the illegal sale of tobacco products on the Internet. For example, consumers should be cautious when Web sites offer “free” information and ask consumers to provide payment information to cover a small shipping and handling fee. In some instances and without proper disclosure, consumers who agreed to pay these fees, often found their bank accounts debited for more than the fee and enrolled in costly plans without their full understanding and consent.⁸

Generally, high-risk transactions occur when the consumer does not have a familiarity with the merchant, or when the quality of the goods and services being sold is uncertain.

Activities involving purchases made over the telephone or on the Internet tend to be riskier in

⁷ Changes to Federal Reserve Bank Operating Circular No. 3 on the Collection of Cash Items and Returned Checks clarifies that electronically created images (including RCC items) that were not originally captured from paper are not eligible to be processed as Check 21 items (effective July 15, 2008). www.frb-services.org/files/regulations.pdf#operating_circular_3.pdf.

⁸ Rules governing the use of telemarketing require verifiable authorization of payment for services. See the Federal Trade Commission Telemarketing Sales Rule [16 CFR 310]. See: <http://www.ftc.gov/os/2002/12/astfinalrule.pdf>.

that the consumer cannot fully examine or evaluate the product or service purchased. Similarly, the consumer may not be able to verify the identity or legitimacy of the person or organization making the sale.

Some merchant categories that have been associated with high-risk activity include, but are not limited to:

- Ammunition Sales
- Cable Box de-scramblers
- Coin Dealers
- Credit Card Schemes
- Credit Repair Services
- Dating Services
- Debt Consolidation Scams
- Drug Paraphernalia
- Escort Services
- Firearms Sales
- Fireworks Sales
- Gambling
- Get Rich Products
- Government Grants
- Home-Based Charities
- Human Growth Hormone
- Life Time Guarantees
- Life Time Memberships
- Debt Consolidation Scams
- Lottery Sales
- Mailing Lists/Personal Info
- Money Transfer Networks
- Pyramid Type Sales
- Pay Day Loans
- Pharmaceutical Sales
- Pornography
- Ponzi Schemes
- Racist materials
- Surveillance equipment
- Telemarketing
- Tobacco Sales
- Travel clubs

Of particular concern, the FDIC and other federal regulators have seen an increase in payment processors initiating payment for online gaming activities that may be illegal. The Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) prohibits financial institutions from accepting payments from any person engaged in the business of betting or wagering with a business in unlawful Internet gambling (see the FDIC's Financial Institution Letter on the *Unlawful Internet Gambling Enforcement Act*, FIL-35-2010, dated June 30, 2010).⁹

High-Risk Payment Processor Relationship Red Flags

Financial institutions and examiners should be aware of the warning signs that may indicate heightened risk in a payment processor relationship. One of the more telling is a high volume of consumer complaints that suggest a merchant client is inappropriately obtaining personal account information; misleading customers as to the quality, effectiveness, and usefulness of the goods or services being offered; or misstating the sales price or charging additional, and sometimes recurring, fees that are not accurately disclosed or properly authorized during the sales transaction. However, this may be somewhat difficult to determine in that it may be almost impossible for financial institutions and examiners to know if consumers are submitting complaints directly to the payment processor or the merchants. Although, in some cases, consumers voice their dissatisfaction on Web sites, such as those for regional Better Business Bureaus, or blogs intended to collect and share such information to alert other consumers.

⁹ 12 CFR Part 233 Regulation GG, Financial Institution Letter (FIL) 35-2010. *Unlawful Internet Gambling Enforcement Act*, dated June 30, 2010. See <http://www.fdic.gov/news/news.financial/2010/fil10035.html>

In response, financial institutions with third-party payment processor relationships should monitor the Internet for complaints that mention them by name. The financial institution's name typically appears on the face of a RCC or in the record of an ACH debit. As a result, consumers often associate the financial institution with the transaction and may complain about the institution facilitating the payment. Finally, complaints also may be lodged with the depository financial institution by the financial institution of the consumer whose account was charged. As required by statute and federal regulation, the depository financial institution must acknowledge, research, and respond to each complaint made directly to them.

Another indication of the potential for heightened risk in a payment processor relationship is a large number of returns or charge backs. Consumers who are dissatisfied with goods or services delivered or provided, or consumers who feel they were deceived or coerced into providing their account information, can request their financial institution return the RCC or ACH debit to the depository financial institution as an unauthorized transaction. In addition, items may be returned if insufficient funds are available to cover the unauthorized items, resulting in the consumer's account being overdrawn. In these circumstances, the items often are returned as "NSF" rather than as "unauthorized." Accordingly, financial institutions with payment processor relationships should implement systems to monitor for higher rates of returns or charge backs, which can be evidence of fraudulent activity.

Another red flag is a significant amount of activity which generates a higher than normal level of fee income. In an increasingly competitive market place, financial institutions are looking for ways to grow non-interest fee income, and this is especially true for troubled

institutions. Although fee income from third-party payment processor relationships may benefit an institution's bottom line, it can indicate an increased level of risk. Side agreements may be established between payment processors and financial institutions, whereby the payment processor pays the institution a fee for each item deposited, generating a higher level of fee income. However, the greatest source of income from these relationships tends to be those fees generated by the financial institution charging the payment processor for each returned item.

As a caveat, financial institutions and examiners should be alert for payment processors that use more than one financial institution to process merchant client payments, or nested arrangements where a payment processor's merchant client is also doing third-party payment processing. Spreading the processing by and among several institutions may allow processors to avoid detection, such as through ongoing, high levels of returned items at a single institution. Payment processors also may use multiple financial institutions in case one or more of the relationships is terminated as a result of suspicious activity.

Finally, another troubling development is payment processors that purposefully solicit business relationships with troubled institutions in need of capital. Payment processors identify and establish relationships with troubled institutions as these institutions may be more willing to engage in higher-risk transactions in return for increased fee income. In some cases, payment processors have made a commitment to purchase stock in certain troubled financial institutions or guarantee to retain a large deposit with the institution, thereby providing additional, needed capital. Often, the targeted financial institutions are smaller institutions that lack the infrastructure to properly manage or control a third-party payment processor relationship.

Risk Mitigation Controls

As mentioned earlier in this article, a framework for prudently managing relationships with third-party payment processors was communicated in the FDIC's 2008 *Guidance on Payment Processor Relationships*.¹⁰ Financial institutions in relationships with payment processors should establish clear lines of responsibility for controlling the associated risks. Such responsibilities include effective due diligence and underwriting, as well as ongoing monitoring of high-risk accounts for an increase in unauthorized returns and suspicious activity and maintenance of adequate reserves. The relationship should be governed by a written contract between the financial institution and the third-party payment processor which outlines each party's duties and responsibilities. Implementing appropriate and effective controls over payment processors and their merchant clients will help identify those processors working with fraudulent telemarketers or other unscrupulous merchants and help ensure the financial institution does not facilitate such transactions.

Due Diligence and Underwriting

Due diligence and prudent underwriting standards are critical components of a risk mitigation program. Financial institutions should implement policies and procedures that reduce the likelihood of establishing or maintaining a relationship with payment processors through which unscrupulous merchants can access customers' deposit accounts.

¹⁰Financial Institution Letter (FIL) 127-2008, *Guidance on Payment Processor Relationships*. November 7, 2008. <http://www.fdic.gov/news/news/financial/2008/fil08127.html>

Financial institutions that initiate transactions for payment processors should develop a processor approval program that extends beyond credit risk management. This program should incorporate an effective due diligence and underwriting policy that, among other things, requires background checks of payment processors and merchant clients. A processor approval program will help validate the activities, creditworthiness, and business practices of the payment processor and should, at a minimum, authenticate the processor's business operations and assess the entity's risk level. Any processor assessment should include:

- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele.

- Determining if the processor re-sells its services to a third party referred to as an "agent or provider of Independent Sales Organization opportunities" or "gateway arrangements."¹¹

- Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants

- Identifying the major lines of business and volume for the processor's customers.

¹¹ An Independent Sales Organization is a company contracted to procure new merchant relationships. Gateway arrangements are similar to Internet service providers that sell excess computer storage capacity to third parties, which in turn distribute computer services to other individuals unknown to the provider. The third party would make decisions about who would be receiving the service, although the provider would be responsible for the ultimate storage capacity.

- Establishing appropriate reserves for each individual merchant processor based on the type of client and the risk involved in the transactions processed.
- Reviewing corporate documentation, including independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.

Financial institutions should require the payment processor to provide information on its merchant clients, such as the merchant's name, principal business activity, geographic location, and sales techniques. Additionally, financial institutions should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business. Such verification could include comparing the identifying information with public record, fraud databases and a trusted third party, such as a credit report from a consumer reporting agency or the state Better Business Bureau, or checking references from other financial institutions.

Ongoing Monitoring

Financial institutions are required to have a Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program and appropriate policies, procedures, and processes in place for monitoring, detecting, and reporting suspicious activity.¹² However, non-bank payment

¹² Banks, bank holding companies, and their subsidiaries are required by federal regulations to file a Suspicious Activity Report if they know, suspect, or have reason to suspect the transaction may involve potential money laundering or other illegal activity: is designed to evade the Bank Secrecy Act or its implementing regulations; has no business or apparent lawful purpose, or is not the type of transaction in which particular customer would normally be expected to engage. See 12 C.F.R. 353.

processors generally are not subject to BSA/AML regulatory requirements and, therefore, some payment processors may be vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. The Federal Financial Institutions Examination Council BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk with respect to third-party payment processors. As a result, a financial institution's risk mitigation program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.¹³

Appropriate Supervisory Responses

In those instances where examiners determine that a financial institution fails to have an adequate program in place to monitor and address risks associated with third-party payment processor relationships, formal or informal enforcement actions may be appropriate. Formal actions have included Cease and Desist Orders under Section 8(b) or 8(c) of the *Federal Deposit Insurance (FDI) Act*, as well as assessment of Civil Money Penalties under Section 8(i) of the FDI Act. These orders have required the financial institution to immediately terminate the high-risk relationship and establish reserves or funds on deposit to cover anticipated charge backs.

As appropriate, the primary federal regulator (PFR) will determine if financial institution management has knowledge that the payment processor or the merchant clients are engaging in unfair and deceptive practices in violation of Section 5 of the FTC Act. In those cases where a financial institution does not conduct due diligence, accepts a heightened level of risk, and

(http://www.ffiec.gov/bsa_aml_infobase/pages_manual/regulations/12CFR353.htm) and 31 CFR 103.18
(http://www.ffiec.gov/bsa_aml_infobase/pages_manual/regulations/31CFR103.pdf)

¹³ See: "Third Party Payment Processors Overview," from the Bank Secrecy Act/Anti Money Laundering Examination Manual.
http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_663.htm

allows transactions for high-risk merchants to pass through it, it may be determined that the financial institution is aiding and abetting the merchants. This also could indicate a disregard for the potential for financial harm to consumers and, as a result, the financial institution may be required to provide restitution.

Conclusion

The FDIC supports financial institution participation in payment systems to serve the needs of legitimate payment processors and their merchant clients. However, to limit potential risks, financial institutions should implement risk mitigation policies and procedures that include appropriate oversight and controls commensurate with the risk and complexity of the activities. At a minimum, risk mitigation programs should assess the financial institution's risk tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, and monitor payment processor relationships for suspicious activity.

Financial institutions should act promptly if they believe fraudulent or improper activities have occurred related to a payment processor's activities. Appropriate actions may include filing a Suspicious Activity Report, requiring the payment processor to cease processing for that specific merchant, or terminating the financial institution's relationship with the payment processor. Should it be determined by the PFR that a financial institution does not have an adequate program in place to monitor and address the risks associated with third-party payment processor relationships, an appropriate supervisory response will be used to require the financial institution to correct the deficiencies.

Michael B. Benardo

Chief, Cyber-Fraud and Financial Crimes Section

Division of Risk Management Supervision



Robert J. Wirtz

Assistant Regional Director (Compliance)

Division of Depositor and Consumer Protection



Kathryn M. Weatherby

Examination Specialist (Fraud)

Cyber-Fraud and Financial Crimes Section

Division of Risk Management Supervision



From: Benardo, Michael B.
Sent: Tuesday, November 15, 2011 2:02 PM
To: Bowman, John B.
Subject: RE: TPPP FIL

John—

Sorry for the delay in getting back to you.

I agree that, from a formatting perspective, the footnote doesn't really work on the cover page. I like where you put it, except that I would suggest a few edits to the footnote, so that it reads like this:

“Examples of telemarketing and online merchants that have displayed a higher incidence of consumer fraud or potentially illegal activities noted by the FDIC include: credit repair services, gambling, government grant or will writing kits, pay day or sub-prime loans, pornography, tobacco or firearms sales, sweepstakes, and magazine subscriptions. This list is not all-inclusive. While some of these activities might be legitimate, financial institutions should be aware of the increased risks associated with payments to such merchants.”

I red lined the attached copy. I would also suggest updating the month from September to November before sending it forward.



Final Revised TPPP
FIL (2011) ...

Let me know if you have any questions.

Mike

From: Bowman, John B.
Sent: Tuesday, November 15, 2011 9:46 AM
To: Benardo, Michael B.
Subject: TPPP FIL

Hi Mike:

I edited the FIL based on the recommendations from yesterday's briefing. I toyed with the idea of including a footnote on the first page but as you can see it moves things to the second page. So, I'm not so sure this is a workable solution. I also included a footnote on the second page, which is still upfront and should grab some attention. I'm just concerned with putting anything later in the document as the reader may not get the message. In any event, this is a starting point. Let me know what you think. Thanks.

<< File: Final Revised TPPP FIL (11-15-2011).doc >>

Regards,

John B. Bowman
Review Examiner Washington Office



PRIVILEGED & CONFIDENTIAL EXAMINATION MATERIAL: This message and any corresponding attachments are confidential and intended for the sole use of the individual(s) or entity(ies) to which the e-mail is addressed. If you are not the intended recipient, you must not review, retransmit, convert to hard-copy, copy, use or disseminate this e-mail or any of its attachments. If you received this e-mail in error please notify the sender immediately and delete it. Thank you.



Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-XX-2011
September November XX, 2011

Payment Processor Relationships Revised Guidance

Summary: Attached is revised guidance describing potential risks associated with relationships with third-party entities that process payments for telemarketers, online businesses, and other merchants. These relationships pose increased risk to institutions and require careful due diligence and monitoring. This guidance outlines certain risk mitigation principles for this type of activity.

Statement of Applicability to Institutions with Total Assets under \$1 Billion: This guidance applies to all FDIC-supervised financial institutions that have relationships with third-party payment processors.

Distribution:

FDIC Supervised Institutions

Suggested Routing:

Chief Executive Officer
Executive Officers
Compliance Officer
Chief Information Officer
BSA Officer

Related Topics:

Guidance on Payment Processor Relationships (FIL 127 2008, November 2008)
Consumer Protection, Compliance Risk, and Risk Management
FDIC Guidance for Managing Third Party Risk (FIL 44 2008, June 2008)
FFIEC Handbook on Retail Payment Systems (February 2010)
FFIEC Handbook on Outsourcing Technology Services (June 2004)
FFIEC Bank Secrecy Act/Anti Money Laundering (BSA/AML)
Examination Manual (April 2010)
Managing Risks in Third Party Payment Processor Relationships
(Summer 2011 Supervisory Insights Journal)

Attachment:

Revised Guidance on Payment Processor Relationships

Contacts:

Kathryn Weatherby, Examination Specialist (Fraud), Division of Risk Management Supervision, at kweatherby@fdic.gov or (703) 254 0469

John Bowman, Review Examiner, Division of Depositor and Consumer Protection, at jbowman@fdic.gov or (202) 898 6574

Note:

FDIC Financial Institution Letters may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2011/index.html

Highlights:

- Account relationships with entities processing payments for telemarketers or other high-risk merchants¹ require careful due diligence, close monitoring, and prudent underwriting.
- Account relationships with high-risk entities pose increased risks, including potentially unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act.
- Certain types of payment processors pose money laundering and fraud risks if merchant client identities are not verified and business practices are not reviewed.
- Financial institutions should assess risk tolerance in their overall risk assessment program and develop policies and procedures addressing due diligence, underwriting, and ongoing monitoring of high-risk payment processor relationships.
- Financial institutions should be alert to consumer complaints or unusual return rates that suggest the inappropriate use of personal account information and possible deception or unfair treatment of consumers.
- Financial institutions should act promptly when fraudulent or improper activities occur relating to a payment processor, including possibly terminating the relationship.
- Improperly managing these risks may result in the imposition of enforcement actions, such as civil

¹ Examples of high-risk telemarketers, merchants, or activities include credit repair services, escort services, gambling, government grant writing kits, pornography, payday loans, tobacco or ammunition sales, etc. This list is not all-inclusive. While some of these activities might be legitimate, financial institutions should be aware of the significant reputational risks associated with such relationships.

To receive FILs electronically, please visit
<http://www.fdic.gov/about/subscriptions/fil.html>
Paper copies may be obtained through the FDIC's Public
Information Center, 3501 Fairfax Drive, E 1002, Arlington, VA
22226 (877-275-3342 or 703-562-2200).

money penalties or restitution orders.

Revised Guidance on Payment Processor Relationships

The FDIC has recently seen an increase in the number of relationships between financial institutions and payment processors in which the payment processor, who is a deposit customer of the financial institution, uses its relationship to process payments for third-party merchant clients. Payment processors typically process payments either by creating and depositing remotely created checks (RCCs) often referred to as “Demand Drafts” or by originating Automated Clearing House (ACH) debits on behalf of their merchant customers. The payment processor may use its own deposit account to process such transactions, or it may establish deposit accounts for its merchant clients.

While many payment processors effect legitimate payment transactions for reputable merchants, telemarketing and online merchants² have displayed a higher incidence of consumer fraud or potentially illegal activities. In the absence of an effective means for verifying their merchant clients’ identities and reviewing their business practices, payment processors pose elevated money laundering and fraud risk for financial institutions, as well as legal, reputational, and compliance risks if consumers are harmed.

Financial institutions should understand, verify, and monitor the activities and the entities related to the account relationship. Although all of the core elements of managing third-party risk should be considered in payment processor relationships (e.g., risk assessment, due diligence, and oversight), managing this risk poses an increased challenge for the financial institution when there may not be a direct customer relationship with the merchant. For example, it may be difficult to obtain necessary information from the payment processor, particularly if a merchant is also a payment processor, resulting in a “nested” payment processor or “aggregator” relationship.

Financial institutions should ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner. These agreements should also protect financial institutions by providing for immediate account closure, contract termination, or similar action, as well as establishing adequate reserve requirements to cover anticipated charge backs. Accordingly, financial institutions should perform due diligence and account monitoring appropriate to the risk posed by the payment processor and its merchant base. Risks associated with this type of activity are further increased if neither the payment processor nor the financial institution performs adequate due diligence on the merchants for which payments are originated. Financial institutions are reminded that they cannot rely solely on due diligence performed by the payment processor. The FDIC expects a financial institution to adequately oversee all transactions and activities that it processes and to appropriately manage

² Examples of some telemarketing and online merchants that have displayed a higher incidence of consumer fraud or potentially illegal activities high-risk merchants or activities noted by the FDIC include: credit repair services, gambling, government grant or will writing kits, pay day or sub-prime loans, pornography, tobacco or firearms sales, sweepstakes, and magazine subscriptions, any activity that is illegal, or any business that seeks to avoid more stringent monitoring or scrutiny. This list is not all-inclusive. While some of these activities might be legitimate, financial institutions should be aware of the significant reputational increased risks associated with payments to such relationshipsmerchants.

and mitigate operational risks, Bank Secrecy Act (BSA) compliance, fraud risks, and consumer protection risks, among others.

Potential Risks Arising from Payment Processor Relationships

Deposit relationships with payment processors expose financial institutions to risks not customarily present in relationships with other commercial customers. These include increased operational, strategic, credit, compliance, and transaction risks. In addition, financial institutions should consider the potential for legal, reputational, and other risks, including risks associated with a high or increasing number of customer complaints and returned items, and the potential for claims of unfair or deceptive practices. *Financial institutions that fail to adequately manage these relationships may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity and, thus, may be liable for such acts or practices.* In such cases, the financial institution and responsible individuals have been subject to a variety of enforcement and other actions. Financial institutions must recognize and understand the businesses and customers with which they have relationships and the liability risk for facilitating or aiding and abetting consumer unfairness or deception under Section 5 of the Federal Trade Commission Act.³

Financial institutions should be alert for payment processors that use more than one financial institution to process merchant client payments or that have a history of moving from one financial institution to another within a short period. Processors may use multiple financial institutions because they recognize that one or more of the relationships may be terminated as a result of suspicious activity.

Financial institutions should also be on alert for payment processors that solicit business relationships with troubled financial institutions in need of capital. In such cases, payment processors will identify and establish relationships with troubled financial institutions because these financial institutions may be more willing to engage in higher-risk transactions in exchange for increased fee income. In some cases, payment processors have also committed to purchasing stock in certain troubled financial institutions or have guaranteed to place a large deposit with the financial institution, thereby providing additional, much-needed capital. Often, the targeted financial institutions are smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

Financial institutions also should be alert to an increase in consumer complaints about payment processors and/or merchant clients or an increase in the amount of returns or chargebacks, all of which may suggest that the originating merchant may be engaged in unfair or deceptive practices or may be inappropriately obtaining or using consumers' personal account information to create unauthorized RCCs or ACH debits. Consumer complaints may be made to a variety of sources and not just directly to the financial institution. They may be sent to the payment processor or

³ Under Section 8 of the Federal Deposit Insurance Act, the FDIC has authority to enforce the prohibitions against Unfair or Deceptive Acts or Practices (UDAP) in the Federal Trade Commission Act. UDAP violations can result in unsatisfactory Community Reinvestment Act ratings, compliance rating downgrades, restitution to consumers, and the pursuit of civil money penalties.

the underlying merchant, or directed to consumer advocacy groups or online complaint Web sites or blogs. Financial institutions should take reasonable steps to ensure they understand the type and level of complaints related to transactions that it processes. Financial institutions should also determine, to the extent possible, if there are any external investigations of or legal actions against a processor or its owners and operators during initial and ongoing due diligence of payment processors.

Financial institutions should act promptly to minimize possible consumer harm, particularly in cases involving potentially fraudulent or improper activities relating to activities of a payment processor or its merchant clients. Appropriate actions include filing a Suspicious Activity Report,⁴ requiring the payment processor to cease processing for a specific merchant, freezing certain deposit account balances to cover anticipated charge backs, and/or terminating the financial institution's relationship with the payment processor.

Risk Mitigation

Financial institutions should delineate clear lines of responsibility for controlling risks associated with payment processor relationships. Controls may include enhanced due diligence; effective underwriting; and increased scrutiny and monitoring of high-risk accounts for an increase in unauthorized returns, charge backs, suspicious activity, and/or consumer complaints. Implementing appropriate controls for payment processors and their merchant clients can help identify payment processors that process items for fraudulent telemarketers, online scammers, or other unscrupulous merchants and help ensure that the financial institution is not facilitating these transactions. Appropriate oversight and monitoring of these accounts may require the involvement of multiple departments, including information technology, operations, BSA/anti-money laundering (AML), and compliance.

Due Diligence and Underwriting

Financial institutions should implement policies and procedures designed to reduce the likelihood of establishing or maintaining inappropriate relationships with payment processors through which unscrupulous merchants can charge consumers. Such policies and procedures should outline the bank's thresholds for unauthorized returns, the possible actions that can be taken against payment processors that exceed these standards, and methods for periodically reporting such activities to the bank's board of directors and senior management.

As part of such policies and procedures, financial institutions should develop a processor approval program that extends beyond credit risk management. This program should include a due diligence and underwriting policy that, among other things, requires a background check of the payment processor, its principal owners, and its merchant clients. This will help validate the activities, creditworthiness, and business practices of the payment processor, as well as identify potential problem merchants. Payment processors may also process transactions for other

⁴ The U.S. Department of Treasury's Regulation 31 (CFR 103.18) requires that every federally supervised banking organization file a SAR when the institution detects a known or suspected violation of federal law. Part 353 of the FDIC's Rules and Regulations addresses SAR filing requirements and makes them applicable to all state-chartered financial institutions that are not members of the Federal Reserve System.

payment processors, resulting in nested payment processors or aggregator relationships. The financial institution should be aware of these activities and obtain data on the nested processor and its merchant clients. Nested processors and aggregator relationships pose additional challenges as they may be extremely difficult to monitor and control; therefore, risk to the institution is significantly elevated in these cases.

Controls and due diligence requirements should be robust for payment processors and their merchant clients. At a minimum, the policies and procedures should authenticate the processor's business operations and assess the entity's risk level. An assessment should include:

- Identifying the major lines of business and volume for the processor's customers;
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants;
- Reviewing corporate documentation, including independent reporting services and, if applicable, documentation on principal owners;
- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele;⁵
- Determining if the processor re-sells its services to a third party that may be referred to as an agent or provider of "Independent Sales Organization opportunities" or a "gateway arrangement"⁶ and whether due diligence procedures applied to those entities are sufficient;
- Visiting the processor's business operations center;
- Reviewing appropriate databases to ensure that the processor and its principal owners and operators have not been subject to law enforcement actions; and,
- Determining whether any conflicts of interest exist between management and insiders of the financial institution.

Financial institutions should require that payment processors provide information on their merchant clients, such as the merchant's name, principal business activity, location, and sales techniques. The same information should be obtained if the merchant uses sub-merchants (often

⁵ Businesses with elevated risk may include offshore companies, online gambling-related operations, and online payday lenders. Other businesses with elevated risks include credit repair schemes, debt consolidation and forgiveness, pharmaceutical sales, telemarketing entities, and online sale of tobacco products.

⁶ An Independent Sales Organization is an outside company contracted to procure new merchant relationships. Gateway arrangements are similar to Internet service providers that sell excess computer storage capacity to third parties, who in turn distribute computer services to other individuals unknown to the provider. The third party would make decisions about who would be receiving the service, although the provider would be responsible for the ultimate storage capacity.

called “affiliates”). Additionally, financial institutions should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business. Such verification could include comparing the identifying information with public record, fraud databases, and a trusted third party, such as a consumer reporting agency or consumer advocacy group, and/or checking references from other financial institutions. The financial institution should also obtain independent operational audits of the payment processor to assess the accuracy and reliability of the processor’s systems. The more the financial institution relies on the payment processor for due diligence and monitoring of its merchant client without direct financial institution involvement and verification, the more important it is to have an independent review to ensure that the processor’s controls are sufficient and that contractual agreements between the financial institution and the third-party payment processor are honored.

Ongoing Monitoring

Financial institutions that initiate transactions for payment processors should implement systems to monitor for higher rates of returns or charge backs and/or high levels of RCCs or ACH debits returned as unauthorized or due to insufficient funds, all of which often indicate fraudulent activity. This would include analyzing and monitoring the adequacy of any reserve balances or accounts established to continually cover charge-back activity.

Financial institutions are required to have a BSA/AML compliance program and appropriate policies, procedures, and processes for monitoring, detecting, and reporting suspicious activity. However, nonbank payment processors generally are not subject to BSA/AML regulatory requirements, and therefore some payment processors are more vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. The FFIEC BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk associated with third-party payment processors. As a result, a financial institution’s risk mitigation program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.

Even more so than high rates of returns, consumer complaints may indicate unauthorized or illegal activity. As such, financial institutions should establish procedures for regularly surveying the sources of consumer complaints that may be lodged with the payment processor, its merchant clients or their affiliates, or on publicly available complaint Web sites and/or blogs. This will help the institutions identify processors and merchants that may pose greater risk.

Similarly, financial institutions should have a formalized process for periodic audit of their third-party payment processing relationships, including reviewing merchant client lists and confirming that the processor is fulfilling contractual obligations to verify the legitimacy of its merchant clients and their business practices.

Conclusion

The FDIC recognizes that financial institutions provide legitimate services for payment processors and their merchant clients. However, to limit potential risks, financial institutions

should implement risk mitigation policies and procedures that include oversight and controls appropriate for the risk and transaction types of the payment processing activities. At a minimum, Board-approved policies and programs should assess the financial institution's risk tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, determine the character of the payment processor's ownership, and ensure ongoing monitoring of payment processor relationships for suspicious activity, among other things. Adequate routines and controls will include sufficient staffing with appropriate background and experience for managing third-party payment processing relationships of the size and scope present at the institution, as well as strong oversight and monitoring by the Board and senior management. Financial institutions should act promptly if they believe fraudulent or improper activities potentially resulting in consumer harm have occurred related to activities of a payment processor or its merchant clients, in accordance with their duties under BSA/AML policies and procedures, as well as under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts and practices.

Sandra L. Thompson
Director
Division of Risk Management Supervision

Mark Pearce
Director
Division of Depositor and Consumer Protection

From: Benardo, Michael B.
Sent: Thursday, December 22, 2011 11:20 AM
To: Valdez, Victor J.
Cc: Jackson, Michael L.; Butler, Janice; Weatherby, Kathryn M.; Sawin, April D.
Subject: RE: TPPP FIL Meeting with Chairman

Better late than never...



Final Revised TPPP
FIL (2011) ...

Here is the FIL with the language added to address the comments made by the Acting Chairman at his briefing. A footnote has been added to the first page of the guidance. It includes a list of the types of high risk merchants we are talking about.

DCP has approved this version to go forward to the 6th floor to see if this addresses the comments made

Please let me know if you have any questions.

Thank you.

Mike

From: Valdez, Victor J.
Sent: Wednesday, November 09, 2011 4:41 PM
To: Benardo, Michael B.
Cc: Jackson, Michael L.; Plunkett, Sylvia H.; Miller, Jonathan N.; Butler, Janice
Subject: TPPP FIL Meeting with Chairman

Mike,

I just spoke to Lorraine and, as of now, we are still on the calendar for briefing the Chairman on Mon. Lorraine does not have a copy of the proposed FIL. I believe the attached e-mail has the latest version of the FIL. Please let me know if this is correct? If so, I will send it to Lorraine as a read-ahead for Mon's meeting. If not, please send me that copy. Also, are there any other read-ahead material you want me to send?

Vic

<< Message: FW: Proposed Third Party Payments Guidance >>



Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-XX-2011
December XX, 2011

Payment Processor Relationships Revised Guidance

Summary: Attached is revised guidance describing potential risks associated with relationships with third-party entities that process payments for telemarketers, online businesses, and other merchants. These relationships pose increased risk to institutions and require careful due diligence and monitoring. This guidance outlines certain risk mitigation principles for this type of activity.

Statement of Applicability to Institutions with Total Assets under \$1 Billion: This guidance applies to all FDIC-supervised financial institutions that have relationships with third-party payment processors.

Distribution:

FDIC Supervised Institutions

Suggested Routing:

Chief Executive Officer
Executive Officers
Compliance Officer
Chief Information Officer
BSA Officer

Related Topics:

Guidance on Payment Processor Relationships (FIL 127 2008, November 2008)
Consumer Protection, Compliance Risk, and Risk Management
FDIC Guidance for Managing Third Party Risk (FIL 44 2008, June 2008)
FFIEC Handbook on Retail Payment Systems (February 2010)
FFIEC Handbook on Outsourcing Technology Services (June 2004)
FFIEC Bank Secrecy Act/Anti Money Laundering (BSA/AML)
Examination Manual (April 2010)
Managing Risks in Third Party Payment Processor Relationships
(Summer 2011 Supervisory Insights Journal)

Attachment:

Revised Guidance on Payment Processor Relationships

Contacts:

Kathryn Weatherby, Examination Specialist (Fraud), Division of Risk Management Supervision, at kweatherby@fdic.gov or (703) 254 0469

John Bowman, Review Examiner, Division of Depositor and Consumer Protection, at jbowman@fdic.gov or (202) 898 6574

Note:

FDIC Financial Institution Letters may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2011/index.html

To receive FILs electronically, please visit <http://www.fdic.gov/about/subscriptions/fil.html>
Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E 1002, Arlington, VA 22226 (877 275 3342 or 703 562 2200).

Highlights:

- Account relationships with entities processing payments for telemarketers or other potentially high-risk merchants require careful due diligence, close monitoring, and prudent underwriting.
- Account relationships with high-risk entities pose increased risks, including potentially unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act.
- Certain types of payment processors pose money laundering and fraud risks if merchant client identities are not verified and business practices are not reviewed.
- Financial institutions should assess risk tolerance in their overall risk assessment program and develop policies and procedures addressing due diligence, underwriting, and ongoing monitoring of high-risk payment processor relationships.
- Financial institutions should be alert to consumer complaints or unusual return rates that suggest the inappropriate use of personal account information and possible deception or unfair treatment of consumers.
- Financial institutions should act promptly when fraudulent or improper activities occur relating to a payment processor, including possibly terminating the relationship.
- Improperly managing these risks may result in the imposition of enforcement actions, such as civil money penalties or restitution orders.

Revised Guidance on Payment Processor Relationships

The FDIC has recently seen an increase in the number of relationships between financial institutions and payment processors in which the payment processor, who is a deposit customer of the financial institution, uses its relationship to process payments for third-party merchant clients. Payment processors typically process payments either by creating and depositing remotely created checks (RCCs) often referred to as “Demand Drafts” or by originating Automated Clearing House (ACH) debits on behalf of their merchant customers. The payment processor may use its own deposit account to process such transactions, or it may establish deposit accounts for its merchant clients.

While many payment processors effect legitimate payment transactions for reputable merchants, telemarketing and online merchants¹ have displayed a higher incidence of consumer fraud or potentially illegal activities. In the absence of an effective means for verifying their merchant clients’ identities and reviewing their business practices, payment processors pose elevated money laundering and fraud risk for financial institutions, as well as legal, reputational, and compliance risks if consumers are harmed.

Financial institutions should understand, verify, and monitor the activities and the entities related to the account relationship. Although all of the core elements of managing third-party risk should be considered in payment processor relationships (e.g., risk assessment, due diligence, and oversight), managing this risk poses an increased challenge for the financial institution when there may not be a direct customer relationship with the merchant. For example, it may be difficult to obtain necessary information from the payment processor, particularly if a merchant is also a payment processor, resulting in a “nested” payment processor or “aggregator” relationship.

Financial institutions should ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner. These agreements should also protect financial institutions by providing for immediate account closure, contract termination, or similar action, as well as establishing adequate reserve requirements to cover anticipated charge backs. Accordingly, financial institutions should perform due diligence and account monitoring appropriate to the risk posed by the payment processor and its merchant base. Risks associated with this type of activity are further increased if neither the payment processor nor the financial institution performs adequate due diligence on the merchants for which payments are originated. Financial institutions are reminded that they cannot rely solely on due diligence performed by the payment processor. The FDIC expects a financial institution to adequately oversee all transactions and activities that it processes and to appropriately manage and mitigate operational risks, Bank Secrecy Act (BSA) compliance, fraud risks, and consumer protection risks, among others.

¹ Examples of telemarketing and online merchants that have displayed a higher incidence of consumer fraud or potentially illegal activities noted by the FDIC include: credit repair services, gambling, government grant or will writing kits, pay day or sub-prime loans, pornography, tobacco or firearms sales, sweepstakes, and magazine subscriptions. This list is not all-inclusive. The risks presented by each relationship must be measured according to its own facts and circumstances. While some of these activities might be legitimate, financial institutions should be aware of the increased risks associated with payments to such merchants.

Potential Risks Arising from Payment Processor Relationships

Deposit relationships with payment processors expose financial institutions to risks not customarily present in relationships with other commercial customers. These include increased operational, strategic, credit, compliance, and transaction risks. In addition, financial institutions should consider the potential for legal, reputational, and other risks, including risks associated with a high or increasing number of customer complaints and returned items, and the potential for claims of unfair or deceptive practices. *Financial institutions that fail to adequately manage these relationships may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity and, thus, may be liable for such acts or practices.* In such cases, the financial institution and responsible individuals have been subject to a variety of enforcement and other actions. Financial institutions must recognize and understand the businesses and customers with which they have relationships and the liability risk for facilitating or aiding and abetting consumer unfairness or deception under Section 5 of the Federal Trade Commission Act.²

Financial institutions should be alert for payment processors that use more than one financial institution to process merchant client payments or that have a history of moving from one financial institution to another within a short period. Processors may use multiple financial institutions because they recognize that one or more of the relationships may be terminated as a result of suspicious activity.

Financial institutions should also be on alert for payment processors that solicit business relationships with troubled financial institutions in need of capital. In such cases, payment processors will identify and establish relationships with troubled financial institutions because these financial institutions may be more willing to engage in higher-risk transactions in exchange for increased fee income. In some cases, payment processors have also committed to purchasing stock in certain troubled financial institutions or have guaranteed to place a large deposit with the financial institution, thereby providing additional, much-needed capital. Often, the targeted financial institutions are smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

Financial institutions also should be alert to an increase in consumer complaints about payment processors and/or merchant clients or an increase in the amount of returns or chargebacks, all of which may suggest that the originating merchant may be engaged in unfair or deceptive practices or may be inappropriately obtaining or using consumers' personal account information to create unauthorized RCCs or ACH debits. Consumer complaints may be made to a variety of sources and not just directly to the financial institution. They may be sent to the payment processor or the underlying merchant, or directed to consumer advocacy groups or online complaint Web sites or blogs. Financial institutions should take reasonable steps to ensure they understand the type and level of complaints related to transactions that it processes. Financial institutions should also

² Under Section 8 of the Federal Deposit Insurance Act, the FDIC has authority to enforce the prohibitions against Unfair or Deceptive Acts or Practices (UDAP) in the Federal Trade Commission Act. UDAP violations can result in unsatisfactory Community Reinvestment Act ratings, compliance rating downgrades, restitution to consumers, and the pursuit of civil money penalties.

determine, to the extent possible, if there are any external investigations of or legal actions against a processor or its owners and operators during initial and ongoing due diligence of payment processors.

Financial institutions should act promptly to minimize possible consumer harm, particularly in cases involving potentially fraudulent or improper activities relating to activities of a payment processor or its merchant clients. Appropriate actions include filing a Suspicious Activity Report,³ requiring the payment processor to cease processing for a specific merchant, freezing certain deposit account balances to cover anticipated charge backs, and/or terminating the financial institution's relationship with the payment processor.

Risk Mitigation

Financial institutions should delineate clear lines of responsibility for controlling risks associated with payment processor relationships. Controls may include enhanced due diligence; effective underwriting; and increased scrutiny and monitoring of high-risk accounts for an increase in unauthorized returns, charge backs, suspicious activity, and/or consumer complaints.

Implementing appropriate controls for payment processors and their merchant clients can help identify payment processors that process items for fraudulent telemarketers, online scammers, or other unscrupulous merchants and help ensure that the financial institution is not facilitating these transactions. Appropriate oversight and monitoring of these accounts may require the involvement of multiple departments, including information technology, operations, BSA/anti-money laundering (AML), and compliance.

Due Diligence and Underwriting

Financial institutions should implement policies and procedures designed to reduce the likelihood of establishing or maintaining inappropriate relationships with payment processors through which unscrupulous merchants can charge consumers. Such policies and procedures should outline the bank's thresholds for unauthorized returns, the possible actions that can be taken against payment processors that exceed these standards, and methods for periodically reporting such activities to the bank's board of directors and senior management.

As part of such policies and procedures, financial institutions should develop a processor approval program that extends beyond credit risk management. This program should include a due diligence and underwriting policy that, among other things, requires a background check of the payment processor, its principal owners, and its merchant clients. This will help validate the activities, creditworthiness, and business practices of the payment processor, as well as identify potential problem merchants. Payment processors may also process transactions for other payment processors, resulting in nested payment processors or aggregator relationships. The financial institution should be aware of these activities and obtain data on the nested processor and its merchant clients. Nested processors and aggregator relationships pose additional

³ The U.S. Department of Treasury's Regulation 31 (CFR 103.18) requires that every federally supervised banking organization file a SAR when the institution detects a known or suspected violation of federal law. Part 353 of the FDIC's Rules and Regulations addresses SAR filing requirements and makes them applicable to all state-chartered financial institutions that are not members of the Federal Reserve System.

challenges as they may be extremely difficult to monitor and control; therefore, risk to the institution is significantly elevated in these cases.

Controls and due diligence requirements should be robust for payment processors and their merchant clients. At a minimum, the policies and procedures should authenticate the processor's business operations and assess the entity's risk level. An assessment should include:

- Identifying the major lines of business and volume for the processor's customers;
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants;
- Reviewing corporate documentation, including independent reporting services and, if applicable, documentation on principal owners;
- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele;⁴
- Determining if the processor re-sells its services to a third party that may be referred to as an agent or provider of "Independent Sales Organization opportunities" or a "gateway arrangement"⁵ and whether due diligence procedures applied to those entities are sufficient;
- Visiting the processor's business operations center;
- Reviewing appropriate databases to ensure that the processor and its principal owners and operators have not been subject to law enforcement actions; and,
- Determining whether any conflicts of interest exist between management and insiders of the financial institution.

Financial institutions should require that payment processors provide information on their merchant clients, such as the merchant's name, principal business activity, location, and sales techniques. The same information should be obtained if the merchant uses sub-merchants (often called "affiliates"). Additionally, financial institutions should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business. Such verification could include comparing the identifying information with

⁴ Businesses with elevated risk may include offshore companies, online gambling-related operations, and online payday lenders. Other businesses with elevated risks include credit repair schemes, debt consolidation and forgiveness, pharmaceutical sales, telemarketing entities, and online sale of tobacco products.

⁵ An Independent Sales Organization is an outside company contracted to procure new merchant relationships. Gateway arrangements are similar to Internet service providers that sell excess computer storage capacity to third parties, who in turn distribute computer services to other individuals unknown to the provider. The third party would make decisions about who would be receiving the service, although the provider would be responsible for the ultimate storage capacity.

public record, fraud databases, and a trusted third party, such as a consumer reporting agency or consumer advocacy group, and/or checking references from other financial institutions. The financial institution should also obtain independent operational audits of the payment processor to assess the accuracy and reliability of the processor's systems. The more the financial institution relies on the payment processor for due diligence and monitoring of its merchant client without direct financial institution involvement and verification, the more important it is to have an independent review to ensure that the processor's controls are sufficient and that contractual agreements between the financial institution and the third-party payment processor are honored.

Ongoing Monitoring

Financial institutions that initiate transactions for payment processors should implement systems to monitor for higher rates of returns or charge backs and/or high levels of RCCs or ACH debits returned as unauthorized or due to insufficient funds, all of which often indicate fraudulent activity. This would include analyzing and monitoring the adequacy of any reserve balances or accounts established to continually cover charge-back activity.

Financial institutions are required to have a BSA/AML compliance program and appropriate policies, procedures, and processes for monitoring, detecting, and reporting suspicious activity. However, nonbank payment processors generally are not subject to BSA/AML regulatory requirements, and therefore some payment processors are more vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. The FFIEC BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk associated with third-party payment processors. As a result, a financial institution's risk mitigation program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.

Even more so than high rates of returns, consumer complaints may indicate unauthorized or illegal activity. As such, financial institutions should establish procedures for regularly surveying the sources of consumer complaints that may be lodged with the payment processor, its merchant clients or their affiliates, or on publicly available complaint Web sites and/or blogs. This will help the institutions identify processors and merchants that may pose greater risk.

Similarly, financial institutions should have a formalized process for periodic audit of their third-party payment processing relationships, including reviewing merchant client lists and confirming that the processor is fulfilling contractual obligations to verify the legitimacy of its merchant clients and their business practices.

Conclusion

The FDIC recognizes that financial institutions provide legitimate services for payment processors and their merchant clients. However, to limit potential risks, financial institutions should implement risk mitigation policies and procedures that include oversight and controls appropriate for the risk and transaction types of the payment processing activities. At a minimum, Board-approved policies and programs should assess the financial institution's risk

tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, determine the character of the payment processor's ownership, and ensure ongoing monitoring of payment processor relationships for suspicious activity, among other things. Adequate routines and controls will include sufficient staffing with appropriate background and experience for managing third-party payment processing relationships of the size and scope present at the institution, as well as strong oversight and monitoring by the Board and senior management. Financial institutions should act promptly if they believe fraudulent or improper activities potentially resulting in consumer harm have occurred related to activities of a payment processor or its merchant clients, in accordance with their duties under BSA/AML policies and procedures, as well as under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts and practices.

Sandra L. Thompson
Director
Division of Risk Management Supervision

Mark Pearce
Director
Division of Depositor and Consumer Protection

From: Benardo, Michael B.
Sent: Tuesday, January 31, 2012 9:15 AM
To: Coleman, Frederick M.; Cooley, Corey L.; Drozdowski, Robert C.; Hahn, Richard K.; Henley, Kay E.; Hill, Victoria R.; Howe, Randall D.; Jay, J. Malcolm; Kahn, Lisa; Kopchik, Jeff; Kotsiras, John P.; Lacek, Charles A.; Lapin, Laura; Lataille, Michael S.; Lee, Robert D.; McElderry, Mark T.; Morris, Mark S.; Munnely, Jay; Nelson, David M.; Oxendine, Kiyana D.; Papierski, Mark R.; Spencer, Millie H.; Stabile, Debra L.; Templemon, Terrie; Tuzinski, Thomas J.; Weatherby, Kathryn M.
Cc: Lloyd, Edwin H.
Subject: FW: Third Party Payment Processors FIL

FYI.

From: Valdez, Victor J.
Sent: Tuesday, January 31, 2012 8:53 AM
To: Watkins, James C.; French, George; RDs; Frye, Daniel E.
Cc: Butler, Janice; Paul, Larry N.; Benardo, Michael B.; Lloyd, Edwin H.
Subject: Third Party Payment Processors FIL

All,
Morning. The Chairman has approved the release of the attached TPPP FIL. We will be sending it to OPA this morning.
Vic



TPPP FIL (2012)
FINAL, 2012-01...



Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-XX-2012
January 31, 2012

Payment Processor Relationships Revised Guidance

Summary: Attached is revised guidance describing potential risks associated with relationships with third-party entities that process payments for telemarketers, online businesses, and other merchants (collectively "merchants"). These relationships can pose increased risk to institutions and require careful due diligence and monitoring. This guidance outlines certain risk mitigation principles for this type of activity.

Statement of Applicability to Institutions with Total Assets under \$1 Billion: This guidance applies to all FDIC-supervised financial institutions that have relationships with third-party payment processors.

Distribution:

FDIC Supervised Institutions

Suggested Routing:

Chief Executive Officer
Executive Officers
Compliance Officer
Chief Information Officer
BSA Officer

Related Topics:

Guidance on Payment Processor Relationships (FIL 127 2008, November 2008)
Consumer Protection, Compliance Risk, and Risk Management
FDIC Guidance for Managing Third Party Risk (FIL 44 2008, June 2008)
FFIEC Handbook on Retail Payment Systems (February 2010)
FFIEC Handbook on Outsourcing Technology Services (June 2004)
FFIEC Bank Secrecy Act/Anti Money Laundering (BSA/AML)
Examination Manual (April 2010)
Managing Risks in Third Party Payment Processor Relationships
(Summer 2011 Supervisory Insights Journal)

Attachment:

Revised Guidance on Payment Processor Relationships

Contacts:

Kathryn Weatherby, Examination Specialist (Fraud), Division of Risk Management Supervision, at kweatherby@fdic.gov or (703) 254 0469

John Bowman, Review Examiner, Division of Depositor and Consumer Protection, at jbowman@fdic.gov or (202) 898 6574

Note:

FDIC Financial Institution Letters may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2012/index.html.

To receive FILs electronically, please visit <http://www.fdic.gov/about/subscriptions/fil.html>. Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E 1002, Arlington, VA 22226 (877 275 3342 or 703 562 2200).

Highlights:

- Account relationships with third-party entities that process payments for merchants require careful due diligence, close monitoring, and prudent underwriting.
- Account relationships with high-risk entities pose increased risks, including potentially unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act.
- Certain types of payment processors may pose heightened money laundering and fraud risks if merchant client identities are not verified and business practices are not reviewed.
- Financial institutions should assess risk tolerance in their overall risk assessment program and develop policies and procedures addressing due diligence, underwriting, and ongoing monitoring of high-risk payment processor relationships.
- Financial institutions should be alert to consumer complaints or unusual return rates that suggest the inappropriate use of personal account information and possible deception or unfair treatment of consumers.
- Financial institutions should act promptly when fraudulent or improper activities occur relating to a payment processor, including possibly terminating the relationship.
- Improperly managing these risks may result in the imposition of enforcement actions, such as civil money penalties or restitution orders.

Revised Guidance on Payment Processor Relationships

The FDIC has recently seen an increase in the number of relationships between financial institutions and payment processors in which the payment processor, who is a deposit customer of the financial institution, uses its relationship to process payments for third-party merchant clients. Payment processors typically process payments either by creating and depositing remotely created checks (RCCs) often referred to as “Demand Drafts” or by originating Automated Clearing House (ACH) debits on behalf of their merchant customers. The payment processor may use its own deposit account to process such transactions, or it may establish deposit accounts for its merchant clients.

While payment processors generally effect legitimate payment transactions for reputable merchants, the risk profile of such entities can vary significantly depending on the make-up of their customer base. For example, payment processors that deal with telemarketing and online merchants¹ may have a higher risk profile because such entities have tended to display a higher incidence of consumer fraud or potentially illegal activities than some other businesses. Given this variability of risk, payment processors must have effective processes for verifying their merchant clients’ identities and reviewing their business practices. Payment processors that do not have such processes can pose elevated money laundering and fraud risk for financial institutions, as well as legal, reputational, and compliance risks if consumers are harmed.

Financial institutions should understand, verify, and monitor the activities and the entities related to the account relationship. Although all of the core elements of managing third-party risk should be considered in payment processor relationships (e.g., risk assessment, due diligence, and oversight), managing this risk poses an increased challenge for the financial institution when there may not be a direct customer relationship with the merchant. For example, it may be difficult to obtain necessary information from the payment processor, particularly if a merchant is also a payment processor, resulting in a “nested” payment processor or “aggregator” relationship.

Financial institutions should ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner. These agreements should also protect financial institutions by providing for immediate account closure, contract termination, or similar action, as well as establishing adequate reserve requirements to cover anticipated charge backs. Accordingly, financial institutions should perform due diligence and account monitoring appropriate to the risk posed by the payment processor and its merchant

¹ Examples of telemarketing, online businesses, and other merchants that may have a higher incidence of consumer fraud or potentially illegal activities or may otherwise pose elevated risk include credit repair services, debt consolidation and forgiveness programs, online gambling-related operations, government grant or will-writing kits, payday or subprime loans, pornography, online tobacco or firearms sales, pharmaceutical sales, sweepstakes, and magazine subscriptions. This list is not all-inclusive. -

base. Risks associated with this type of activity are further increased if neither the payment processor nor the financial institution performs adequate due diligence on the merchants for which payments are originated. Financial institutions are reminded that they cannot rely solely on due diligence performed by the payment processor. The FDIC expects a financial institution to adequately oversee all transactions and activities that it processes and to appropriately manage and mitigate operational risks, Bank Secrecy Act (BSA) compliance, fraud risks, and consumer protection risks, among others.

Potential Risks Arising from Payment Processor Relationships

Deposit relationships with payment processors expose financial institutions to risks not customarily present in relationships with other commercial customers. These include increased operational, strategic, credit, compliance, and transaction risks. In addition, financial institutions should consider the potential for legal, reputational, and other risks, including risks associated with a high or increasing number of customer complaints and returned items, and the potential for claims of unfair or deceptive practices. *Financial institutions that fail to adequately manage these relationships may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity and, thus, may be liable for such acts or practices.* In such cases, the financial institution and responsible individuals have been subject to a variety of enforcement and other actions. Financial institutions must recognize and understand the businesses and customers with which they have relationships and the liability risk for facilitating or aiding and abetting consumer unfairness or deception under Section 5 of the Federal Trade Commission Act.²

Financial institutions should be alert for payment processors that use more than one financial institution to process merchant client payments or that have a history of moving from one financial institution to another within a short period. Processors may use multiple financial institutions because they recognize that one or more of the relationships may be terminated as a result of suspicious activity.

Financial institutions should also be on alert for payment processors that solicit business relationships with troubled financial institutions in need of capital. In such cases, payment processors will identify and establish relationships with troubled financial institutions because these financial institutions may be more willing to engage in higher-risk transactions in exchange for increased fee income. In some cases, payment processors have also committed to purchasing stock in certain troubled financial institutions or have guaranteed to place a large deposit with the financial institution, thereby providing additional, much-needed capital. Often, the targeted financial institutions are smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

² Under Section 8 of the Federal Deposit Insurance Act, the FDIC has authority to enforce the prohibitions against Unfair or Deceptive Acts or Practices (UDAP) in the Federal Trade Commission Act. UDAP violations can result in unsatisfactory Community Reinvestment Act ratings, compliance rating downgrades, restitution to consumers, and the pursuit of civil money penalties.

Financial institutions also should be alert to an increase in consumer complaints about payment processors and/or merchant clients or an increase in the amount of returns or charge backs, all of which may suggest that the originating merchant may be engaged in unfair or deceptive practices or may be inappropriately obtaining or using consumers' personal account information to create unauthorized RCCs or ACH debits. Consumer complaints may be made to a variety of sources and not just directly to the financial institution. They may be sent to the payment processor or the underlying merchant, or directed to consumer advocacy groups or online complaint Web sites or blogs. Financial institutions should take reasonable steps to ensure they understand the type and level of complaints related to transactions that it processes. Financial institutions should also determine, to the extent possible, if there are any external investigations of or legal actions against a processor or its owners and operators during initial and ongoing due diligence of payment processors.

Financial institutions should act promptly to minimize possible consumer harm, particularly in cases involving potentially fraudulent or improper activities relating to activities of a payment processor or its merchant clients. Appropriate actions include filing a Suspicious Activity Report,³ requiring the payment processor to cease processing for a specific merchant, freezing certain deposit account balances to cover anticipated charge backs, and/or terminating the financial institution's relationship with the payment processor.

Risk Mitigation

Financial institutions should delineate clear lines of responsibility for controlling risks associated with payment processor relationships. Controls may include enhanced due diligence; effective underwriting; and increased scrutiny and monitoring of high-risk accounts for an increase in unauthorized returns, charge backs, suspicious activity, and/or consumer complaints.

Implementing appropriate controls for payment processors and their merchant clients can help identify payment processors that process items for fraudulent telemarketers, online scammers, or other unscrupulous merchants and help ensure that the financial institution is not facilitating these transactions. Appropriate oversight and monitoring of these accounts may require the involvement of multiple departments, including information technology, operations, BSA/anti-money laundering (AML), and compliance.

Due Diligence and Underwriting

Financial institutions should implement policies and procedures designed to reduce the likelihood of establishing or maintaining inappropriate relationships with payment processors used by unscrupulous merchants. Such policies and procedures should outline the bank's thresholds for unauthorized returns, the possible actions that can be taken against payment processors that exceed these standards, and methods for periodically reporting such activities to the bank's board of directors and senior management.

³ The U.S. Department of Treasury's Regulation 31 (CFR 103.18) requires that every federally supervised banking organization file a SAR when the institution detects a known or suspected violation of federal law. Part 353 of the FDIC's Rules and Regulations addresses SAR filing requirements and makes them applicable to all state-chartered financial institutions that are not members of the Federal Reserve System.

As part of such policies and procedures, financial institutions should develop a processor approval program that extends beyond credit risk management. This program should include a due diligence and underwriting policy that, among other things, requires a background check of the payment processor, its principal owners, and its merchant clients. This will help validate the activities, creditworthiness, and business practices of the payment processor, as well as identify potential problem merchants. Payment processors may also process transactions for other payment processors, resulting in nested payment processors or aggregator relationships. The financial institution should be aware of these activities and obtain data on the nested processor and its merchant clients. Nested processors and aggregator relationships pose additional challenges as they may be extremely difficult to monitor and control; therefore, risk to the institution is significantly elevated in these cases.

Controls and due diligence requirements should be robust for payment processors and their merchant clients. At a minimum, the policies and procedures should authenticate the processor's business operations and assess the entity's risk level. An assessment should include:

- Identifying the major lines of business and volume for the processor's customers;
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants;
- Reviewing corporate documentation, including independent reporting services and, if applicable, documentation on principal owners;
- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele;⁴
- Determining if the processor re-sells its services to a third party that may be referred to as an agent or provider of "Independent Sales Organization opportunities" or a "gateway arrangement"⁵ and whether due diligence procedures applied to those entities are sufficient;
- Visiting the processor's business operations center;
- Reviewing appropriate databases to ensure that the processor and its principal owners and operators have not been subject to law enforcement actions; and,
- Determining whether any conflicts of interest exist between management and insiders of the financial institution.

⁴ See footnote 1 for examples of potentially high-risk areas.

⁵ An Independent Sales Organization is an outside company contracted to procure new merchant relationships. Gateway arrangements are similar to Internet service providers that sell excess computer storage capacity to third parties, who in turn distribute computer services to other individuals unknown to the provider. The third party would make decisions about who would be receiving the service, although the provider would be responsible for the ultimate storage capacity.

Financial institutions should require that payment processors provide information on their merchant clients, such as the merchant's name, principal business activity, location, and sales techniques. The same information should be obtained if the merchant uses sub-merchants (often called "affiliates"). Additionally, financial institutions should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business. Such verification could include comparing the identifying information with public record, fraud databases, and a trusted third party, such as a consumer reporting agency or consumer advocacy group, and/or checking references from other financial institutions. The financial institution should also obtain independent operational audits of the payment processor to assess the accuracy and reliability of the processor's systems. The more the financial institution relies on the payment processor for due diligence and monitoring of its merchant client without direct financial institution involvement and verification, the more important it is to have an independent review to ensure that the processor's controls are sufficient and that contractual agreements between the financial institution and the third-party payment processor are honored.

Ongoing Monitoring

Financial institutions that initiate transactions for payment processors should implement systems to monitor for higher rates of returns or charge backs and/or high levels of RCCs or ACH debits returned as unauthorized or due to insufficient funds, all of which often indicate fraudulent activity. This would include analyzing and monitoring the adequacy of any reserve balances or accounts established to continually cover charge-back activity.

Financial institutions are required to have a BSA/AML compliance program and appropriate policies, procedures, and processes for monitoring, detecting, and reporting suspicious activity. However, nonbank payment processors generally are not subject to BSA/AML regulatory requirements, and therefore some payment processors are more vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. The FFIEC BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk associated with third-party payment processors. As a result, a financial institution's risk mitigation program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.

Consumer complaints and/or high rates of return may be an indicator of unauthorized or illegal activity. As such, financial institutions should establish procedures for regularly surveying the sources of consumer complaints that may be lodged with the payment processor, its merchant clients or their affiliates, or on publicly available complaint Web sites and/or blogs. This will help the institutions identify processors and merchants that may pose greater risk.

Similarly, financial institutions should have a formalized process for periodically auditing their third-party payment processing relationships; including reviewing merchant client lists and confirming that the processor is fulfilling contractual obligations to verify the legitimacy of its merchant clients and their business practices.

Conclusion

The FDIC recognizes that financial institutions provide legitimate services for payment processors and their merchant clients. However, to limit potential risks, financial institutions should implement risk mitigation policies and procedures that include oversight and controls appropriate for the risk and transaction types of the payment processing activities. At a minimum, Board-approved policies and programs should assess the financial institution's risk tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, determine the character of the payment processor's ownership, and ensure ongoing monitoring of payment processor relationships for suspicious activity, among other things. Adequate routines and controls will include sufficient staffing with the appropriate background and experience for managing third-party payment processing relationships of the size and scope present at the institution, as well as strong oversight and monitoring by the board and senior management. Financial institutions should act promptly if they believe fraudulent or improper activities potentially resulting in consumer harm have occurred related to activities of a payment processor or its merchant clients, in accordance with their duties under BSA/AML policies and procedures, as well as under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts and practices.

Sandra L. Thompson
Director
Division of Risk Management Supervision

Mark Pearce
Director
Division of Depositor and Consumer Protection

From: Benardo, Michael B. [REDACTED]
Sent: Monday, April 18, 2011 5:28 PM
To: Pearce, Mark (DCP); Plunkett, Sylvia H.; Miller, Jonathan N.; Brown, Luke H.
Cc: Hartigan, Frank A.; Wirtz, Robert J.; Bowman, John B.; Jackwood, John M.
Subject: [REDACTED] Initial Summary of E Payment Concerns
Attachments: TPPP Article v4 - clean.docx

All---

Attached please find the latest version of the Supervisory Insight (SI) Journal article on Risks Associated with Third Party Payment Processors (TPPP). Please keep in mind that it is not yet finalized. It still needs to receive final approval by George French, and the other Deputies, RDs and the 6th floor. The schedule for this issue of SI is to publish the issue by the end of June.

The TPPP working will next analyze the outstanding guidance to determine what, if any, updates are needed. This, along with a RAC call, should be accomplished by the end of May.

Please let me know if you have any questions.

Thank you,

Mike

Michael B. Benardo
Chief, Cyber-Fraud and Financial Crimes Section
Division of Risk Management Supervision

From: Hartigan, Frank A.
Sent: Sunday, April 17, 2011 9:42 AM
To: Benardo, Michael B.; Bowman, John B.; Jackwood, John M.; Wirtz, Robert J.
Cc: Miller, Jonathan N.; Brown, Luke H.
Subject: [REDACTED] Initial Summary of E-Payment Concerns

Hi all -

See Mark Pearce's comments about Third Party Payment Processors.

Mike Benardo can you send the Supervisory Insight Journal to Mark, Sylvia, Jonathan, and Luke? Also, please provide an update on the group's efforts on the FIL, examiner guidance and RAC call.

Thanks.

Frank

From: Hartigan, Frank A.
Sent: Sunday, April 17, 2011 09:37 AM
To: Pearce, Mark (DCP); Plunkett, Sylvia H.
Subject: [REDACTED] Initial Summary of E-Payment Concerns

Step one is the article for the Supervisory Insight Journal which goes out to bankers and examiners. I'll have Mike Benardo send the version which is ready for production.

Step two is a Financial Institution Letter which should be easy to prepare now that the article is draft. We'll push to get a draft by the end of the month.

Other steps are more guidance for examiners followed by a RAC call.

The companies are out there - they've already proliferated. Our challenges is to identify them and effectively deal with them. Our supervisory strategy needs more work. So far we've done only Orders but no CMP or restitution for harmed consumers. In San Francisco we wanted to do more but didn't get the support we needed. Legal was a major obstacle. OCC has had 2 public cases with Orders, CMP and restitution.

From: Pearce, Mark (DCP)
Sent: Sunday, April 17, 2011 07:39 AM
To: Hartigan, Frank A.; Plunkett, Sylvia H.
Subject: **Redacted** Initial Summary of E Payment Concerns

Where are we on our next steps list for these TPPPs? I am worried about the proliferation of these issues.
m.

This material has been redacted as non-responsive.

Managing Risks in Third-Party Payment Processor Relationships

During the past few years, the Federal Deposit Insurance Corporation (FDIC) has observed an increase in the number of deposit relationships between financial institutions and third-party payment processors and a corresponding increase in the risks associated with these relationships. Deposit relationships with payment processors can expose financial institutions to risks not present in typical commercial customer relationships, including greater strategic, credit, compliance, transaction, legal, and reputation risk. It was for this reason in 2008 that the FDIC issued *Guidance on Payment Processor Relationships* which outlines risk mitigation principles for this type of higher-risk activity.¹

Although many payment processors effect legitimate payment transactions for a variety of reputable merchants, an increasing number of processors have been initiating payments for abusive telemarketers, deceptive online merchants, and organizations that engage in high risk or illegal activities. In the absence of adequate monitoring systems and controls, a financial institution could be facilitating unauthorized transactions and, ultimately, unfair and deceptive practices resulting in financial harm to the consumer. Therefore, it is essential that financial institutions and examiners recognize and understand the risks associated with these relationships.

This article explains the role of third-party payment processors and the risks they can present to financial institutions, identifies warning signs that may indicate heightened risk in a payment processor relationship, and discusses the risk mitigation controls that should be in place

¹Financial Institution Letter (FIL) 127-2008. *Guidance on Payment Processor Relationships*, dated November 7, 2008. See: <http://www.fdic.gov/news/news/financial/2008/fil08127.html>

to manage this risk. The article concludes with an overview of supervisory remedies that may be used when it is determined that a financial institution does not have an adequate program in place for monitoring and addressing the risks associated with third-party payment processor relationships.

Background

The core elements of managing third-party risk are present in payment processor relationships (e.g., risk assessment, policies and procedures, due diligence, and oversight). However, managing these risks can be particularly challenging as the financial institution does not have a direct customer relationship with the payment processor's merchant clients. Furthermore, the risks associated with this type of activity are heightened when neither the payment processor nor the financial institution performs adequate due diligence, such as verifying the identities and business practices of the merchants for which payments are originated and implementing a program of ongoing monitoring for suspicious activity.

For example, in a typical third-party payment processor relationship, the payment processor is a deposit customer of the financial institution which uses its deposit account to process payments for its merchant clients. The payment processor receives lists of payments to be generated by the merchant clients for the payment of goods or services and initiates the payments by creating and depositing them into a transaction account at a financial institution. In some cases, the payment processor may establish individual accounts at the financial institution in the name of each merchant client and deposit the appropriate payments into these accounts. The merchant may then be a co-owner of the deposit account and make withdrawals from the

account to receive its sales proceeds, or the payment processor may periodically forward the sales proceeds from the account to the merchant. Alternatively, the payment processor may commingle payments originated by the merchant clients into a single deposit account in the name of the payment processor. In this case, the payment processor should maintain records to allocate the deposit account balance among the merchant clients.

Payment Types Used by Third-Party Payment Processors

Payment processors may offer merchants a variety of alternatives for accepting payments including credit and debit card transactions, traditional check acceptance, Automated Clearing House (ACH) debits and other alternative payment channels. The potential for misuse or fraud exists in all payment channels. However, the FDIC has observed that some of the most problematic activity occurs when originating ACH debits or creating and depositing remotely created checks.

Automated Clearing House Debits

The ACH network is a nationwide electronic payment network which enables participating financial institutions to distribute electronic credit and debit entries to bank accounts and settle these entries.

Common ACH credit transfers include the direct deposit of payroll and certain benefits payments. Direct debit transfers also may be made through the ACH network and include consumer payments for insurance premiums, mortgage loans, and other types of bills. Rules and regulations governing the ACH networks are established by NACHA - The Electronic Payments

Association (formerly National Automated Clearing House Association)² and the Board of Governors of the Federal Reserve.

Third-party payment processors initiate ACH debit transfers as payments for merchant clients by submitting these transfers, which contain the consumer's financial institution routing number and account number (found at the bottom of a check) to their financial institution to enter into the ACH networks. Telemarketers and online merchants obtain this information from the consumer and transmit it to the payment processor to initiate the ACH debit transfers. The risk of fraud arises when an illicit telemarketer or online merchant obtains the consumer's account information through coercion or deception and initiates an ACH debit transfer that may not be fully understood or authorized by the consumer.

As with all payment systems and mechanisms, the financial institution bears the responsibility of implementing an effective system of internal controls and ongoing account monitoring for the detection and resolution of fraudulent ACH transfers. If an unauthorized ACH debit is posted to a consumer's account, the procedures for resolving errors contained in the Federal Reserve Board's Regulation E, which governs electronic funds transfers,³ provide the consumer 60 days after the financial institution sends an account statement to report the unauthorized ACH debit.⁴ Regulation E requires the consumer's financial institution to investigate the matter and report to the consumer the results of the investigation within a

² NACHA establishes the rules and procedures governing the exchange of automated clearinghouse payments. See http://www.nacha.org/c_achrules.cfm.

³ Provisions of the Federal Reserve Board's Regulation E establish the rights, liabilities, and responsibilities of participants in electronic fund transfer systems, such as automated teller machine transfers, telephone bill-payment services, point-of-sale terminal transfers, and preauthorized transfers from or to a consumer's account.

⁴ 12 CFR Section 205.11

prescribed time frame. In the case of an ACH debit, when a consumer receives a refund for an unauthorized debit, ACH rules permit the consumer's financial institution to recover the amount of the unauthorized payment by returning the debit item to the originating financial institution.

Remotely Created Checks

Remotely Created Checks (RCCs), often referred to as “demand drafts,” are payment instruments that do not bear the signature of a person on whose account it is drawn. In place of the signature, the RCC bears the account holder's printed or typed name, or a statement that the account holder's signature is not required or the account holder has authorized the issuance of the check. Similar to the initiation of an ACH debit transfer, an account holder authorizes the creation of an RCC by providing his financial institution's routing number and his account number. Examples of RCCs are those created by a credit card or utility company to make a payment on an account, or those initiated by telemarketers or online merchants to purchase goods or services.

The risk of fraud associated with RCCs is often greater than the risk associated with other kinds of debits that post to transaction accounts. For example, an illicit payment originator might obtain a consumer's account information by copying it from an authorized check or misleading the consumer into providing the information over the telephone or the Internet. Once the necessary information is obtained, the payment originator can generate unauthorized RCCs and forward them for processing. Similar to the responsibilities associated with the ACH network, the financial institution should implement an effective system of internal controls and account monitoring to identify and resolve the unauthorized RCC. However, because RCCs are

cleared in the same manner as traditional checks, there is no way to differentiate between the two and, therefore, no efficient way to measure the volume or use of RCCs.

RCCs may be processed as a paper item through the customary clearing networks or converted to and processed as an ACH debit. However, check clearing and ACH rules differ as to the re-crediting of an accountholder for an unauthorized RCC and how losses are allocated by and between the participating financial institutions. RCCs processed as checks are governed by provisions of the Uniform Commercial Code (UCC) and the Expedited Funds Availability Act,⁵ as implemented by Regulation CC. RCCs converted to ACH debits are governed by applicable ACH rules, the Electronic Fund Transfer Act, and Regulation E.

In response to heightened concern about the risk of fraud, in 2005 the Board of Governors of the Federal Reserve amended Regulation CC to transfer the liability for losses resulting from unauthorized RCCs.⁶ At the same time, the Board also amended Regulation J (the Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire) to clarify that certain warranties, similar to those provided under the UCC, apply to RCCs collected through the Reserve Banks. In conjunction with Regulation CC, the amendments to Regulation J shifted the liability for losses attributed to unauthorized RCCs to the financial institution where the check is first deposited as this institution is in the best position to know its customer (the creator of the RCC) and determine the legitimacy of the deposits. The liability also creates an economic incentive for depository institutions to perform enhanced due

⁵ The Expedited Funds Availability Act (EFAA) enacted in 1987, addresses the issue of delayed availability of funds by banks. The EFAA requires banks to (1) make funds deposited in transaction accounts available to customers within specified time frames, (2) pay interest on interest-bearing transaction accounts not later than the day the bank receives credit, and (3) disclose funds-availability policies to customers.

⁶ Effective July 1, 2006 [70 Fed. Reg. 71218-71226 (November 28, 2005)]

diligence on those customers depositing RCCs. Furthermore, by providing the paying financial institution with the ability to recover against the financial institution presenting the unauthorized RCC, it should make it easier for customers to obtain re-credits.⁷

Types of High Risk Payments

Although many clients of payment processors are reputable merchants, an increasing number are not and should be considered “high risk.” These disreputable merchants use payment processors to charge consumers for questionable or fraudulent goods and services. Often a disreputable merchant will engage in high pressure and deceptive sales tactics, such as aggressive telemarketing or enticing and misleading pop-up advertisements on Web sites. For example, consumers should be cautious when Web sites offer “free” information and ask consumers to provide payment information to cover a small shipping and handling fee. In some instances and without proper disclosure, consumers who agreed to pay these fees, often found their bank accounts debited for more than the fee and enrolled in costly plans without their full understanding and consent.⁸ Still other disreputable merchants will use processors to initiate payments for the sale of products and services, including, but not limited to, unlawful Internet gambling and the illegal sale of tobacco products on the Internet.

Generally, high-risk transactions occur when the consumer does not have a familiarity with the merchant, or when the quality of the goods and services being sold is uncertain.

Activities involving purchases made over the telephone or on the Internet tend to be riskier in

⁷ Changes to Federal Reserve Bank Operating Circular No. 3 on the Collection of Cash Items and Returned Checks clarifies that electronically created images (including RCC items) that were not originally captured from paper are not eligible to be processed as Check 21 items (effective July 15, 2008). www.frb-services.org/files/regulations.pdf#operating_circular_3.pdf.

⁸ Rules governing the use of telemarketing require verifiable authorization of payment for services. See the Federal Trade Commission Telemarketing Sales Rule [16 CFR 310]. See: <http://www.ftc.gov/os/2002/12/Asi-finalrule.pdf>.

that the consumer cannot fully examine or evaluate the product or service purchased. Similarly, the consumer may not be able to verify the identity or legitimacy of the person or organization making the sale.

Some merchant categories that have been associated with high-risk activity include, but are not limited to:

- Ammunition Sales
- Cable Box de-scramblers
- Coin Dealers
- Credit Card Schemes
- Credit Repair Services
- Dating Services
- Debt Consolidation Scams
- Drug Paraphernalia
- Escort Services
- Firearms Sales
- Fireworks Sales
- Gambling
- Get Rich Products
- Government Grants
- Home-Based Charities
- Life Time Guarantees
- Life Time Memberships
- Lottery Sales
- Mailing Lists/Personal Info
- Money Transfer Networks
- Pyramid Type Sales
- PayDay Loans
- Pharmaceutical Sales
- Pornography
- Ponzi Schemes
- Racist materials
- Surveillance equipment
- Telemarketing
- Tobacco Sales
- Travel clubs

Of particular concern, the FDIC and other federal regulators have seen an increase in payment processors initiating payment for online gaming activities that may be illegal. The

Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) prohibits financial institutions from accepting payments from any person engaged in the business of betting or wagering with a business in unlawful Internet gambling (see the FDIC's Financial Institution Letter on the *Unlawful Internet Gambling Enforcement Act*, FIL-35-2010, dated June 30, 2010).⁹

High-Risk Payment Processor Relationship Warning Signs

Financial institutions and examiners should be aware of the warning signs that may indicate heightened risk in a payment processor relationship. One of the more telling is a high volume of consumer complaints that suggest a merchant client is inappropriately obtaining personal account information; misleading customers as to the quality, effectiveness, and usefulness of the goods or services being offered; or misstating the sales price or charging additional, and sometimes recurring, fees that are not accurately disclosed or properly authorized during the sales transaction. However, this may be somewhat difficult to determine in that it may be almost impossible for financial institutions and examiners to know if consumers are submitting complaints directly to the payment processor or the merchants. One way that financial institutions and examiners can determine if consumers are making complaints or voicing their dissatisfaction is to review certain Web sites, such as those for regional Better Business Bureaus, or blogs intended to collect and share such information to alert other consumers.

Financial institutions with third-party payment processor relationships should consider monitoring the Internet for complaints that mention them by name. The financial institution's

⁹ 12 CFR Part 233 Regulation GG, Financial Institution Letter (FIL) 35-2010. *Unlawful Internet Gambling Enforcement Act*, dated June 30, 2010. See <http://www.fdic.gov/news/news/financial/2010/fil10035.html>

name typically appears on the face of a RCC or in the record of an ACH debit. As a result, consumers often associate the financial institution with the transaction and may complain about the institution facilitating the payment. Complaints also may be lodged with the depository financial institution by the financial institution of the consumer whose account was charged. As required by statute and federal regulation, the depository financial institution must acknowledge, research, and respond to each complaint made directly to them.

Another indication of the potential for heightened risk in a payment processor relationship is a large number of returns or charge backs. Consumers who are dissatisfied with goods or services delivered or provided, or consumers who feel they were deceived or coerced into providing their account information, can request their financial institution return the RCC or ACH debit to the depository financial institution as an unauthorized transaction. In addition, items may be returned if insufficient funds are available to cover the unauthorized items, resulting in the consumer's account being overdrawn. In these circumstances, the items often are returned as "NSF" rather than as "unauthorized." Accordingly, financial institutions with payment processor relationships should implement systems to monitor for higher rates of returns or charge backs, which can be evidence of fraudulent activity.

Another warning sign is a significant amount of activity which generates a higher than normal level of fee income. In an increasingly competitive market place, financial institutions are looking for ways to grow non-interest fee income, and this is especially true for troubled institutions. Although fee income from third-party payment processor relationships may benefit an institution's bottom line, it can indicate an increased level of risk. Side agreements may be

established between payment processors and financial institutions, whereby the payment processor pays the institution a fee for each item deposited, generating a higher level of fee income. However, the greatest source of income from these relationships tends to be returned item fees. Financial institutions routinely charge deposit customers a fee for each returned item. Because payment processors may generate a high volume of returned items, the fee income associated with this activity is typically much higher.

As a caveat, financial institutions and examiners should be alert for payment processors that use more than one financial institution to process merchant client payments, or nested arrangements where a payment processor's merchant client is also doing third-party payment processing. Spreading the activity among several institutions may allow processors that engage in inappropriate activity to avoid detection. For example, a single institution may not detect high levels of returned items if they are spread among several financial institutions. Payment processors also may use multiple financial institutions in case one or more of the relationships is terminated as a result of suspicious activity.

Finally, another troubling development is payment processors that purposefully solicit business relationships with troubled institutions in need of capital. Payment processors identify and establish relationships with troubled institutions as these institutions may be more willing to engage in higher-risk transactions in return for increased fee income. In some cases, payment processors have made a commitment to purchase stock in certain troubled financial institutions or guarantee to retain a large deposit with the institution, thereby providing additional, needed

capital. Often, the targeted financial institutions are smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

Risk Controls

A framework for prudently managing relationships with third-party payment processors was communicated in the FDIC's 2008 *Guidance on Payment Processor Relationships*.¹⁰ Financial institutions in relationships with payment processors should establish clear lines of responsibility for controlling the associated risks. Such responsibilities include effective due diligence and underwriting, as well as ongoing monitoring of high-risk accounts for an increase in unauthorized returns and suspicious activity and maintenance of adequate balances or reserves to cover expected high levels of returned items. The relationship should be governed by a written contract between the financial institution and the third-party payment processor which outlines each party's duties and responsibilities. Implementing appropriate and effective controls over payment processors and their merchant clients will help identify those processors working with fraudulent telemarketers or other unscrupulous merchants and help ensure the financial institution does not facilitate such transactions.

Due Diligence and Underwriting

Due diligence and prudent underwriting standards are critical components of a risk mitigation program. Financial institutions should implement policies and procedures that reduce the likelihood of establishing or maintaining a relationship with payment processors through which unscrupulous merchants can access customers' deposit accounts.

¹⁰ Financial Institution Letter (FIL) 127-2008, *Guidance on Payment Processor Relationships*. November 7, 2008. <http://www.fdic.gov/news/news/financial/2008/fil08127.html>

Financial institutions that initiate transactions for payment processors should develop a processor approval program that extends beyond credit risk management. This program should incorporate an effective due diligence and underwriting policy that, among other things, requires background checks of payment processors and merchant clients. A processor approval program will help validate the activities, creditworthiness, and business practices of the payment processor and should, at a minimum, authenticate the processor's business operations and assess the entity's risk level. Any processor assessment should include:

- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele.
- Determining if the processor re-sells its services to "Independent Sales Organizations" (a company contracted to procure new merchant relationships) or through "gateway arrangements" (selling excess capacity to third parties, which in turn sell services to other individuals unknown to the payment processor).
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants.
- Identifying the major lines of business and volume for the processor's customers.

- Maintaining appropriate balances or reserves for each individual merchant based on the type of client and the risk involved in the transactions processed and the expected volume of returned items.

- Reviewing corporate documentation, obtaining information on the processor from independent reporting services and, if applicable, documentation on principal owners.

- Visiting the processor's business operations center.

- Requesting copies of consumer complaints and the procedures for handling consumer complaints and redress.

- Information pertaining to any litigation, and actions brought by federal, state, or local regulatory or enforcement agencies.

- Information about the history of returned items and customer refunds.

Financial institutions should require the payment processor to provide information on its merchant clients, such as the merchant's name, principal business activity, geographic location, and sales techniques. Additionally, financial institutions should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business. Such verification could include comparing the identifying information with public record, fraud databases and a trusted third party, such as a credit report from a consumer

reporting agency or the state Better Business Bureau, or checking references from other financial institutions.

Ongoing Monitoring

Financial institutions are required to have a Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program and appropriate policies, procedures, and processes in place for monitoring, detecting, and reporting suspicious activity.¹¹ However, non-bank payment processors generally are not subject to BSA/AML regulatory requirements and, therefore, some payment processors may be vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. The Federal Financial Institutions Examination Council BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk with respect to third-party payment processors. As a result, a financial institution's risk mitigation program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.¹²

Appropriate Supervisory Responses

In those instances where examiners determine that a financial institution fails to have an adequate program in place to monitor and address risks associated with third-party payment processor relationships, formal or informal enforcement actions may be appropriate. Formal actions have included Cease and Desist Orders under Section 8(b) or 8(c) of the *Federal Deposit*

¹¹ Banks, bank holding companies, and their subsidiaries are required by federal regulations to file a Suspicious Activity Report if they know, suspect, or have reason to suspect the transaction may involve potential money laundering or other illegal activity: is designed to evade the Bank Secrecy Act or its implementing regulations; has no business or apparent lawful purpose; or is not the type of transaction in which particular customer would normally be expected to engage. See 12 CFR 353 (http://www.ffiec.gov/bsa_aml_infobase/pages_manual/regulations/12CFR353.htm) and 31 CFR 103.18 (http://www.ffiec.gov/bsa_aml_infobase/pages_manual/regulations/31CFR103.pdf).

¹² See: "Third Party Payment Processors - Overview," from the Bank Secrecy Act/Anti Money Laundering Examination Manual. http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm

Insurance (FDI) Act, as well as assessment of Civil Money Penalties under Section 8(i) of the FDI Act. These orders have required the financial institution to immediately terminate the high risk relationship and establish reserves or funds on deposit to cover anticipated charge backs.

As appropriate, the examiner will determine if financial institution management has knowledge that the payment processor or the merchant clients are engaging in unfair and deceptive practices in violation of Section 5 of the Federal Trade Commission Act. In those cases where a financial institution does not conduct due diligence, accepts a heightened level of risk, and allows transactions for high-risk merchants to pass through it, it may be determined that the financial institution is aiding and abetting the merchants. This also could indicate a disregard for the potential for financial harm to consumers and, as a result, the financial institution may be subject to civil money penalties or required to provide restitution.

Conclusion

Deposit relationships with payment processors expose financial institutions to risks that may not be present in relationships with other commercial customers. To limit potential risks, financial institutions should implement risk mitigation policies and procedures that include appropriate oversight and controls commensurate with the risk and complexity of the activities. At a minimum, risk mitigation programs should provide that the financial institution assess its risk tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, and monitor payment processor relationships for suspicious activity.

Financial institutions should act promptly if they believe fraudulent or improper activities have occurred related to a payment processor's activities. Appropriate actions may include filing a Suspicious Activity Report, requiring the payment processor to cease processing for that specific merchant, or terminating the financial institution's relationship with the payment processor. Should it be determined that a financial institution does not have an adequate program in place to monitor and address the risks associated with third-party payment processor relationships, an appropriate supervisory response will be used to require the financial institution to correct the deficiencies.

Michael B. Benardo

Chief, Cyber-Fraud and Financial Crimes Section
Division of Risk Management Supervision
mbenardo@fdic.gov

Robert J. Wirtz

Assistant Regional Director (Compliance)
Division of Depositor and Consumer Protection
rwirtz@fdic.gov

Kathryn M. Weatherby

Examination Specialist (Fraud)
Cyber-Fraud and Financial Crimes Section
Division of Risk Management Supervision
kweatherby@fdic.gov

From: [REDACTED]
Sent: Thursday, June 27, 2013 4:58 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Creating new matters in ALIS

Ma'am -- Could you please create for Lance and me a matter called "Operation Chokepoint"? We are working on a multi-agency taskforce headed by DOJ that focuses on third party payment processors and their relationships with banks and the ACH network. As part of that project we are reviewing subpoenas served upon financial institutions and IAPs.

Let me know if you have any questions or need any additional info.

[can you pretty that up and make it work?]

From: [REDACTED]
Sent: Thursday, June 27, 2013 4:45 PM
To: Legal Consumer Section
Subject: Creating new matters in ALIS

Good afternoon everyone. Regardless of the status of new ALIS matters with Chris TA, there continue to be a steady flow of new matters coming from DCP. Some of you have created several already. In early June, I had offered to create matters in ALIS once it went live for consumer matters and sent around a spreadsheet for each office for that purpose.

To the extent that you have matters not yet created and would like some help with that, I am available to help create them tomorrow or Monday. If so, please send me your list.

Today I also recorded a CMP payment in ALIS if anyone has questions on doing that.

Thanks.

[REDACTED]
Management Analyst
Legal Division, Consumer Section
Federal Deposit Insurance Corporation
550 17th Street, NW
[REDACTED]
Washington, DC 20429 0002
[REDACTED]
[REDACTED]
[REDACTED]

From: [REDACTED]
Sent: Wednesday, July 24, 2013 9:59 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Did you open Project Chokepoint (our DOJ /Spike Lee Joint) on Go Ask ALIS?

No worries. Thanks.

From: [REDACTED]
Sent: Wednesday, July 24, 2013 9:41 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Did you open Project Chokepoint (our DOJ /Spike Lee Joint) on Go Ask ALIS?

Opening it now as I type this sorry for the delay.

[REDACTED]
Management Analyst
Legal Division, Consumer Section
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429-0002

From: [REDACTED]
Sent: Tuesday, July 23, 2013 4:02 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: Did you open Project Chokepoint (our DOJ /Spike Lee Joint) on Go Ask ALIS?

[REDACTED]
Counsel, Consumer Enforcement Unit
Legal Division, FDIC

This material has been redacted.

April 2, 2014

M. Anthony Lowe
Regional Director
Federal Deposit Insurance Corporation
Chicago Regional Office
300 South Riverside Plaza, Suite 1700
Chicago, IL 60606

Charles Vice
Commissioner
Commonwealth of Kentucky
Public Protection Cabinet
Department of Financial Institutions
1025 Capital Center, Suite 200
Frankfort, KY 40601

RE: Response to Item 2 of Memorandum of Understanding

Gentlemen:

Enclosed you will find our Due Diligence Program ("Program") that was drafted pursuant to item 2 of a Memorandum of Understanding (MOU) among the Bank, the Regional Director of the Federal Deposit Insurance Corporation and the Commissioner of the Kentucky Department of Financial Institutions, effective February 3, 2014. The Program will be incorporated into our Policy which we anticipate will be presented to the Board in the second quarter.

If you have any questions regarding this analysis, feel free to contact me at **Redacted**

This material has been redacted.

Customer Awareness

The Bank will make conscientious efforts to inform its customer base of known or perceived threats and risks associated with associated with ACH origination activity.

Non-Qualified and High Risk Customer List

The following is a sample listing of the types of companies/merchants The Bank considers an unacceptable business category from which to accept ACH files for processing or High Risk business or services that require additional due diligence.

1. Restricted Products, Services and Methods of selling:

- Auctions
- Bail Bond Services
- Bars/Taverns (not serving food)
- Credit Restoration, Debt Relief Services
- Modeling Agencies
- Resort Land Promotions
- Talent Booking Agencies
- Third Party Hotel Reservation Services
- Vitamin and Supplement Sales

2. Prohibited Products and Services:

- Adult Entertainment
- Check Cashing Institutions
- Companion or Escort Services
- Debt Relief Services
- Drug Paraphernalia
- Gambling Establishments
- Lotteries or Raffles
- Massage Parlors
- Nested Payment Processors
- Payday Lenders
- Ponzi Schemes
- Pornographic/Adult Materials
- Sexual Encounter Agencies
- Tattoo Parlors
- Tax Anticipation Programs

3. *Prohibited Methods of Selling:*

- Door to Door
- Flea Markets
- Neighborhood Party Sales
- Pyramid/Multi-Level Sales

4. *High Risk Merchant Types*

- Short term loans with high interest rates
- Ammunition Sales
- "As Seen on TV"
- Credit Card Schemes
- Escort Service
- Firearms/Fireworks Sales
- Get Rich Product
- Government Grants
- Home Based Charities
- Lifetime Guarantees
- Pawn Shops
- Pyramid Type Sales
- Pharmaceutical Sales
- Raffle/Sweepstakes
- Surveillance equipment
- Telemarketing
- Tobacco Sales
- Other Payment Processors

Additional Guidelines for Internet Merchant Customers

It is the responsibility of an evaluating officer to conduct thorough underwriting reviews of customers whose business operations involve Internet sales using bank and trade verifications. During the underwriting process, the customer relationship officer is to determine whether heightened fraud and returned item risk warrants the use of additional risk mitigation techniques, such as establishing a reserve.

Electronic commerce over the Internet poses privacy and security concerns to the Bank, and those concerns are to be addressed in an officer's initial underwriting, including the assurance of the appropriate security of transactions in addition to stored data by the customer are properly provided for. Such security techniques include secured servers and data encryption technologies (e.g., Secured Socket Layers) to help protect data and transaction integrity. Therefore, an Internet based business customer is required by the Bank as part of its credit underwriting approval process to have the following items appear on its website:

This material has been redacted.



FDIC

Federal Deposit Insurance Corporation
Division of Supervision and Consumer Protection
2345 Grand Boulevard, Suite 100
Kansas City, MO 64108

AUG24'10 RCVD

Consumer Response Center
1-800-378-9581
Fax number 703-812-1020

August 18, 2010

Redacted

This material has been redacted.

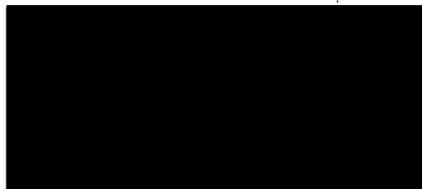
Dear **Redacted**:

We have completed our review of your email and the Bank's research into your experience with the bill payment service it offers. The FDIC contacted the Bank on your behalf and received the enclosed response.

You used the **Redacted** (bill payment service) interface to make a \$192.37 payment. When the bill payment service set up the Bank's account, the incorrect routing number was input. The Bank became aware that bill payment service customers were being negatively impacted by this input error and it placed a notice on its website **Redacted** alerting depositors that payments were being returned and providing a telephone number for customers to use to regarding the situation.

Please refer to the enclosed terms and conditions of the bill pay service, which explains payment scheduling/authorization/methods and other features. The Bank credited your checking account on July 7, the same day that you discussed this matter with its representative. We enclose the Winter edition of the FDIC's *Consumer News*, as this issue contains information pertaining to on-line banking.

We hope this helps to resolve the matter. The FDIC appreciates hearing from the public, as these letters provide comment to the banking industry and help us tailor examinations to areas of concern. If you would like to discuss this response, please contact me at, 800.756.3558, x-8116 (8:a.m. – 5:p.m. Pacific Time, M-F).



Enclosures

Redacted

GOVERNING LAW

This Agreement shall be governed by and construed in accordance with the laws of the State of Georgia, without regard to its conflicts of laws provisions. To the extent that the terms of this Agreement conflict with applicable state or federal law, such state or federal law shall replace such conflicting terms only to the extent required by law. Unless expressly stated otherwise, all other terms of this Agreement shall remain in full force and effect.

THE FOREGOING SHALL CONSTITUTE THE SERVICE'S ENTIRE LIABILITY AND YOUR EXCLUSIVE REMEDY. IN NO EVENT SHALL THE SERVICE BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING LOST PROFITS (EVEN IF ADVISED OF THE POSSIBILITY THEREOF) ARISING IN ANY WAY OUT OF THE INSTALLATION, USE, OR MAINTENANCE OF THE EQUIPMENT, SOFTWARE, AND/OR THE SERVICE.

TERMS OF USE ([Redacted] Personal Payments Service)

Last updated May 6, 2010.

1. **Introduction.** This Terms of Use document (hereinafter "Agreement") is a contract between [Redacted] (hereinafter "we" or "us") in connection with the [Redacted] Personal Payments Service (the "Service") offered through our online banking site (the "Site"). This Agreement applies to your use of the Service and the portion of the Site through which the Service is offered.
2. **Service Providers.** We are offering you the Service through one or more "Service Providers" that we have engaged to render some or all of the Service to you on our behalf. You agree that we have the right under this Agreement to delegate to Service Providers all of the rights and performance obligations that we have under this Agreement, and that the Service Providers will be third party beneficiaries of this Agreement and will be entitled to all the rights and protections that this Agreement provides to us. "Service Provider" and certain other terms are defined in a "Definitions" section at the bottom of this Agreement.
3. **Amendments.** We may amend this Agreement and any applicable fees and charges for the Service at any time by posting a revised version on the Site. The revised version will be effective at the time it is posted unless a delayed effective date is expressly stated in the revision. Any use of the Service after a notice of change will constitute your agreement to such changes. Further, we may, from time to time, revise or update the Service and/or related applications or material, which may render all such prior versions obsolete. Consequently, we reserve the right to terminate this Agreement as to all such prior versions of the Service, and/or related applications and material and limit access to only the Service's more recent revisions and updates.
4. **Our Relationship With You.** We are an independent contractor for all purposes, except that we act as your agent with respect to the custody of your funds for the Service. We do not have control of, or liability for, any products or services that are paid for with our Service. We also do not guarantee the identity of any user of the Service (including but not limited to Receivers to whom you send payments).
5. **Assignment.** You may not transfer or assign any rights or obligations you have under this Agreement without our prior written consent, which we may withhold in our sole discretion. We reserve the right to transfer or assign this Agreement or any right or obligation under this

[Redacted]

7/19/2010

Agreement at any time to any party. We may also assign or delegate certain of our rights and responsibilities under this Agreement to independent contractors or other third parties.

6. **Notices to Us Regarding the Service.** Except as otherwise stated below, notice to us concerning the Site or the Service must be sent by postal mail to:

This material has been redacted.

We may also be reached at **Redacted** for questions and other purposes concerning the Service, but such telephone calls will not constitute legal notices under this Agreement.

7. **Notices to You.** You agree that we may provide notice to you by posting it on the Site, sending you an in-product message within the Service, emailing it to an email address that you have provided us, mailing it to any postal address that you have provided us, or by sending it as a text messages to any cellphone number that you have provided us, including but not limited to the cellphone number that you have listed in your Service Setup. For example, users of the Service may receive certain notices (such as notices of payment, alerts for validation and receipt of transfers) as text messages on their cellphones. All notices by any of these methods shall be deemed received by you no later than twenty-four (24) hours after they are sent or posted, except for notice by postal mail, which shall be deemed received by you no later than three (3) business days after it is mailed. You may request a paper copy of any legally required disclosures and you may terminate your consent to receive required disclosures through electronic communications by contacting us as described in section 6 above. We reserve the right to charge you a reasonable fee not to exceed twenty (20) dollars to respond to each such request. We reserve the right to close your account if you withdraw your consent to receive electronic communications.
8. **Calls to You.** By providing us with a telephone number (including a wireless/cellular telephone), you consent to receiving autodialed and prerecorded message calls from us at that number for non-marketing purposes.
9. **Receipts and Transaction History.** You may view at least six months of your transaction history by logging into your account and looking at your account transaction history. You agree to review your transactions by this method instead of receiving receipts or periodic statements by mail.
10. **Your Privacy.** Protecting your privacy is very important to us. Please review our Privacy Policy in order to better understand our commitment to maintaining your privacy, as well as our use and disclosure of your information.
11. **Privacy of Others.** If you receive information about another person through the Service, you agree to keep the information confidential and only use it in connection with the Service.
12. **Eligibility.** The Service is offered only to individual residents of the United States who can form legally binding contracts under applicable law. Without limiting the foregoing, the Service is not offered to minors. By using the Service, you represent that you meet these requirements and that you agree to be bound by this Agreement.
13. **Prohibited Payments.** The following types of payments are prohibited through the Service, and we have the right but not the obligation to monitor for, block and/or reverse such payments:
- Payments to or from persons or entities located outside of the United States and its territories; and
 - Payments that violate any law, statute, ordinance or regulation; and
 - Payments that violate the Acceptable Use terms in section 14 below; and
 - Payments related to: (1) tobacco products, (2) prescription drugs and devices; (3) narcotics, steroids, controlled substances or other products that present a risk to consumer safety; (4) drug paraphernalia; (5) ammunition, firearms, or firearm parts or related accessories; (6) weapons or knives regulated under applicable law; (7) goods or services that encourage, promote, facilitate or instruct others to engage in illegal activity; (8) goods or services that are sexually oriented; (8) goods or services that promote hate, violence, racial intolerance,

Redacted

7/19/2010

This material has been redacted.

Memorandum

Date: 13 August 2013
To: [REDACTED] FDIC; [REDACTED], PA Department of Banking
From: [REDACTED]
RE: Quarterly Submission

Subsequent to the Bank's 15 May 2013 quarterly submission, the Bank has continued to take substantive action to comply with the 19 October 2012 Consent Order, including but not limited to the following:

- The last merchants of our last ISO transitioned to a new financial institution as of 23 July 2013. (Trailing chargeback activity will continue for another six months);
- We have engaged Accume Partners to complete our internal BSA Audit for 2013, and the fieldwork is ongoing as of this writing;
- As of June 2013, we have commenced the Independent Monitoring Program—retroactive to December 2012—for the E-Payments area;
- [REDACTED] has been submitted to the FDIC as the new BSA Officer;
- We have resubmitted our 2011 and 2012 HMDA data as directed in conjunction with the 2013 Compliance Exam;
- Pending the completion of Accume Partners' BSA Audit—the expected report date is September 20, 2013—all items under the Consent Order will have been completed, or have been addressed in an ongoing manner.

Should you have any questions or concerns, please do not hesitate to contact me.

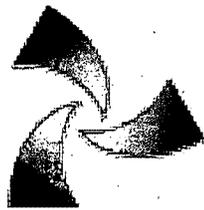
This material has been redacted.

CONSENT ORDER
QUARTERLY SUBMISSION—AUGUST 2013

ITEM 9

4(b) and 4(c) EXTERNAL TRAINING—Banker's Hub

N.B. The Bank purchased—prior to the original presentation—the audio recording and the associated slides for the webinar that was originally broadcast on July 30, 2013. Those who have signed the sheet below participated in a “replay” on August 12, 2013;



BankersHub
Getting from Here to There

BSA Audit Prep for Payments

ACH, Wire Transfer, RDC and Cards

July 30, 2013



Third Party Payment Processor

Non-bank financial institution

- ◇ NOT currently directly subject to Bank Secrecy Act compliance
- ◇ provides gateway to banking system
- ◇ *State money transmitter licensing may be required*
- ◇ *subject to examination by state(s) where licensed*
- ◇ 3rd party review on behalf of servicing bank(s)

--	--



TPPP Overview

- ◆ A bank's business customer that uses its deposit relationship to process payments on behalf of other businesses.
- ◆ Bank provides channel for clearing and settlement a variety of payment types: ACH, checks, payment cards, digital currencies, etc.
 - ◆ May include electronic checks created through Remote Deposit Capture, or
 - ◆ Remotely Created Checks (RCCs) that never existed in paper form.
- ◆ Differs from traditional business banking relationships where payment transactions (e.g., ACH, checks, etc.) are made on behalf of the business customer.



TPPP Merchant Clients

- ◆ What type of merchants? Risk level?
- ◆ How are merchants qualified and accepted?
- ◆ Who is served under what conditions?
- ◆ How and when are merchant relationships terminated?



Higher Potential Risk Merchants / Activities

★ Other Payment Processors

- ◆ Ammunition Sales
- ◆ "As Seen on TV"
- ◆ Coin Dealers
- ◆ Credit Card Schemes
- ◆ Credit Repair Services
- ◆ Dating Services
- ◆ Drug Paraphernalia
- ◆ Escort Services
- ◆ Firearms/Fireworks Sales
- ◆ Gambling
- ◆ Get Rich Quick Products
- ◆ Government Grants
- ◆ Home Based Charities/Businesses
- ◆ Life Time Guarantees
- ◆ Membership/Purchasing Clubs
- ◆ Pyramid Type Sales
- ◆ Pay Day Loans
- ◆ Pharmaceutical Sales
- ◆ Pornography
- ◆ Ponzi Schemes
- ◆ Racist materials
- ◆ Raffles/Sweepstakes
- ◆ Surveillance equipment
- ◆ Telemarketing
- ◆ Tobacco Sales
- ◆ Travel Clubs



Red Flags

- ◆ Significant Consumer Complaints
 - ◆ unauthorized, misrepresented, intimidated, threatened into providing account information
- ◆ High level of unauthorized returns/charge-backs
- ◆ Unverifiable merchant information (e.g., website, business registration, etc.)
- ◆ Unexpected volume/value activity or change
- ◆ Prior civil, criminal and regulatory actions against processor or its principals
- ◆ Law enforcement inquiries



Bank's Minimum Responsibilities

- ◆ Comprehensive Policies and Procedures
- ◆ Assess risk of TPPPs (including review of merchant clients)
- ◆ Review Contracts with Processors and Sub-Processors
- ◆ Establish sound and enforceable contractual requirements for all parties
- ◆ In-Depth Enhanced Due Diligence



Bank's Minimum Responsibilities

- ◆ Evaluate Due Diligence Performed by Processors on the Merchants they work with
- ◆ Perform Ongoing Monitoring
 - ◆ Consumer complaints
 - ◆ High rates of returns or charge backs
- ◆ Establish and Maintain Adequate Reserve Accounts
- ◆ Ongoing Training so staff can effectively monitor/identify problems

--	--



Reliance on TPPPs

- ◆ Banks *must not rely entirely* on TPPP systems for merchant approval and monitoring.
- ◆ Cursory merchant reviews without ensuring appropriate ongoing monitoring of the TPPP and transaction activity is inappropriate.
- ◆ Any reliance placed on TPPP for initial or ongoing tasks need to be *verified periodically by external and/or bank review* of TPPP policies, procedures, and processes



Best Practices

- ◇ Require TPPP to provide documented analysis / legal opinion regarding potential state licensing issues
- ◇ Require TPPP to have written risk-based BSA/AML program
- ◇ independent review
- ◇ Periodic bank review and/or 3rd party examination
- ◇ Negative news monitoring of TPPP, merchant clients



Remember!

- ◇ Bank *retains ultimate responsibility* for all transactions flowing through the bank.
- ◇ Must file SARs on unusual or suspicious activities
- ◇ Bank must have sufficient understanding of each TPPP and its merchant processing to identify unusual activity.



When Bank Finds Suspicious Activity

- ◇ File a Suspicious Activity Report
- ◇ If fraudulent merchant activity suspected,
 - ◇ require TPPP to cease processing for that specific merchant
 - ◇ reexamine TPPP and merchant activity
 - ◇ Terminate relationship with TPPP when appropriate

This material has been redacted.

MEMORANDUM

To: Board of Directors

From: **Redacted**, BSA/AML/OFAC Compliance Officer

Re: Bank Secrecy Act (BSA) & Anti-Money Laundering (AML) Report: June 2011

Date: July 21, 2011

Background

This material has been redacted.

This material has been redacted.

AML News Bits	
<p>The FDIC Supervisory Committee Releases their Supervisory Insights – Summer 2011</p> <p>June 2011</p>	<p style="text-align: center;">Excerpt From the Supervisory Insights – Summer 2011 edition:</p> <p>For the full report, or additional information, please refer to http://www.fdic.gov/regulations/examinations/supervisory/insights/sisum11/si_sum11.pdf</p> <p>Managing Risks in Third-Party Payment Processor Relationships During the past few years, the Federal Deposit Insurance Corporation (FDIC) has observed an increase in the number of deposit relationships between financial institutions and third-party payment processors and a corresponding increase in the risks associated with these relationships. Deposit relationships with payment processors can expose financial institutions to risks not present in typical commercial customer relationships, including greater strategic, credit, compliance, transaction, legal, and reputation risk.</p> <p>Although many payment processors effect legitimate payment transactions for a variety of reputable merchants, an increasing number of processors have been initiating payments for abusive telemarketers, deceptive online merchants, and organizations that engage in high risk or illegal activities.</p> <p>The potential for misuse or fraud exists in all payment channels. However, the FDIC has observed that some of the most problematic activity occurs in the origination of ACH debits or the creation and deposit of remotely created checks.</p> <p>Types of High Risk Payments Although many clients of payment processors are reputable merchants, an increasing number are not and should be considered “high risk.” These disreputable merchants use payment processors to charge consumers for questionable or fraudulent goods and services. Often a disreputable merchant will engage in high pressure and deceptive sales tactics, such as aggressive telemarketing or enticing and misleading pop-up advertisements on Web sites.</p> <p>Still other disreputable merchants will use processors to initiate payments for the sale of products and services, including, but not limited to, unlawful Internet gambling and the illegal sale of tobacco products on the Internet.</p> <p>Some merchant categories that have been associated with high-risk activity include, but are not limited to:</p> <ul style="list-style-type: none"> • Ammunition or Firearms Sales • Life-Time Memberships • Coin Dealers • Lottery Sales

- Credit Card Schemes
- Credit Repair Services
- Dating Services
- Debt Consolidation Scams
- Drug Paraphernalia
- Pornography or Escort Services
- Fireworks Sales
- Get Rich Products
- Government Grants
- Home-Based Charities
- Life-Time Guarantees
- Mailing Lists/Personal Info
- Money Transfer Networks
- On-line Gambling
- PayDay Loans
- Pharmaceutical Sales
- Ponzi Schemes or Pyramid-Type Sales
- Racist Materials
- Surveillance Equipment
- Telemarketing
- Tobacco Sales
- Travel Clubs

Of particular concern, the FDIC and other federal regulators have seen an increase in payment processors initiating payment for online gaming activities that may be illegal. The Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) prohibits financial institutions from accepting payments from any person engaged in the business of betting or wagering with a business in unlawful Internet gambling.

High-Risk Payment Processor Relationship Warning Signs

Financial institutions and examiners should be aware of the warning signs that may indicate heightened risk in a payment processor relationship. Some warning signs are:

- A high volume of consumer complaints that suggest a merchant client is inappropriately obtaining personal account information; misleading customers as to the quality, effectiveness, and usefulness of the goods or services being offered; or misstating the sales price or charging additional and sometimes recurring fees that are not accurately disclosed or properly authorized during the sales transaction.
- A large number of returns or chargebacks
- A significant amount of activity which generates a higher than normal level of fee income.
- Payment processors that use more than one financial institution to process merchant client payments; thereby helping to avoid detection of inappropriate activity.

Finally, another troubling development is payment processors that purposefully solicit business relationships with troubled institutions in need of capital.

Conclusion

Deposit relationships with payment processors expose financial institutions to risks that may not be present in relationships with other commercial customers. To limit potential risks, financial institutions should implement risk mitigation policies and procedures that include appropriate oversight and controls commensurate with the risk and complexity of the activities.

R

Elston, Dennis R.**This material has been redacted as non-responsive.**

From: Elston, Dennis R.
Sent: Thursday, March 06, 2014 9:43 AM
To: Redacted
Cc: Elston, Dennis R.
Subject: Payday Lending and Related Guidance

Redacted

To follow-up on our phone call conversation, the following Financial Institution Letters (FILs) should be considered:

- FIL-14-2005: Guidelines for Payday Lending
- FIL-44-2008: Guidance for Managing Third-Party Risk

The FILs can be accessed from our external website www.fdic.gov by selecting the laws and regulations tabs and picking the FILs option. If I understand what is being proposed, a Native-American group is proposing to offer payday loan products online and funds will flow from the bank through ACH transactions. As I mentioned earlier, while the bank is not expected to directly offer payday loans, it will facilitate such lending and the risks discussed in FIL-14-2005 should be closely considered. I am not sure how the arrangement is expected to work, but if a third-party vendor will be involved, or any relationship connecting the bank with the depositor group that must be supervised, the concerns raised in FIL-44-2008 must be addressed.

As I stated earlier, the arrangement will receive close regulatory scrutiny from the FDIC and State Banking Department. In-depth BSA and IT reviews of this relationship will also take place. Even under the best circumstances, if this venture is undertaken with the proper controls and strategies to try to mitigate risks, since your institution will be linked to an organization providing payday services, your reputation could suffer.

If the Board plans to go forward with this venture, please reduce your plans to writing by submitting a letter to the FDIC's Regional Director (Thomas J. Dujenski) and the Superintendent of Banks for the State of Alabama (John Harrison) outlining your proposal.

Thanks,
Dennis

Elston, Dennis R.

From: Warren, Gregory R.
Sent: Thursday, March 06, 2014 1:14 PM
To: Elston, Dennis R.
Subject: Payday Lending

Dennis,

Georgia Bass received a phone call from President [Redacted] of [Redacted] Bank regarding payday lending. An attorney who represented payday lenders out in the Western part of the country contacted [Redacted] inquiring to see if the bank would open an online payday lending account to Native Americans. Apparently, the Native Americans are located on an Indian reservation. He stated that there would be a large volume of ACH transactions. He wanted to talk with the FDIC to determine the associated risks of opening such an account and to get the FDIC's position on payday lending. Georgia mentioned that President [Redacted] was keenly concerned with an attorney in another part of the country contacting his bank to request to open an account. I told Georgia that I would send you this information since the bank was in the [Redacted] geographic region.

Greg

From: Miller, Jonathan N. (DCP)
Sent: Thursday, September 05, 2013 6:13 PM
To: Pearce, Mark (DCP)
Subject: FW: Follow Up

Mark I took a quick look at her draft "guidance."

I just don't see how we can do this. It is a roadmap to blessing pay day or high cost installment loans.

I think what I will tell her, generally speaking, is that her draft really speaks past the issues we discussed. We are talking about third party relationships and the banks' obligations to identify and manage those risks on an ongoing basis, notwithstanding the specific business involved.

Her draft goes far, far beyond anything I have seen in my tenure at the FDIC regarding specifics dealing with products. I will tell her that we are in absolutely no position to say the things she is saying in this doc.

Finally, I'd like to make it clear to her that we are unlikely to put out specific guidance about dealing with one set of lenders or another that we believe our outstanding guidance addresses the issues we think are relevant to our banks.

I may have to confront the issue of overzealous examiners (immoral issue). I would do so by making clear that it is not FDIC policy to pass moral judgment on specific products. Rather, we look at risk to banks and consumers. But our job is to make sure banks understand their risks, and are in a position to manage them effectively, whatever the product. Our guidance does that. Her's does not.

How's that sound?

Jonathan

From: [Redacted]
Sent: Thursday, September 05, 2013 11:38 AM
To: Miller, Jonathan N. (DCP)
Subject: Follow Up

Hi Jonathan -

Thanks again for taking the time to meet with us. I really do appreciate the time and attention that you and Director Pearce have paid to this issue. As I indicated yesterday, my clients are interested in following up on whether the FDIC is willing to publish guidance for banks when doing business with online lenders (tribal lenders in particular).

If you have time, my calendar is free much of tomorrow if you want to have a call.

And if you need any additional material, please let me know. We want to try to give you any information that you may need to better understand the lending model and the relationships that tribal lenders have with banks (directly - not via payment processors).

Thanks!

[Redacted]

Redacted

Redacted

From: [REDACTED]
Sent: Friday, March 08, 2013 2:53 PM
To: Sagatelian, Marguerite; [REDACTED]
Subject: RE: Payday Lending

Will do.

A note that both Joel Sweet (of DOJ) and Mike Bernardo emphasized: although payday lending is a particularly ugly practice, it is only one of the TPPP problems out there. And as we have noted, [REDACTED] *may* be one of them, where the non-bank part of the equation was misusing payroll taxes and apparently was quite well known in the lower echelons.

From: Sagatelian, Marguerite
Sent: Friday, March 08, 2013 10:49 AM
To: [REDACTED]; [REDACTED]
Subject: RE: Payday Lending

Thank you, both. What has prompted today's inquiry is that the Chairman is meeting with some bankers next week, and DCP wants to give the Chairman some "talking points" as to how banks facilitate payday lending and why the FDIC is concerned. I think your supplemental memo addresses that point. We have a few TPPP cases right now, two of which are with [REDACTED] and [REDACTED]. Please make sure that you coordinate your efforts with [REDACTED] and [REDACTED] so that we develop a consistent approach regarding TPPPs. Thanks.

From: [REDACTED]
Sent: Friday, March 08, 2013 10:41 AM
To: [REDACTED] Sagatelian, Marguerite
Subject: RE: Payday Lending

I echo what [REDACTED] said below. Let me add the following:

Just so we are all on the same page, we did two memos, the second a supplemental memo in which we outlined four situations in which a bank might be involved with payday lending, including TPPPs. That second memo seems to go to what DCP was asking you. I am attaching a copy of that second memo again for your convenience; if DCP hasn't seen that memo, that may be the one they want. The memo concludes that a bank's relationship to payday lending (some engage in it directly) or to the payday lender or TPPP might by itself give rise to a possible enforcement action, depending on the nature of the relationship. Also, the KYC regulations for banks and regulatory guidance on TPPPs imposing due diligence requirements obligate banks to make sufficient inquiries that should allow banks to uncover most really bad behavior. Those due diligence requirements definitely give us (the FDIC) grounds for asking banks to keep track of what their payday lender/TPPP account holders are doing and a failure of banks to perform that due diligence may be grounds for an enforcement action, again in the right situations.

If DCP is looking for more than that, we are happy to look into whatever they want. What I just said is a little abstract but the nature of the relationships and underlying conduct will really be key to any consideration of an enforcement action so any more specific delineation of a possible enforcement action would be easier in the context of a specific bank and payday lending situation.

In that regard, I have also been doing some general research into how payday lending operates in practice particularly as it relates to insured depository financial institutions. While not directly involving payday lending, I also agree with [REDACTED] that the [REDACTED] case looks to be a good case regarding TPPPs that warrants further inquiry.

From: [REDACTED]
Sent: Friday, March 08, 2013 10:06 AM
To: Sagatelian, Marguerite; [REDACTED]
Subject: RE: Payday Lending

Marguerite,

We have not updated the memo as yet because we have taken many steps in the right direction, I think but are still working on putting together a solid approach on this issue. Director Pearce asked us to follow up with Mike Benardo, which I did. Mike had a wealth of information as to how payday lenders use weak or failing banks – sometimes with the banks' awareness and sometimes not – as essentially shells out of which they operate. (Note: That scenario may also be present in the [REDACTED] Bank Case.)

As I think I mentioned in a couple of emails and in my status updates, my meeting with Mike Benardo led me to an invitation to his presentation on third party processors last week. There he introduced me to Joel Sweet, an AUSA who specializes in consumer cases involving 3d party processors. Joel has a wealth of knowledge about how to get both the payday lender and the bank that facilitates the lending. Luckily for us, Joel is just starting (last week) a 6 month detail at Main Justice. Joel, Lance and I are working to schedule a meeting next week. Our goal is to come out of that meeting with at least a broad outline of how to approach this problem.

I hope this is helpful. Please let me know if you have any questions.

Thanks.

From: Sagatelian, Marguerite
Sent: Friday, March 08, 2013 9:32 AM
To: [REDACTED]
Subject: Payday Lending

[REDACTED] and [REDACTED]

I've received an inquiry from DCP about where we stand regarding our research into what avenues are available to the FDIC to take action against banks that facilitate payday lending. I have the memo you did a while back. Has that memo been updated? I know that after we met with Mark, you were going to explore the BSA/Know Your Customer requirements to see if that would provide the FDIC with the means to get at payday lending (either by the bank's direct customer or through a third party payment processor).

Please let me know where things stand and send me any updated memo you have completed.

Thanks,
Marguerite

Marguerite Sagatelian
FDIC
Senior Counsel - Consumer Enforcement Unit
550 17th Street, N.W., [REDACTED]
Washington, DC 20429
[REDACTED]

From: Barr, David
Sent: Friday, September 13, 2013 10:38 AM
To: Pearce, Mark (DCP); Brueger, Kathleen S.; Spitler, Eric J.; Miller, Rae-Ann; Watkins, James C.
Cc: Gray, Andrew; French, George; Plunkett, Sylvia H.; Eberley, Doreen R.; Miller, Jonathan N. (DCP); Brown, Luke H.
Subject: RE: 3rd Party Payment Providers

I got a bit more background from Joe on this piece. They are looking at the on-line lending issue as a whole. Part of it will focus on regulators forcing banks out of relationships with payment processors who work with these on-line lenders. Joe has heard second and third hand information that a senior FDIC official has called on-line lending immoral, according to a banker who heard it from an examiner. Some of the pushback from The Hill is that it is not up to the FDIC decide what is moral and immoral, but rather what type of lending is legal. The GOP is saying that the FDIC doesn't like on-line lending and is forcing banks to end their relationships with payment providers. This is hurting even the good "apples" out there. They agree that some of the on-line lenders are not good, but our widespread decision to force banks out of the business is cutting off credit to those that need it, and forcing even the good lenders to exit the business. Joe has also heard that there was a recent Hill briefing on this and we have denied that we are forcing banks to end these relationships. It's the same thing we said a couple of years ago when it was the brick-and-mortar payday lenders that we denied forcing out of banking relationships. Now it's on-line lenders.

--db

From: Pearce, Mark (DCP)
Sent: Friday, September 13, 2013 7:02 AM
To: Brueger, Kathleen S.; Spitler, Eric J.; Miller, Rae-Ann; Watkins, James C.; Barr, David
Cc: Gray, Andrew; French, George; Plunkett, Sylvia H.; Eberley, Doreen R.; Miller, Jonathan N. (DCP); Brown, Luke H.
Subject: RE: 3rd Party Payment Providers

Had a brief conversation with Chairman and he suggested pushing this off to next week, if we could, given that there are so many of us traveling.

Mark Pearce
Director, Division of Depositor and Consumer Protection
Federal Deposit Insurance Corporation


From: Brueger, Kathleen S.
Sent: Thursday, September 12, 2013 4:55 PM
To: Spitler, Eric J.; Miller, Rae-Ann; Watkins, James C.; Barr, David
Cc: Gray, Andrew; Pearce, Mark (DCP); French, George; Plunkett, Sylvia H.; Eberley, Doreen R.; Miller, Jonathan N. (DCP); Brown, Luke H.
Subject: RE: 3rd Party Payment Providers

Just looping in Jonathan and Luke...

From: Spitler, Eric J.
Sent: Thursday, September 12, 2013 4:52 PM
To: Miller, Rae-Ann; Watkins, James C.; Barr, David

Cc: Gray, Andrew; Pearce, Mark (DCP); French, George; Plunkett, Sylvia H.; Eberley, Doreen R.; Brueger, Kathleen S.
Subject: RE: 3rd Party Payment Providers

I would also note that we should push back on framing the issue that we are pressuring banks not to provide this service. As I understand it, we are making certain that banks understand the risks in these relationships and take appropriate steps to manage the risks -- not to get out of the business.

From: Spitler, Eric J.

Sent: Thursday, September 12, 2013 4:49 PM

To: Miller, Rae-Ann; Watkins, James C.; Barr, David

Cc: Gray, Andrew; Pearce, Mark (DCP); French, George; Plunkett, Sylvia H.; Eberley, Doreen R.; Brueger, Kathleen S.

Subject: RE: 3rd Party Payment Providers

Agree that our speaking representative, if we choose to provide one, should be someone senior who has been involved in the response to the Hill -- and that the Chairman's office should be informed about the inquiry.

From: Miller, Rae-Ann

Sent: Thursday, September 12, 2013 4:13 PM

To: Watkins, James C.; Barr, David

Cc: Gray, Andrew; Pearce, Mark (DCP); French, George; Plunkett, Sylvia H.; Eberley, Doreen R.; Spitler, Eric J.; Brueger, Kathleen S.

Subject: RE: 3rd Party Payment Providers

Mark P has been our chief communicator on this issue and I am copying Eric on it, since it is an issue of interest on the Hill at the moment.

From: Watkins, James C.

Sent: Thursday, September 12, 2013 4:10 PM

To: Barr, David

Cc: Gray, Andrew; Pearce, Mark (DCP); Miller, Rae-Ann; French, George; Plunkett, Sylvia H.; Eberley, Doreen R.

Subject: Re: 3rd Party Payment Providers

We should probably keep comments limited if it relates to online lending but could reference our guidance on third party providers and Supervisory Journal articles.

From: Barr, David

Sent: Thursday, September 12, 2013 04:02 PM Eastern Standard Time

To: Watkins, James C.

Cc: Gray, Andrew

Subject: 3rd Party Payment Providers

The American Banker newspaper is working on an item about on-line lenders that look a lot like payday lenders and their use of banks for their payment systems. Joe Adler indicated that some banks are pushing back on regulators' pressure to persuade banks from providing this type of service for on-line lenders. We have been steering clear of the on-line lender issue, but didn't know if it would be a good opportunity to discuss the risks of third-party relationships. It probably isn't since the article will be tied to the on-line lenders, which is a very, very small part of the banking industry. He has no immediate deadline, but as usual, the sooner the better. If you think it might be worth pursuing, I'd run it past the sixth floor first. I also assume this is an RMS area and not a DCP one.

Thanks.

--db

From: Sagatelian, Marguerite
Sent: Friday, March 08, 2013 9:32 AM
To: [REDACTED]; [REDACTED]
Subject: Payday Lending

[REDACTED] and [REDACTED]

I've received an inquiry from DCP about where we stand regarding our research into what avenues are available to the FDIC to take action against banks that facilitate payday lending. I have the memo you did a while back. Has that memo been updated? I know that after we met with Mark, you were going to explore the BSA/Know Your Customer requirements to see if that would provide the FDIC with the means to get at payday lending (either by the bank's direct customer or through a third party payment processor).

Please let me know where things stand and send me any updated memo you have completed.

Thanks,
Marguerite

Marguerite Sagatelian
FDIC
Senior Counsel Consumer Enforcement Unit
550 17th Street, N.W., [REDACTED]
Washington, DC 20429
[REDACTED]

From: Sen, Surge
Sent: Friday, March 08, 2013 11:18 AM
To: Sagatelian, Marguerite
Subject: RE: Request for Information - Banks facilitating payday lending

Marguerite,

This is extremely helpful.

Many thanks,

Surge

From: Sagatelian, Marguerite
Sent: Friday, March 08, 2013 11:15 AM
To: Sen, Surge
Subject: RE: Request for Information - Banks facilitating payday lending

Hi Surge,

There are a couple of things we in Legal are working on right now. First, we have at least two active cases involving third party payment processors (TPPPs). In one case we obtained and are reviewing e-mails to determine whether bank management knew or was put on notice of the activities of the customers of the TPPPs, including payday lenders. Obviously, we cannot share with [Redacted] anything about current investigations.

Second, at the request of Mark Pearce, we are looking into avenues by which the FDIC can potentially prevent our banks from facilitating payday lending. Two of my staff members, [Redacted] and [Redacted] did some initial research, after which we met with Director Pearce. Subsequent to that meeting, we determined that a potentially viable avenue was BSA requirements imposed upon banks to conduct due diligence of their customers, and enhanced due diligence if the customer was engaged in higher-risk activity. At Director Pearce's suggestion, [Redacted] and [Redacted] have been in discussions with Mike Benardo in RMS (financial crimes section) and they will likely be meeting with attorneys at DOJ in the next few weeks. We hope to develop a more definitive game plan on how to address the payday lending issue after those meetings. We are also looking at the TPPP guidance (which, of course, is not itself enforceable)

I'm not sure if this addresses your questions. In terms of talking points for the Chairman, I think we should just say that Legal is looking into the different ways payday lending is conducted through our institutions, and what the bank's responsibility is depending on its relationship with the payday lender. Moreover, while payday lending is illegal in several states, in some states it is legal, and in most states it is subject to regulatory restrictions. Thus, one additional issue is that, in the context of Internet banking, where is the loan deemed to be made? In the state where the bank is located, or the state where the consumer resides? Most importantly, we believe that BSA requirements give the FDIC a good regulatory tool by which to uncover and address payday lending conducted through our institutions.

I have attached for reference a short memo prepared by [REDACTED] and [REDACTED] a couple of months ago. They are working on updating this memo, but you will get a sense of what we are looking at and what we believe the issues to be.

Let me know if you have any further questions.

Thanks,
Marguerite

From: Sen, Surge
Sent: Friday, March 08, 2013 9:11 AM
To: Sagatelian, Marguerite
Subject: Request for Information - Banks facilitating payday lending

Marguerite,

Happy Friday:)

We are working on some talking points for the Chairman's meeting with [Redacted] early next week. Specifically, we want to brief him on how large nationwide banks are facilitating payday lending through: Extending lines of credit to payday lenders, payment processing for payday lenders, and being nonresponsive to customer requests to stop payment/close their account when payday lenders attempt to withdraw funds from the customer's account.

During a DCP/Legal meeting you mentioned Legal's investigation in some of these activities by lenders (I thought it was the payment processing aspect). Are there any updates that you can provide us? What can we say about Legal's efforts?

Many thanks,

Surge

From: [REDACTED]
Sent: Wednesday, August 28, 2013 9:56 AM
To: [REDACTED]
Subject: RE: Pornography

And porn ain't illegal; obscenity is, which is subject to community standards.

From: [REDACTED]
Sent: Wednesday, August 28, 2013 9:53 AM
To: [REDACTED]
Subject: RE: Pornography

I don't have a legal argument to make (i don't think) but I agree that tying payday lending to pornography is a bit moralistic to me. I still think the better analogy is to telemarketing. Payday lending may be illegal some places, but it is legal IN ABOUT 35 STATES!!! In other words, in about 2/3 of the states (depending on which assessment of the various state laws you accept). And, whether we agree with them or not, there is still an argument made by some advocates of payday lending beyond the usual industry shills that payday lending done right serves a legitimate purpose for the unbanked that regular banks won't/can't meet. (In 2009 FDIC urged its banks to offer a new pdl-like product with an interest rate cap around 36% and it got no takers.) Failing to make that distinction between illegal and legal payday lending and instead lumping it in with purely objectionable products seems to me to feed the impression that we are trying to combat: that this is not a full-blown assault on payday lending but is instead targeted to on-line payday lending in states where it is illegal. If we really think it is that pernicious a practice, we should expand our enforcement approach beyond that limited target.

From: [REDACTED]
Sent: Wednesday, August 28, 2013 9:34 AM
To: [REDACTED]
Subject: RE: Pornography

PAY DDAY LENDING MAKES PORN LOOK BAD?

From: Rosebrock, Seth P.
Sent: Wednesday, August 28, 2013 9:33 AM
To: Lesemann, Dana J.
Subject: RE: Pornography

That was the idea ;)

[REDACTED]
Direct: [REDACTED]
Cellular: [REDACTED]

This communication is confidential and may contain privileged information. If you have received it in error, please notify the sender by reply e-mail and immediately delete it and any attachments without copying or further transmitting the same.

From: [REDACTED]
Sent: Wednesday, August 28, 2013 9:33 AM
To: [REDACTED]
Subject: RE: Pornography

Well, that got my attention. Now I will read the email.

From: [REDACTED]
Sent: Wednesday, August 28, 2013 9:32 AM
To: Sagatelian, Marguerite
Cc: [REDACTED]
Subject: Pornography

FYI:

I just got a call from Jonathan Miller regarding why we kept taking pornography out of their write up.

I explained that we felt there was a difference between on-line gambling and payday lending (which are illegal in some states) and pornography (which may be immoral, but which is not per se illegal). I noted that we didn't want to seem like we as a regulator were making moral judgments regarding the types of businesses with which our institutions deal. Rather, we wanted to make it clear that we were making rational safety and soundness decisions by discouraging our institutions from engaging in or facilitating illegal transactions.

Jonathan heard where we were coming from, but nonetheless wants to retain a reference to pornography in our letters / talking points. He thinks it's important for Congress to get a good picture regarding the unsavory nature of the businesses at issue. He repeated that "one is judged by the friends one keeps," and he seems to feel strongly that including payday lenders in the same circle as pornographers and on-line gambling businesses will ultimately help with the messaging on this issue.

If you feel that there is legal argument beyond the one I made, and would like us to push back on this issue, please let me know.

[REDACTED]

[REDACTED] Counsel
Federal Deposit Insurance Corporation
Legal Division, Consumer Enforcement Unit
1776 F. Street NW, [REDACTED]
Washington, DC 20429
Direct: [REDACTED] Cellular: [REDACTED]

This communication is confidential and may contain privileged information. If you have received it in error, please notify the sender by reply e mail and immediately delete it and any attachments without copying or further transmitting the same



Federal Deposit Insurance Corporation
 Division of Depositor and Consumer Protection
 Division of Risk Management Supervision
 300 South Riverside Plaza, Suite 1700, Chicago, IL 60606

Chicago Regional Office

Phone (312) 382-7500
 Fax (312) 382-6901

February 15, 2013

Board of Directors

Redacted

Members of the Board:

The FDIC continually assesses the risk and appropriateness of the business lines and activities of our supervised institutions. We have recently become aware of [Redacted] Bank's involvement in activities related to payday lending, specifically, the processing of transactions on behalf of [Redacted]. As a result, the FDIC and State of Ohio conducted a joint Compliance and Risk Management visitation of your bank as of December 17, 2012.

The focus of our visitation was on the risk associated with this relationship, compliance with consumer protection laws and regulations, and the effectiveness of Board and senior management due diligence and oversight of this relationship and the corresponding payday lending-related activities. It is our view that payday loans are costly, and offer limited utility for consumers, as compared to traditional loan products. Furthermore, the [Redacted] relationship carries a high degree of risk to the institution, including third-party, reputational, compliance, and legal risk, which may expose the bank to individual and class actions by borrowers and local regulatory authorities. Consequently, we have generally found that activities related to payday lending are unacceptable for an insured depository institution.

On February 5, 2013, Field Supervisor Jim Meyer and Supervisory Examiners John George and Sean Blair of the FDIC, along with Deputy Superintendent Kevin Allard, District Supervisor Brian Morgan and Chief Examiner Sheila Schroer of the Ohio Department of Financial Institutions, held a conference call with President [Redacted] and Chief Financial Officer [Redacted] to discuss the FDIC's concerns relative to the [Redacted] relationship. Members of our Region's Senior Management will contact you in the near term to schedule a meeting to further discuss our concerns relative to the aforementioned relationship.

Redacted

If you have any questions regarding this correspondence, please contact Assistant Regional Director [REDACTED] at [REDACTED] or Assistant Regional Director [REDACTED] at [REDACTED]

Sincerely,



M. Anthony Lowe
Regional Director

Redacted

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

NOV-05-2012

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: *FRI*
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	<i>SFP</i> NOV 5 2012	1/10/13
		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 &*

Make & 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.

HOCR-3PPP000016

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 identities 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 through accounts of suspicious third-party 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



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.

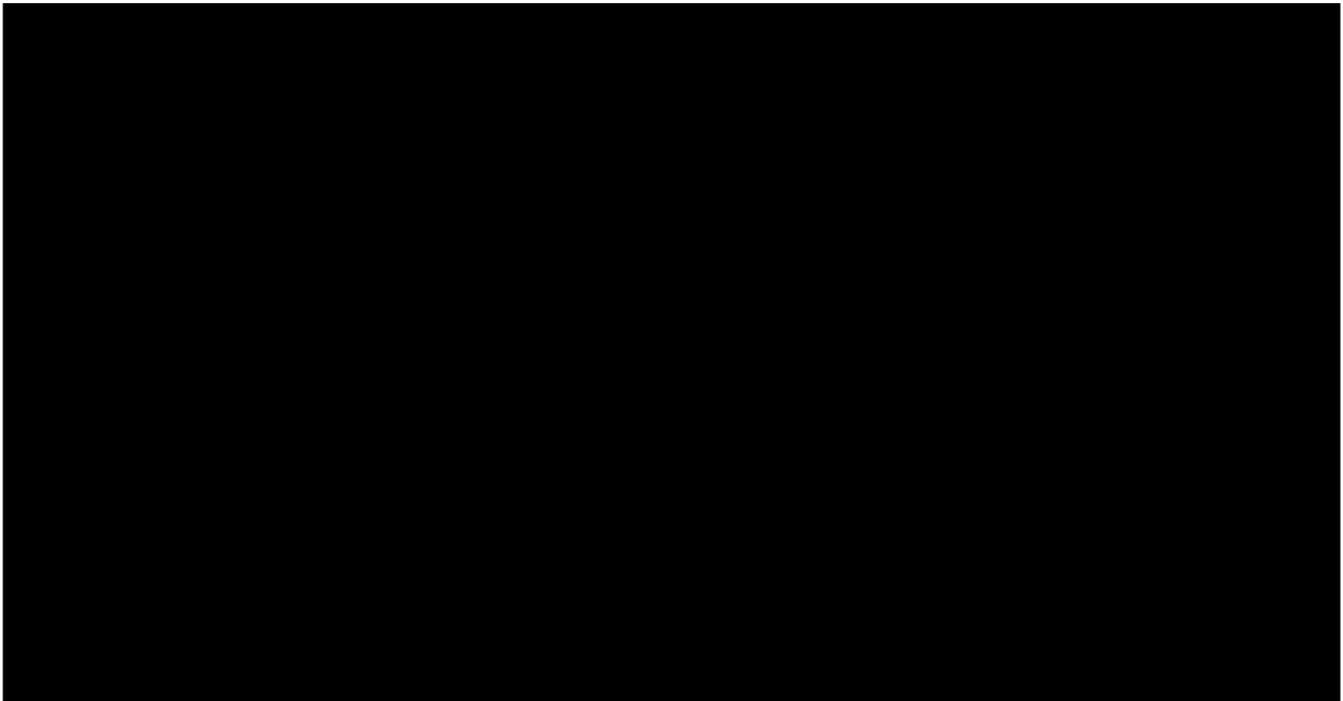
The subpoena returns we have received indicate that we are on the right path. Even before our first enforcement action, our activity has helped stem the tide of consumer fraud. As we expected, the mere receipt of a subpoena has caused many financial institutions to reconsider the wisdom and risks of 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

HOG-3PPP000167

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.



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 payday 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, USPS, 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 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])

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) (Jolin@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

Office: (202) 514-7281
Fax: (202) 307-2825

*" 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



2. Third Party Payment Processor Investigations



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.



Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-3-2012
January 31, 2012

Payment Processor Relationships Revised Guidance

Summary: Attached is revised guidance describing potential risks associated with relationships with third-party entities that process payments for telemarketers, online businesses, and other merchants (collectively "merchants"). These relationships can pose increased risk to institutions and require careful due diligence and monitoring. This guidance outlines certain risk mitigation principles for this type of activity.

Statement of Applicability to Institutions with Total Assets under \$1 Billion: This guidance applies to all FDIC-supervised financial institutions that have relationships with third-party payment processors.

Distribution:

FDIC Supervised Institutions

Suggested Routing:

Chief Executive Officer
Executive Officers
Compliance Officer
Chief Information Officer
BSA Officer

Related Topics:

Guidance on Payment Processor Relationships (FIL 127-2008, November 2008)
Consumer Protection, Compliance Risk, and Risk Management
FDIC Guidance for Managing Third Party Risk (FIL 44 2008, June 2008)
FFIEC Handbook on Retail Payment Systems (February 2010)
FFIEC Handbook on Outsourcing Technology Services (June 2004)
FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML)
Examination Manual (April 2010)
Managing Risks in Third-Party Payment Processor Relationships
(Summer 2011 Supervisory Insights Journal)

Attachment:

Revised Guidance on Payment Processor Relationships

Contacts:

Kathryn Weatherby, Examination Specialist (Fraud), Division of Risk Management Supervision, at kweatherby@fdic.gov or (703) 254 0469

John Bowman, Review Examiner, Division of Depositor and Consumer Protection, at jb Bowman@fdic.gov or (202) 898-6574

Note:

FDIC Financial Institution Letters may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2012/index.html.

To receive Financial Institution Letters electronically, please visit <http://www.fdic.gov/about/subscriptions/fil.html>. Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (877 275 3342 or 703 562-2200).

Highlights:

- Account relationships with third-party entities that process payments for merchants require careful due diligence, close monitoring, and prudent underwriting.
- Account relationships with high-risk entities pose increased risks, including potentially unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act.
- Certain types of payment processors may pose heightened money laundering and fraud risks if merchant client identities are not verified and business practices are not reviewed.
- Financial institutions should assess risk tolerance in their overall risk assessment program and develop policies and procedures addressing due diligence, underwriting, and ongoing monitoring of high-risk payment processor relationships.
- Financial institutions should be alert to consumer complaints or unusual return rates that suggest the inappropriate use of personal account information and possible deception or unfair treatment of consumers.
- Financial institutions should act promptly when fraudulent or improper activities occur relating to a payment processor, including possibly terminating the relationship.
- Improperly managing these risks may result in the imposition of enforcement actions, such as civil money penalties or restitution orders.

Revised Guidance on Payment Processor Relationships

The FDIC has recently seen an increase in the number of relationships between financial institutions and payment processors in which the payment processor, who is a deposit customer of the financial institution, uses its relationship to process payments for third-party merchant clients. Payment processors typically process payments either by creating and depositing remotely created checks (RCCs) often referred to as “Demand Drafts” or by originating Automated Clearing House (ACH) debits on behalf of their merchant customers. The payment processor may use its own deposit account to process such transactions, or it may establish deposit accounts for its merchant clients.

While payment processors generally effect legitimate payment transactions for reputable merchants, the risk profile of such entities can vary significantly depending on the make-up of their customer base. For example, payment processors that deal with telemarketing and online merchants¹ may have a higher risk profile because such entities have tended to display a higher incidence of consumer fraud or potentially illegal activities than some other businesses. Given this variability of risk, payment processors must have effective processes for verifying their merchant clients’ identities and reviewing their business practices. Payment processors that do not have such processes can pose elevated money laundering and fraud risk for financial institutions, as well as legal, reputational, and compliance risks if consumers are harmed.

Financial institutions should understand, verify, and monitor the activities and the entities related to the account relationship. Although all of the core elements of managing third-party risk should be considered in payment processor relationships (e.g., risk assessment, due diligence, and oversight), managing this risk poses an increased challenge for the financial institution when there may not be a direct customer relationship with the merchant. For example, it may be difficult to obtain necessary information from the payment processor, particularly if a merchant is also a payment processor, resulting in a “nested” payment processor or “aggregator” relationship.

Financial institutions should ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner. These agreements should also protect financial institutions by providing for immediate account closure, contract termination, or similar action, as well as establishing adequate reserve requirements to cover anticipated charge backs. Accordingly, financial institutions should perform due diligence and account monitoring appropriate to the risk posed by the payment processor and its merchant

¹ Examples of telemarketing, online businesses, and other merchants that may have a higher incidence of consumer fraud or potentially illegal activities or may otherwise pose elevated risk include credit repair services, debt consolidation and forgiveness programs, online gambling-related operations, government grant or will-writing kits, payday or subprime loans, pornography, online tobacco or firearms sales, pharmaceutical sales, sweepstakes, and magazine subscriptions. This list is not all-inclusive.

base. Risks associated with this type of activity are further increased if neither the payment processor nor the financial institution performs adequate due diligence on the merchants for which payments are originated. Financial institutions are reminded that they cannot rely solely on due diligence performed by the payment processor. The FDIC expects a financial institution to adequately oversee all transactions and activities that it processes and to appropriately manage and mitigate operational risks, Bank Secrecy Act (BSA) compliance, fraud risks, and consumer protection risks, among others.

Potential Risks Arising from Payment Processor Relationships

Deposit relationships with payment processors expose financial institutions to risks not customarily present in relationships with other commercial customers. These include increased operational, strategic, credit, compliance, and transaction risks. In addition, financial institutions should consider the potential for legal, reputational, and other risks, including risks associated with a high or increasing number of customer complaints and returned items, and the potential for claims of unfair or deceptive practices. *Financial institutions that fail to adequately manage these relationships may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity and, thus, may be liable for such acts or practices.* In such cases, the financial institution and responsible individuals have been subject to a variety of enforcement and other actions. Financial institutions must recognize and understand the businesses and customers with which they have relationships and the liability risk for facilitating or aiding and abetting consumer unfairness or deception under Section 5 of the Federal Trade Commission Act.²

Financial institutions should be alert for payment processors that use more than one financial institution to process merchant client payments or that have a history of moving from one financial institution to another within a short period. Processors may use multiple financial institutions because they recognize that one or more of the relationships may be terminated as a result of suspicious activity.

Financial institutions should also be on alert for payment processors that solicit business relationships with troubled financial institutions in need of capital. In such cases, payment processors will identify and establish relationships with troubled financial institutions because these financial institutions may be more willing to engage in higher-risk transactions in exchange for increased fee income. In some cases, payment processors have also committed to purchasing stock in certain troubled financial institutions or have guaranteed to place a large deposit with the financial institution, thereby providing additional, much-needed capital. Often, the targeted financial institutions are smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

² Under Section 8 of the Federal Deposit Insurance Act, the FDIC has authority to enforce the prohibitions against Unfair or Deceptive Acts or Practices (UDAP) in the Federal Trade Commission Act. UDAP violations can result in unsatisfactory Community Reinvestment Act ratings, compliance rating downgrades, restitution to consumers, and the pursuit of civil money penalties.

Financial institutions also should be alert to an increase in consumer complaints about payment processors and/or merchant clients or an increase in the amount of returns or charge backs, all of which may suggest that the originating merchant may be engaged in unfair or deceptive practices or may be inappropriately obtaining or using consumers' personal account information to create unauthorized RCCs or ACH debits. Consumer complaints may be made to a variety of sources and not just directly to the financial institution. They may be sent to the payment processor or the underlying merchant, or directed to consumer advocacy groups or online complaint Web sites or blogs. Financial institutions should take reasonable steps to ensure they understand the type and level of complaints related to transactions that it processes. Financial institutions should also determine, to the extent possible, if there are any external investigations of or legal actions against a processor or its owners and operators during initial and ongoing due diligence of payment processors.

Financial institutions should act promptly to minimize possible consumer harm, particularly in cases involving potentially fraudulent or improper activities relating to activities of a payment processor or its merchant clients. Appropriate actions include filing a Suspicious Activity Report,³ requiring the payment processor to cease processing for a specific merchant, freezing certain deposit account balances to cover anticipated charge backs, and/or terminating the financial institution's relationship with the payment processor.

Risk Mitigation

Financial institutions should delineate clear lines of responsibility for controlling risks associated with payment processor relationships. Controls may include enhanced due diligence; effective underwriting; and increased scrutiny and monitoring of high-risk accounts for an increase in unauthorized returns, charge backs, suspicious activity, and/or consumer complaints. Implementing appropriate controls for payment processors and their merchant clients can help identify payment processors that process items for fraudulent telemarketers, online scammers, or other unscrupulous merchants and help ensure that the financial institution is not facilitating these transactions. Appropriate oversight and monitoring of these accounts may require the involvement of multiple departments, including information technology, operations, BSA/anti-money laundering (AML), and compliance.

Due Diligence and Underwriting

Financial institutions should implement policies and procedures designed to reduce the likelihood of establishing or maintaining inappropriate relationships with payment processors used by unscrupulous merchants. Such policies and procedures should outline the bank's thresholds for unauthorized returns, the possible actions that can be taken against payment processors that exceed these standards, and methods for periodically reporting such activities to the bank's board of directors and senior management.

³ The U.S. Department of Treasury's Regulation 31 (CFR 103.18) requires that every federally supervised banking organization file a SAR when the institution detects a known or suspected violation of federal law. Part 353 of the FDIC's Rules and Regulations addresses SAR filing requirements and makes them applicable to all state-chartered financial institutions that are not members of the Federal Reserve System.

As part of such policies and procedures, financial institutions should develop a processor approval program that extends beyond credit risk management. This program should include a due diligence and underwriting policy that, among other things, requires a background check of the payment processor, its principal owners, and its merchant clients. This will help validate the activities, creditworthiness, and business practices of the payment processor, as well as identify potential problem merchants. Payment processors may also process transactions for other payment processors, resulting in nested payment processors or aggregator relationships. The financial institution should be aware of these activities and obtain data on the nested processor and its merchant clients. Nested processors and aggregator relationships pose additional challenges as they may be extremely difficult to monitor and control; therefore, risk to the institution is significantly elevated in these cases.

Controls and due diligence requirements should be robust for payment processors and their merchant clients. At a minimum, the policies and procedures should authenticate the processor's business operations and assess the entity's risk level. An assessment should include:

- Identifying the major lines of business and volume for the processor's customers;
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants;
- Reviewing corporate documentation, including independent reporting services and, if applicable, documentation on principal owners;
- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele;⁴
- Determining if the processor re-sells its services to a third party that may be referred to as an agent or provider of "Independent Sales Organization opportunities" or a "gateway arrangement"⁵ and whether due diligence procedures applied to those entities are sufficient;
- Visiting the processor's business operations center;
- Reviewing appropriate databases to ensure that the processor and its principal owners and operators have not been subject to law enforcement actions; and,
- Determining whether any conflicts of interest exist between management and insiders of the financial institution.

⁴ See footnote 1 for examples of potentially high-risk areas.

⁵ An Independent Sales Organization is an outside company contracted to procure new merchant relationships. Gateway arrangements are similar to Internet service providers that sell excess computer storage capacity to third parties, who in turn distribute computer services to other individuals unknown to the provider. The third party would make decisions about who would be receiving the service, although the provider would be responsible for the ultimate storage capacity.

Financial institutions should require that payment processors provide information on their merchant clients, such as the merchant's name, principal business activity, location, and sales techniques. The same information should be obtained if the merchant uses sub-merchants (often called "affiliates"). Additionally, financial institutions should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business. Such verification could include comparing the identifying information with public record, fraud databases, and a trusted third party, such as a consumer reporting agency or consumer advocacy group, and/or checking references from other financial institutions. The financial institution should also obtain independent operational audits of the payment processor to assess the accuracy and reliability of the processor's systems. The more the financial institution relies on the payment processor for due diligence and monitoring of its merchant client without direct financial institution involvement and verification, the more important it is to have an independent review to ensure that the processor's controls are sufficient and that contractual agreements between the financial institution and the third-party payment processor are honored.

Ongoing Monitoring

Financial institutions that initiate transactions for payment processors should implement systems to monitor for higher rates of returns or charge backs and/or high levels of RCCs or ACH debits returned as unauthorized or due to insufficient funds, all of which often indicate fraudulent activity. This would include analyzing and monitoring the adequacy of any reserve balances or accounts established to continually cover charge-back activity.

Financial institutions are required to have a BSA/AML compliance program and appropriate policies, procedures, and processes for monitoring, detecting, and reporting suspicious activity. However, nonbank payment processors generally are not subject to BSA/AML regulatory requirements, and therefore some payment processors are more vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. The FFIEC BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk associated with third-party payment processors. As a result, a financial institution's risk mitigation program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.

Consumer complaints and/or high rates of return may be an indicator of unauthorized or illegal activity. As such, financial institutions should establish procedures for regularly surveying the sources of consumer complaints that may be lodged with the payment processor, its merchant clients or their affiliates, or on publicly available complaint Web sites and/or blogs. This will help the institutions identify processors and merchants that may pose greater risk.

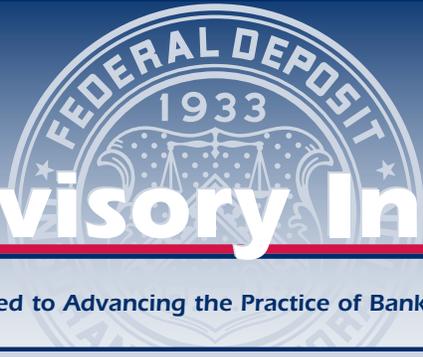
Similarly, financial institutions should have a formalized process for periodically auditing their third-party payment processing relationships; including reviewing merchant client lists and confirming that the processor is fulfilling contractual obligations to verify the legitimacy of its merchant clients and their business practices.

Conclusion

The FDIC recognizes that financial institutions provide legitimate services for payment processors and their merchant clients. However, to limit potential risks, financial institutions should implement risk mitigation policies and procedures that include oversight and controls appropriate for the risk and transaction types of the payment processing activities. At a minimum, Board-approved policies and programs should assess the financial institution's risk tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, determine the character of the payment processor's ownership, and ensure ongoing monitoring of payment processor relationships for suspicious activity, among other things. Adequate routines and controls will include sufficient staffing with the appropriate background and experience for managing third-party payment processing relationships of the size and scope present at the institution, as well as strong oversight and monitoring by the board and senior management. Financial institutions should act promptly if they believe fraudulent or improper activities potentially resulting in consumer harm have occurred related to activities of a payment processor or its merchant clients, in accordance with their duties under BSA/AML policies and procedures, as well as under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts and practices.

Sandra L. Thompson
Director
Division of Risk Management Supervision

Mark Pearce
Director
Division of Depositor and Consumer Protection



Supervisory Insights

Devoted to Advancing the Practice of Bank Supervision

Vol. 8, Issue 1

Summer 2011

Inside

Third-Party Payment
Processor Relationships

Small Business
Administration Lending



Supervisory Insights

Supervisory Insights is published by the Division of Risk Management Supervision of the Federal Deposit Insurance Corporation to promote sound principles and best practices for bank supervision.

Sheila C. Bair
Chairman, FDIC

Sandra L. Thompson
Director, Division of Risk Management Supervision

Journal Executive Board

Division of Risk Management Supervision

George E. French, Deputy Director and Executive Editor

Christopher J. Spoth, Senior Deputy Director

Victor J. Valdez, Deputy Director,
James C. Watkins, Deputy Director

Division of Depositor and Consumer Protection

Sylvia H. Plunkett, Senior Deputy Director

Jonathan N. Miller, Deputy Director

Robert W. Mooney, Deputy Director

Regional Directors

Thomas J. Dujenski, Atlanta Region

Kristie K. Elmquist, Acting Regional Director, Dallas Region

Daniel E. Frye, Acting Regional Director, New York Region

Stan R. Ivie, San Francisco Region

James D. La Pierre, Kansas City Region

M. Anthony Lowe, Chicago Region

Journal Staff

Kim E. Lowry
Managing Editor

Jane Coburn
Financial Writer

Estela R. Gauna
Financial Writer

Supervisory Insights is available online by visiting the FDIC's Web site at www.fdic.gov. To provide comments or suggestions for future articles, request permission to reprint individual articles, or request print copies, send an e-mail to SupervisoryJournal@fdic.gov.

The views expressed in *Supervisory Insights* are those of the authors and do not necessarily reflect official positions of the Federal Deposit Insurance Corporation. In particular, articles should not be construed as definitive regulatory or supervisory guidance. Some of the information used in the preparation of this publication was obtained from publicly available sources that are considered reliable. However, the use of this information does not constitute an endorsement of its accuracy by the Federal Deposit Insurance Corporation.

Issue at a Glance

Volume 8, Issue 1

Summer 2011

Letter from the Director 2

Articles

Managing Risks in Third-Party Payment Processor Relationships 3

An increasing number of financial institutions are entering deposit relationships with third-party payment processors that effect payment transactions for merchant clients. This activity can expose institutions to risks not present in other commercial customer relationships. This article explains the role of third-party payment processors, identifies warning signs that may indicate heightened risk in a payment processor relationship, and discusses the controls that should be in place to manage this risk.

Regular Features

From the Examiner's Desk: SBA Lending: Insights for Lenders and Examiners 13

The FDIC encourages banks to lend to credit-worthy small businesses. The guaranty that accompanies a Small Business Administration (SBA) loan is increasingly attractive to banks looking to expand lending opportunities. Banks that wish to participate in SBA lending programs need to develop specialized expertise. This article reviews the SBA products lenders most often use and provides useful information for institutions about the technical requirements for underwriting, servicing, risk grading, liquidating and selling SBA loans. The article also provides information that may be helpful for examiners when reviewing bank SBA loan portfolios.

Regulatory and Supervisory Roundup 25

This feature provides an overview of recently released regulations and supervisory guidance.

Letter from the Director

As the economic recovery continues to take hold across the country, many banks are exploring ways to increase revenues and expand small business lending. Lending programs offered by the Small Business Administration (SBA) provide an opportunity for banks to lend to small businesses while benefiting from an SBA guaranty. “SBA Lending: Insights for Lenders and Examiners” provides useful information for institutions interested in participating in the SBA program. This article describes the technical underwriting, servicing, and liquidation requirements associated with SBA loan products and provides helpful information for examiners when reviewing bank SBA loan portfolios.

An increasing number of financial institutions are entering into deposit relationships with third-party payment processors that effect payment transactions for merchant clients. As described in “Managing Risks in Third-Party Payment Processor Relationships,” this activity can expose institutions to risks not present in other commercial customer relationships. This article explains the role of third-party payment processors, identifies warning signs that may indicate heightened risk in a payment processor relationship, and discusses the controls that

should be in place to manage this risk. The article concludes with an overview of supervisory remedies that may be used when it is determined a financial institution does not have an adequate program to monitor and mitigate the risks.

We hope you find the articles in this issue to be informative and useful. We encourage our readers to provide feedback and suggest topics for future issues. Please e-mail your comments and suggestions to SupervisoryJournal@fdic.gov.

Sandra L. Thompson
Director
Division of Risk Management
Supervision

Managing Risks in Third-Party Payment Processor Relationships

During the past few years, the Federal Deposit Insurance Corporation (FDIC) has observed an increase in the number of deposit relationships between financial institutions and third-party payment processors and a corresponding increase in the risks associated with these relationships. Deposit relationships with payment processors can expose financial institutions to risks not present in typical commercial customer relationships, including greater strategic, credit, compliance, transaction, legal, and reputation risk. It was for this reason in 2008 that the FDIC issued *Guidance on Payment Processor Relationships* which outlines risk mitigation principles for this type of higher-risk activity.¹

Although many payment processors effect legitimate payment transactions for a variety of reputable merchants, an increasing number of processors have been initiating payments for abusive telemarketers, deceptive online merchants, and organizations that engage in high risk or illegal activities. In the absence of adequate monitoring systems and controls, a financial institution could be facilitating unauthorized transactions or unfair or deceptive practices resulting in financial harm to the consumer. Therefore, it is essential that financial institutions and examiners recognize and understand the risks associated with these relationships.

This article explains the role of third-party payment processors and the risks they can present to financial institutions, identifies warning signs that may indicate heightened risk in a payment processor relationship, and discusses the risk mitigation controls that should be in place to manage this risk. The article concludes with an overview

of supervisory remedies that may be used when it is determined that a financial institution does not have an adequate program in place for monitoring and addressing the risks associated with third-party payment processor relationships.

Background

The core elements of managing third-party risk are present in payment processor relationships (e.g., risk assessment, policies and procedures, due diligence, and oversight). Managing these risks can be particularly challenging as the financial institution does not have a direct customer relationship with the payment processor's merchant clients. Furthermore, the risks associated with this type of activity are heightened when neither the payment processor nor the financial institution performs adequate due diligence, such as verifying the identities and business practices of the merchants for which payments are originated and implementing a program of ongoing monitoring for suspicious activity.

For example, in a typical third-party payment processor relationship, the payment processor is a deposit customer of the financial institution which uses its deposit account to process payments for its merchant clients. The payment processor receives lists of payments to be generated by the merchant clients for the payment of goods or services and initiates the payments by creating and depositing them into a transaction account at a financial institution. In some cases, the payment processor may establish individual accounts at the financial institution in the name

¹ Financial Institution Letter (FIL) 127-2008, *Guidance on Payment Processor Relationships*, dated November 7, 2008. See: <http://www.fdic.gov/news/news/financial/2008/fil08127.html>.

Third-Party Payment Processors

continued from pg. 3

of each merchant client and deposit the appropriate payments into these accounts. The merchant may then be a co-owner of the deposit account and make withdrawals from the account to receive its sales proceeds, or the payment processor may periodically forward the sales proceeds from the account to the merchant. Alternatively, the payment processor may commingle payments originated by the merchant clients into a single deposit account in the name of the payment processor. In this case, the payment processor should maintain records to allocate the deposit account balance among the merchant clients.

Payment Types Used by Third-Party Payment Processors

Payment processors may offer merchants a variety of alternatives for accepting payments including credit and debit card transactions, traditional check acceptance, Automated Clearing House (ACH) debits and other alternative payment channels. The potential for misuse or fraud exists in all payment channels. However, the FDIC has observed that some of the most problematic activity occurs in the origination of ACH debits or the creation and deposit of remotely created checks.

Automated Clearing House Debits

The ACH network is a nationwide electronic payment network which enables participating financial institutions to distribute electronic credit and debit entries to bank accounts and settle these entries.

Common ACH credit transfers include the direct deposit of payroll and certain benefits payments. Direct debit transfers also may be made through the ACH network and include consumer payments for insurance premiums, mortgage loans, and other types of bills. Rules and regulations governing the ACH networks are established by NACHA - The Electronic Payments Association (formerly National Automated Clearing House Association)² and the Board of Governors of the Federal Reserve System.

Third-party payment processors initiate ACH debit transfers as payments for merchant clients by submitting these transfers, which contain the consumer's financial institution routing number and account number (found at the bottom of a check) to their financial institution to enter into the ACH networks. Telemarketers and online merchants obtain this information from the consumer and transmit it to the payment processor to initiate the ACH debit transfers. The risk of fraud arises when an illicit telemarketer or online merchant obtains the consumer's account information through coercion or deception and initiates an ACH debit transfer that may not be fully understood or authorized by the consumer.

As with all payment systems and mechanisms, the financial institution bears the responsibility of implementing an effective system of internal controls and ongoing account monitoring for the detection and resolution of fraudulent ACH transfers. If an unauthorized ACH debit is posted to a consumer's account, the procedures for resolving errors contained in the Federal Reserve Board's Regulation E,

² NACHA establishes the rules and procedures governing the exchange of automated clearinghouse payments. See <http://www.nacha.org/c/achrules.cfm>.

which governs electronic funds transfers,³ provide the consumer 60 days after the financial institution sends an account statement to report the unauthorized ACH debit.⁴ Regulation E requires the consumer's financial institution to investigate the matter and report to the consumer the results of the investigation within a prescribed time frame. In the case of an ACH debit, when a consumer receives a refund for an unauthorized debit, ACH rules permit the consumer's financial institution to recover the amount of the unauthorized payment by returning the debit item to the originating financial institution.

Remotely Created Checks

Remotely Created Checks (RCCs), often referred to as "demand drafts," are payment instruments that do not bear the signature of a person on whose account the payments are drawn. In place of the signature, the RCC bears the account holder's printed or typed name, or a statement that the account holder's signature is not required or the account holder has authorized the issuance of the check. Similar to the initiation of an ACH debit transfer, an account holder authorizes the creation of an RCC by providing his financial institution's routing number and his account number. Examples of RCCs are those created by a credit card or utility company to make a payment on an account, or those initiated by telemarketers or online merchants to purchase goods or services.

The risk of fraud associated with RCCs is often greater than the risk associated with other kinds of debits that post to transaction accounts. For example, an illicit payment originator might obtain a consumer's account information by copying it from an authorized check or misleading the consumer into providing the information over the telephone or the Internet. Once the necessary information is obtained, the payment originator can generate unauthorized RCCs and forward them for processing. Similar to the responsibilities associated with the ACH network, the financial institution should implement an effective system of internal controls and account monitoring to identify and resolve the unauthorized RCC.

RCCs may be processed as a paper item through the customary clearing networks or converted to and processed as an ACH debit. However, check clearing and ACH rules differ as to the re-crediting of an accountholder for an unauthorized RCC and how losses are allocated by and between the participating financial institutions. RCCs processed as checks are governed by provisions of the Uniform Commercial Code (UCC) and the Expedited Funds Availability Act,⁵ as implemented by Regulation CC. RCCs converted to ACH debits are governed by applicable ACH rules, the Electronic Fund Transfer Act, and Regulation E.

In response to heightened concern about the risk of fraud, in 2005 the Federal Reserve amended Regulation CC to transfer the liability for losses

³ Provisions of the Federal Reserve Board's Regulation E establish the rights, liabilities, and responsibilities of participants in electronic fund transfer systems, such as automated teller machine transfers, telephone bill-payment services, point-of-sale terminal transfers, and preauthorized transfers from or to a consumer's account.

⁴ 12 CFR Section 205.11.

⁵ The Expedited Funds Availability Act (EFAA), enacted in 1987, addresses the issue of delayed availability of funds by banks. The EFAA requires banks to (1) make funds deposited in transaction accounts available to customers within specified time frames, (2) pay interest on interest-bearing transaction accounts not later than the day the bank receives credit, and (3) disclose funds-availability policies to customers.

Third-Party Payment Processors

continued from pg. 5

resulting from unauthorized RCCs.⁶ At the same time, the Board also amended Regulation J (the Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire) to clarify that certain warranties, similar to those provided under the UCC, apply to RCCs collected through the Reserve Banks. In conjunction with Regulation CC, the amendments to Regulation J shifted the liability for losses attributed to unauthorized RCCs to the financial institution where the check is first deposited as this institution is in the best position to know its customer (the creator of the RCC) and determine the legitimacy of the deposits. The liability also creates an economic incentive for depository institutions to perform enhanced due diligence on those customers depositing RCCs. Furthermore, by providing the paying financial institution with the ability to recover against the financial institution presenting the unauthorized RCC, these regulatory changes should make it easier for customers to obtain re-credits.⁷

Types of High Risk Payments

Although many clients of payment processors are reputable merchants, an increasing number are not and should be considered “high risk.” These disreputable merchants use payment processors to charge consumers for

questionable or fraudulent goods and services. Often a disreputable merchant will engage in high pressure and deceptive sales tactics, such as aggressive telemarketing or enticing and misleading pop-up advertisements on Web sites. For example, consumers should be cautious when Web sites offer “free” information and ask consumers to provide payment information to cover a small shipping and handling fee. In some instances and without proper disclosure, consumers who agreed to pay these fees, often found their bank accounts debited for more than the fee and enrolled in costly plans without their full understanding and consent.⁸ Still other disreputable merchants will use processors to initiate payments for the sale of products and services, including, but not limited to, unlawful Internet gambling and the illegal sale of tobacco products on the Internet.

Generally, high-risk transactions occur when the consumer does not have a familiarity with the merchant, or when the quality of the goods and services being sold is uncertain. Activities involving purchases made over the telephone or on the Internet tend to be riskier in that the consumer cannot fully examine or evaluate the product or service purchased. Similarly, the consumer may not be able to verify the identity or legitimacy of the person or organization making the sale.

⁶ Effective July 1, 2006 [70 Fed. Reg. 71218-71226 (November 28, 2005)].

⁷ Changes to Federal Reserve Bank Operating Circular No. 3 on the Collection of Cash Items and Returned Checks clarifies that electronically created images (including RCC items) that were not originally captured from paper are not eligible to be processed as Check 21 items (effective July 15, 2008), www.frbsservices.org/files/regulations/pdf/operating_circular_3.pdf.

⁸ Rules governing the use of telemarketing require verifiable authorization of payment for services. See the Federal Trade Commission Telemarketing Sales Rule [16 CFR 310]. See: <http://www.ftc.gov/os/2002/12/tsrfinalrule.pdf>.

Some merchant categories that have been associated with high-risk activity include, but are not limited to:

- Ammunition Sales
- Cable Box De-scramblers
- Coin Dealers
- Credit Card Schemes
- Credit Repair Services
- Dating Services
- Debt Consolidation Scams
- Drug Paraphernalia
- Escort Services
- Firearms Sales
- Fireworks Sales
- Get Rich Products
- Government Grants
- Home-Based Charities
- Life-Time Guarantees
- Life-Time Memberships
- Lottery Sales
- Mailing Lists/Personal Info
- Money Transfer Networks
- On-line Gambling
- PayDay Loans
- Pharmaceutical Sales
- Ponzi Schemes
- Pornography
- Pyramid-Type Sales
- Racist Materials
- Surveillance Equipment
- Telemarketing
- Tobacco Sales
- Travel Clubs

Of particular concern, the FDIC and other federal regulators have seen an increase in payment processors initiating payment for online gaming activities that may be illegal. The Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) prohibits financial institutions from accepting payments from any person engaged in the business of betting or wagering with a business in unlawful Internet gambling (see the FDIC's Financial Institution Letter on the *Unlawful Internet Gambling Enforcement Act*, FIL-35-2010, dated June 30, 2010).⁹

High-Risk Payment Processor Relationship Warning Signs

Financial institutions and examiners should be aware of the warning signs that may indicate heightened risk in a payment processor relationship. One of the more telling signs is a high volume of consumer complaints that suggest a merchant client is inappropriately obtaining personal account information; misleading customers as to the quality, effectiveness, and usefulness of the goods or services being offered; or misstating the sales price or charging additional and sometimes recurring fees that are not accurately disclosed or properly authorized during the sales transaction. However, this may be somewhat difficult to determine in that it may be almost

⁹ 12 CFR Part 233 – Regulation GG, Financial Institution Letter (FIL) 35-2010, *Unlawful Internet Gambling Enforcement Act*, dated June 30, 2010. See <http://www.fdic.gov/news/news/financial/2010/fil10035.html>.

Third-Party Payment Processors

continued from pg. 7

impossible for financial institutions and examiners to know if consumers are submitting complaints directly to the payment processor or the merchants. One way financial institutions and examiners can determine if consumers are making complaints or voicing their dissatisfaction is to review certain Web sites, such as those for regional Better Business Bureaus, or blogs intended to collect and share such information to alert other consumers.

Financial institutions with third-party payment processor relationships should consider monitoring the Internet for complaints that mention them by name. The financial institution's name typically appears on the face of a RCC or in the record of an ACH debit. As a result, consumers often associate the financial institution with the transaction and may complain about the institution facilitating the payment. Complaints also may be lodged with the depository financial institution by the financial institution of the consumer whose account was charged. As required by statute and federal regulation, the depository financial institution must acknowledge, research, and respond to each complaint made directly to them.

Another indication of the potential for heightened risk in a payment processor relationship is a large number of returns or charge backs. Consumers who are dissatisfied with goods or services delivered or provided, or consumers who feel they were deceived or coerced into providing their account information, can request their financial institution return the RCC or ACH debit to the depository financial institution as an unauthorized transaction. In addition, items may be returned if insufficient funds are available to cover the unauthorized items, resulting in the consumer's account being overdrawn. In these circumstances, the items

often are returned as "NSF" rather than as "unauthorized." Accordingly, financial institutions with payment processor relationships should implement systems to monitor for higher rates of returns or charge backs, which can be evidence of fraudulent activity.

Another warning sign is a significant amount of activity which generates a higher than normal level of fee income. In an increasingly competitive market place, financial institutions are looking for ways to grow non-interest fee income, and this is especially true for troubled institutions. Although fee income from third-party payment processor relationships may benefit an institution's bottom line, it can indicate an increased level of risk. Side agreements may be established between payment processors and financial institutions, whereby the payment processor pays the institution a fee for each item deposited, generating a higher level of fee income. However, the greatest source of income from these relationships tends to be returned item fees. Financial institutions routinely charge deposit customers a fee for each returned item. Because payment processors may generate a high volume of returned items, the fee income associated with this activity is typically much higher.

As a caveat, financial institutions and examiners should be alert for payment processors that use more than one financial institution to process merchant client payments, or nested arrangements where a payment processor's merchant client is also doing third-party payment processing. Spreading the activity among several institutions may allow processors that engage in inappropriate activity to avoid detection. For example, a single institution may not detect high levels of returned items if they are spread among several financial institutions.

Payment processors also may use multiple financial institutions in case one or more of the relationships is terminated as a result of suspicious activity.

Finally, another troubling development is payment processors that purposefully solicit business relationships with troubled institutions in need of capital. Payment processors identify and establish relationships with troubled institutions as these institutions may be more willing to engage in higher-risk transactions in return for increased fee income. In some cases, payment processors have made a commitment to purchase stock in certain troubled financial institutions or guarantee to retain a large deposit with the institution, thereby providing additional, needed capital. Often, the targeted financial institutions are smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

Risk Controls

A framework for prudently managing relationships with third-party payment processors was communicated in the FDIC's 2008 *Guidance on Payment Processor Relationships*.¹⁰ Financial institutions in relationships with payment processors should establish clear lines of responsibility for controlling the associated risks. Such responsibilities include effective due diligence and underwriting, as well as ongoing monitoring of high-risk accounts for an increase in unauthorized returns and suspicious

activity and maintenance of adequate balances or reserves to cover expected high levels of returned items. The relationship should be governed by a written contract between the financial institution and the third-party payment processor which outlines each party's duties and responsibilities. Implementing appropriate and effective controls over payment processors and their merchant clients will help identify those processors working with fraudulent telemarketers or other unscrupulous merchants and help ensure the financial institution does not facilitate such transactions.

Due Diligence and Underwriting

Due diligence and prudent underwriting standards are critical components of a risk mitigation program. Financial institutions should implement policies and procedures that reduce the likelihood of establishing or maintaining a relationship with payment processors through which unscrupulous merchants can access customers' deposit accounts.

Financial institutions that initiate transactions for payment processors should develop a processor approval program that extends beyond credit risk management. This program should incorporate an effective due diligence and underwriting policy that, among other things, requires background checks of payment processors and merchant clients. A processor approval program will help validate the activities, creditworthiness, and business practices of the payment processor and should, at a minimum,

¹⁰ Financial Institution Letter (FIL) 127-2008, *Guidance on Payment Processor Relationships*, November 7, 2008, <http://www.fdic.gov/news/news/financial/2008/fil08127.html>.

Third-Party Payment Processors

continued from pg. 9

authenticate the processor's business operations and assess the entity's risk level. Any processor assessment should include:

- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele.
- Determining if the processor re-sells its services to "Independent Sales Organizations" (companies contracted to procure new merchant relationships) or through "gateway arrangements" (selling excess capacity to third parties, which in turn sell services to other individuals unknown to the payment processor).
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants.
- Identifying the major lines of business and volume for the processor's customers.
- Determining whether the institution maintains appropriate balances or reserves for each individual merchant based on the type of client and the risk involved in the transactions processed and the expected volume of returned items.
- Reviewing corporate documentation, obtaining information on the processor from independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.
- Requesting copies of consumer complaints and the procedures for handling consumer complaints and redress.
- Obtaining information pertaining to any litigation and actions brought by federal, state, or local regulatory or enforcement agencies.
- Obtaining information about the history of returned items and customer refunds.

Financial institutions should require the payment processor to provide information on its merchant clients, such as the merchant's name, principal business activity, geographic location, and sales techniques. Additionally, financial institutions should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business. Such verification could include comparing the identifying information with public record, fraud databases and a trusted third party, such as a credit report from a consumer reporting agency or the state Better Business Bureau, or checking references from other financial institutions.

Ongoing Monitoring

Financial institutions are required to have a Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program and appropriate policies, procedures, and processes in place for monitoring, detecting, and reporting suspicious activity.¹¹ However, non-bank payment processors generally are not subject to BSA/AML regulatory requirements and, therefore, some payment processors may be vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. The Federal Financial Institutions Examination Council BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk with respect to third-party payment processors. As a result, a financial institution's risk mitigation program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.¹²

Appropriate Supervisory Responses

In those instances where examiners determine that a financial institution fails to have an adequate program in place to monitor and address risks associated with third-party payment processor relationships, formal or informal enforcement actions may

be appropriate. Formal actions have included Cease and Desist Orders under Section 8(b) or 8(c) of the *Federal Deposit Insurance (FDI) Act*, as well as assessment of Civil Money Penalties under Section 8(i) of the FDI Act. These orders have required the financial institution to immediately terminate the high-risk relationship and establish reserves or funds on deposit to cover anticipated charge backs.

As appropriate, the examiner will determine if financial institution management has knowledge that the payment processor or the merchant clients are engaging in unfair or deceptive practices in violation of Section 5 of the Federal Trade Commission Act. In those cases where a financial institution does not conduct due diligence, accepts a heightened level of risk, and allows transactions for high-risk merchants to pass through it, it may be determined that the financial institution is aiding and abetting the merchants. This also could indicate a disregard for the potential for financial harm to consumers and, as a result, the financial institution may be subject to civil money penalties or required to provide restitution.

¹¹ Banks, bank holding companies, and their subsidiaries are required by federal regulations to file a Suspicious Activity Report if they know, suspect, or have reason to suspect the transaction may involve potential money laundering or other illegal activity, is designed to evade the Bank Secrecy Act or its implementing regulations, has no business or apparent lawful purpose, or is not the type of transaction in which particular customer would normally be expected to engage. See 12 CFR 353 (http://www.ffiec.gov/bsa_aml_infobase/pages_manual/regulations/12CFR353.htm) and 31 CFR 103.18 (http://www.ffiec.gov/bsa_aml_infobase/pages_manual/regulations/31CFR103.pdf.)

¹² See "Third-Party Payment Processors—Overview," from the Bank Secrecy Act/Anti-Money Laundering Examination Manual, http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm.

Third-Party Payment Processors

continued from pg. 11

Conclusion

Deposit relationships with payment processors expose financial institutions to risks that may not be present in relationships with other commercial customers. To limit potential risks, financial institutions should implement risk mitigation policies and procedures that include appropriate oversight and controls commensurate with the risk and complexity of the activities. At a minimum, risk mitigation programs should result in the financial institution assessing its risk tolerance for this type of activity, verifying the legitimacy of the payment processor's business operations, and monitoring payment processor relationships for suspicious activity.

Financial institutions should act promptly if they believe fraudulent or improper activities have occurred related to a payment processor's activities. Appropriate actions may include filing a Suspicious Activity Report, requiring the payment processor to cease processing for that specific merchant, or terminating the financial institution's relationship with the payment processor. Should it be determined that a financial institution

does not have an adequate program in place to monitor and address the risks associated with third-party payment processor relationships, an appropriate supervisory response will be used to require the financial institution to correct the deficiencies.

Michael B. Benardo

*Chief, Cyber-Fraud and
Financial Crimes Section
Division of Risk Management
Supervision
mbenardo@fdic.gov*

Kathryn M. Weatherby

*Examination Specialist
(Fraud)
Cyber-Fraud and Financial
Crimes Section
Division of Risk Management
Supervision
kweatherby@fdic.gov*

Robert J. Wirtz

*Assistant Regional Director
(Compliance)
Division of Depositor and
Consumer Protection
rwirtz@fdic.gov*