July 15, 2026

Testimony of
Dr. David Maimon

On Behalf of

SentiLink

Before the

United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on Government Operations

Hearing entitled

"Emerging Fraud Threats and the Evolving Fraud Landscape"

Chairman Sessions, Ranking Member Mfume and Members of the Subcommittee, thank you for having me here today to discuss an issue of critical importance to the federal government and American taxpayers: fraud. I serve as the Head of Fraud Insights at SentiLink[1] and as a Professor in the Department of Criminal Justice and Criminology at Georgia State University. For nearly two decades, my research has focused on cybercrime and online fraud, examining the behavior of cybercriminals and the effectiveness of interventions designed to prevent and disrupt online crime. My work has explored topics including hacking, online child exploitation, darknet marketplaces, fraud ecosystems, identity theft, and the evolving underground economy that enables financial crime.

A central question has guided my research throughout my career: What works -- and what does not -- in preventing and disrupting cybercrime? To answer this question, my teams collect data directly from the online environments where cybercrime occurs. Rather than relying solely on victim reports or law enforcement records, we study offenders, targets, guardians, and the infrastructure that connects them in the wild. This has involved deploying experimental systems such as honeypots (i.e. computers which are designed to allow hackers access to them) to observe hacker behavior on attacked computer systems[2], developing conversational agents to study online grooming[3], and infiltrating criminal marketplaces to understand how fraud operations function in practice[4].

Today, much of my work focuses on both the domestic and global online fraud ecosystems. My team conducts continuous intelligence collection across darknet marketplaces, Telegram channels, encrypted messaging platforms, and other online communities where fraudsters buy, sell, and exchange stolen identities, counterfeit documents, compromised financial accounts, stolen checks, payment credentials, and fraud-enabling services. These communities also serve as hubs where offenders share operational guidance, recruit collaborators, and discuss emerging techniques.

In addition to collecting intelligence from online fraud ecosystems, I regularly conduct field investigations across the United States to better understand the physical infrastructure that enables fraud. This work takes me to cities throughout the country, where I visit addresses associated with suspected fraud activity, including commercial mail receiving agencies (CMRAs), virtual office locations, residential addresses, home healthcare companies, shell businesses, and other entities linked to fraudulent operations. These on-the-ground

---

[1] SentiLink provides identity verification, fraud mitigation and risk management solutions to US-based financial institutions, telecom providers, educational institutions, government agencies and others. Using human-supervised machine learning models informed by the industry's best risk analysts, our tools enable institutions and individuals to transact confidently with one another by preventing identity fraud at the point that a consumer is applying for any type of service or account. SentiLink was also the first company in history to use the Social Security Administration's Electronic Consent Based SSN Verification service ("eCBSV") to validate account application data, and was the first to integrate with the Treasury Department's Treasury Check Verification System ("TCVS") API. Each day we help verify the identity of over 3,000,000 consumers, and in doing so prevent approximately 100,000 cases of identity fraud daily. We were founded in 2017 and have more than 150 employees based out of our San Francisco headquarters and satellite offices in Los Angeles, Denver, Chicago, Austin, San Ramon and New York.

[2] Maimon et al 2014; Fisher et al 2022.

[3] See, for example, Kamar et al 2025 2024.

[4] Maymoni et al 2026; Kaur et al 2026; Ouellet et al 2022.

investigations allow me to validate intelligence gathered online, identify patterns that cannot be observed through data alone, and better understand how criminal organizations establish legitimacy and sustain fraud at scale.

By combining online intelligence with field verification, I am able to connect digital indicators to real-world operations, generating insights that are both analytically rigorous and operationally relevant for financial institutions, government agencies, and fraud investigators.

This research has helped identify numerous fraud trends before they became widely recognized, including the growth of pandemic unemployment benefit fraud, the industrialization of mail theft and check fraud, the commercialization of synthetic identities, AI-enabled identity attacks, travel fraud, healthcare fraud, and the increasing use of dormant and abandoned identities in financial crime. The objective of this work is not simply to document criminal activity, but to understand how fraud operations evolve and how organizations can better detect and disrupt them.

Note that most of the visual evidence presented in this testimony I have collected from online darkweb and clearnet sites, directly from the fraudsters themselves.

In my testimony, I will first walk through some of the more notable fraud trends my team and I are currently tracking across federal benefit and reimbursement programs, including:

- Theft and forgery of U.S. Treasury checks;
- AI- and deepfake-enabled tax refund fraud;
- Theft and resale of SNAP/EBT benefits;
- Medicare and Medicaid beneficiary fraud;
- Federal student aid fraud, and;
- Fraudulent Small Business Administration loan schemes.

I then identify the cross-cutting patterns connecting these trends, and close with the priorities I believe the federal government should act on to disrupt this infrastructure before it produces further losses.

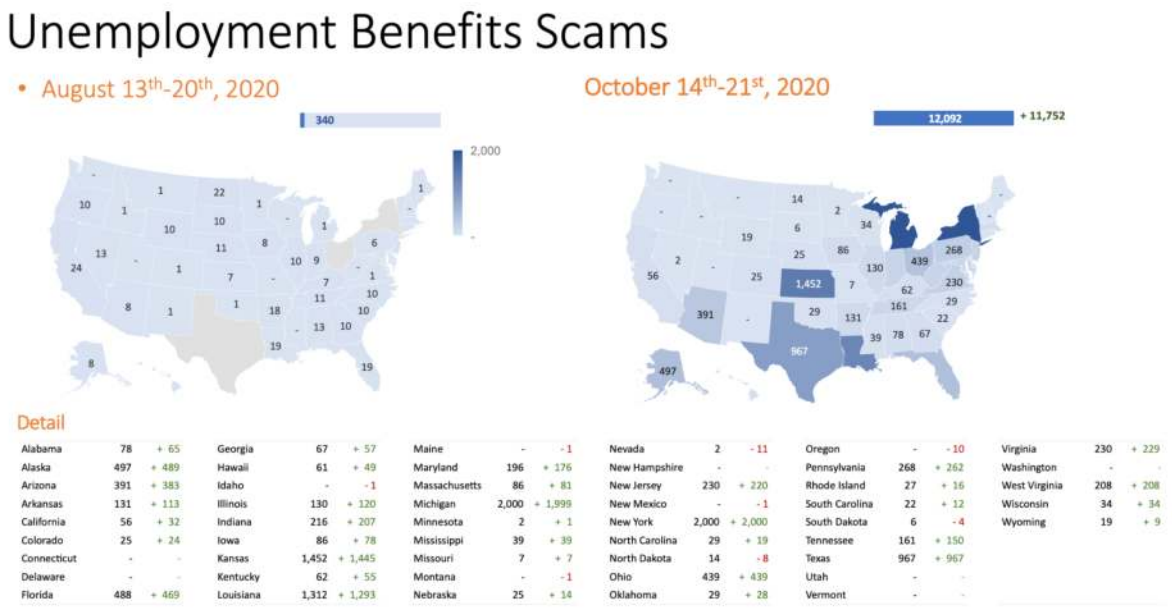
Notable Fraud Trends Observed within the Online Fraud Ecosystem

Background

The COVID-19 pandemic marked one of the first times researchers, investigators, and government agencies could observe -- nearly in real time -- how fraud against federal programs developed and spread across online fraud ecosystems. On Telegram channels, darknet markets, social media groups, and other online platforms, fraudsters openly exchanged instructions, sold stolen identities, advertised application services, recruited money mules, and shared methods for exploiting programs such as unemployment insurance, the Paycheck Protection Program, and Economic Injury Disaster Loans. These online communities allowed

successful techniques to spread rapidly, transforming what might once have been isolated fraud attempts into repeatable and scalable criminal operations.

For example, to better understand the spread of unemployment benefit fraud in 2020, my team and I documented Telegram posts that showed successful fraudulent applications, advertised fraud services, or provided tutorials for exploiting unemployment programs in different states. We examined activity during one week in August and one week in October and created a visual showing how rapidly this fraud expanded across the country. During the week of August 13, 2020, we identified approximately 340 posts related to unemployment benefit fraud. By the week of October 14, 2020, that number had increased to more than 12,000 posts. These findings demonstrate the important role Telegram played in accelerating the dissemination of fraud techniques and supporting the nationwide expansion of unemployment benefit fraud during the pandemic. Furthermore, this exercise demonstrates the value of monitoring social media platforms to identify and track emerging fraud trends across the online fraud ecosystem.



Geographic Distribution of Telegram Unemployment Benefit Fraud Advertisements, August and October 2020

Importantly, the pandemic did not create fraud against government programs. Rather, it revealed how vulnerable many programs were when speed of payment was prioritized over identity verification, eligibility controls, and cross-agency data sharing. Organized fraud rings quickly identified these weaknesses and developed services and operational structures designed to exploit them at scale.

The proceeds generated during this period also gave fraud networks the capital to expand their infrastructure. Criminals invested in stolen and synthetic identities, shell companies, fraudulent documents, bank accounts, money-mule networks, virtual mailboxes, compromised credentials, and specialized cash-out services. Online fraud ecosystems increasingly supported a division of

labor in which different actors supplied identities, prepared applications, opened accounts, moved funds, and converted fraudulent proceeds into usable assets.

That infrastructure did not disappear when pandemic-relief programs ended. It remains active and is now being redirected toward other areas of government spending, including Supplemental Nutrition Assistance Program (SNAP), Medicaid, Medicare, student aid, tax refunds, unemployment benefits, and SBA government-backed loans. Below, I describe several of the key fraud trends targeting government benefit and reimbursement programs that my teams and I are currently monitoring.

Treasury Check Fraud

In 2021, I warned the American public that check theft and check fraud were rapidly increasing[5]. At the time -- and continuing today -- we observed organized domestic criminal groups targeting USPS collection boxes, stealing mail in search of checks, altering them, and cashing them, resulting in millions of dollars in losses for consumers, financial institutions, and the U.S. government. Many of the stolen checks we observed were U.S. Department of the Treasury checks issued to taxpayers as tax refunds or government benefit payments.

Freshly Stolen and Altered U.S. Department of the Treasury Checks Observed on Telegram One Week Before this Testimony

Recognizing the scale of this problem, the U.S. Department of the Treasury announced that it would phase out the use of paper checks by September 2025. Since then, we have observed a substantial decline in the number of Treasury checks being advertised for sale on online fraud marketplaces hosted on social media platforms. However, criminals continue to intercept, forge, and traffic Treasury checks. In addition, we are increasingly observing personal checks mailed by taxpayers to the IRS to pay their federal taxes being stolen and offered for sale within these same criminal ecosystems.

The risks associated with stolen checks extend well beyond check fraud itself. A recent study my colleagues and I published demonstrates a direct relationship between the volume of stolen checks observed in a state and subsequent levels of identity theft in that state[6]. Stolen checks provide

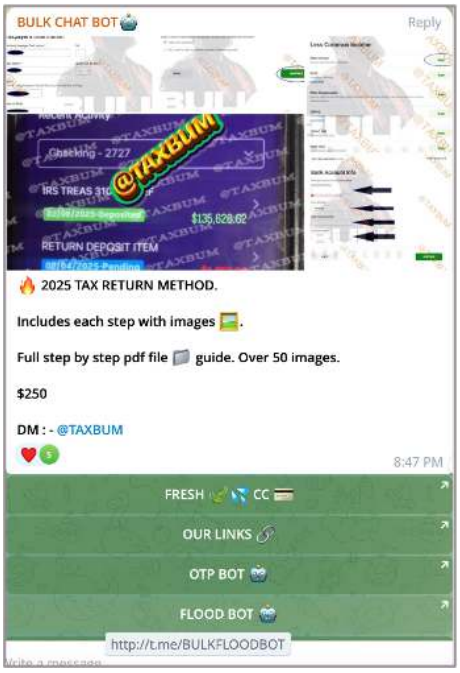
[5] Maimon 2022.
[6] Maimon et al., 2026.

criminals with far more than access to funds -- they contain valuable personally identifiable information that can be repurposed to facilitate identity theft, account takeover, and a wide range of additional fraud targeting governmental reimbursement and benefit programs.

Tax Refund Fraud

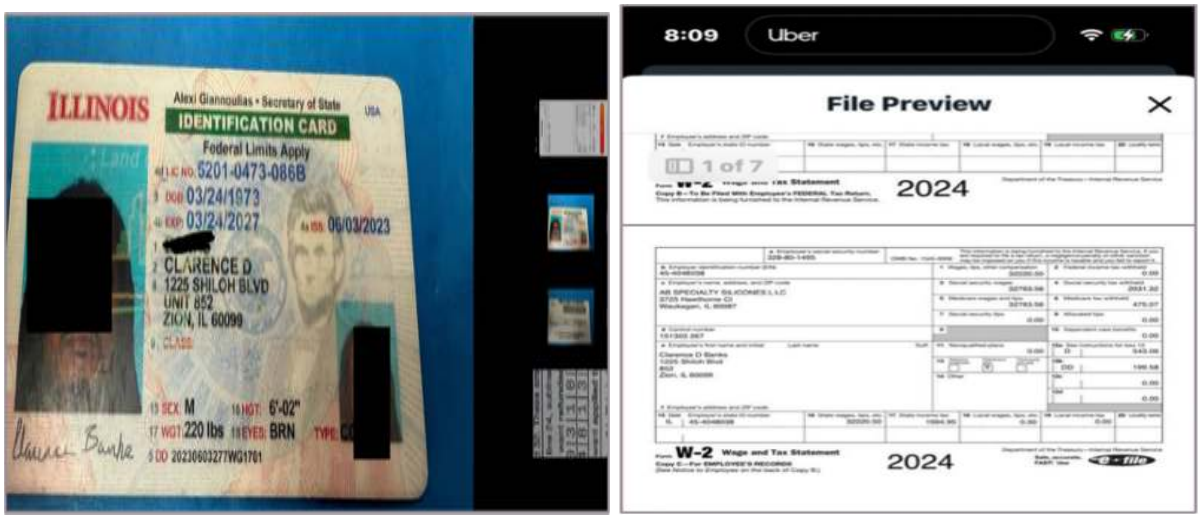
A second trend we are observing is the increasing use of artificial intelligence and deepfake technology to facilitate tax refund fraud. Traditionally, tax refund fraud involved criminals using stolen or synthetic identities to file fraudulent tax returns before legitimate taxpayers could do so. To facilitate this crime, many fraudsters post detailed tutorials of how to bypass many of the verification solutions which are used by the IRS to detect fraud. Reading through these tutorials suggests that these schemes have become far more sophisticated than they were four years ago, prior to proliferation of online fraud markets and the infiltration of Artificial Intelligence to the online fraud ecosystem. Fraudsters are now combining stolen identities with AI-generated faces and deepfake videos to defeat identity verification controls used by tax preparation services and financial institutions.

Our research has shown that these attacks often follow a well-defined sequence. Criminals first purchase stolen identities from online fraud marketplaces, where complete identity packages can cost only a few dollars. They then create brand-new email accounts and open checking accounts -- very often at digital banks -- in the victim's name. Those accounts serve as the destination for fraudulent tax refunds. When additional identity verification is required, fraudsters generate AI-created driver's licenses and use deepfake software to produce convincing "live" videos that can bypass liveness checks during remote onboarding. These videos are often created using readily available software such as OBS Studio together with face-swapping tools, allowing criminals to impersonate victims in real time.



Full tutorials on defrauding the IRS

Importantly, this trend demonstrates that the threat is no longer limited to stolen identities alone. Criminals are now building complete synthetic digital personas around those identities, enabling them to defeat verification systems that were designed to stop traditional identity theft. As AI technology continues to improve, government agencies and financial institutions should place greater emphasis on signals that criminals cannot easily fabricate -- such as historical identity attributes, authoritative data sources, and behavioral patterns -- rather than relying solely on document verification or biometric matching.



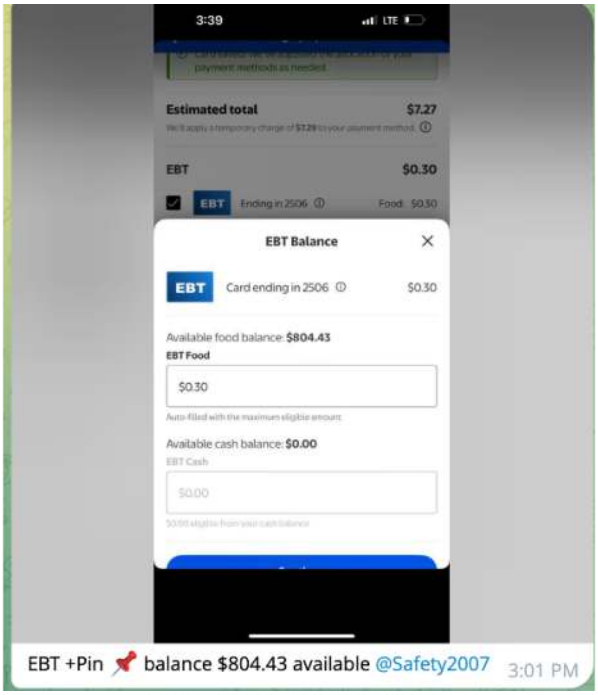
Examples of tax refund fraud packages sold on dark web

AI-Generated Fraud Identities: This individual does not exist and was created using commonly available generative AI tools. Darkweb-marketed tools created the fake driver's license, and AI was used to integrate the two and can even animate them to pass a liveness check.

<u>Supplemental Nutrition Assistance Program (SNAP) Fraud</u>

Another trend my teams and I have observed is the emergence of an online marketplace for stolen Supplemental Nutrition Assistance Program benefits. Criminals obtain recipients' Electronic Benefit Transfer information through card skimming (see image on the right), phishing, account compromise, and

potentially data breaches. They then advertise the stolen account information through Telegram channels, social media, messaging boards, and darknet markets, where buyers can purchase access to benefits belonging to vulnerable households.



EBT Cards and Balances

```
507680  ALABAMA EBT ISSUED BY EFUNDS  DEBIT  PERSONAL  UNITED STATES
507681  COLORADO EBT ISSUED BY JPMORGAN EFS  DEBIT  PERSONAL  UNITED
STATES
507683  MISSOURI EBT ISSUED BY EFUNDS  DEBIT  PERSONAL  UNITED STATES
507700  OHIO EBT ISSUED BY AFFILIATED COMPUTER SERVICES  DEBIT
PERSONAL  UNITED STATES
507707  DISTRICT OF COLUMBIA EBT ISSUED BY JPMORGAN EFS  DEBIT
PERSONAL  UNITED STATES
508147  OKLAHOMA EBT ISSUED BY AFFILIATED COMPUTER SERVICES  DEBIT
PERSONAL  UNITED STATES
508148  GEORGIA EBT ISSUED BY JPMORGAN EFS  DEBIT  PERSONAL  UNITED
STATES
600760  PENNSYLVANIA EBT  DEBIT    UNITED STATES
600875  MARYLAND EBT  DEBIT    UNITED STATES
603953  BLACKHAWK NETWORK  DEBIT  PREPAID  MEXICO
610470  COUTH CAROLINA EBT  DEBIT    UNITED STATES
507680  ALABAMA EBT ISSUED BY EFUNDS  DEBIT  PERSONAL  UNITED STATES
507702  TENNESSEE EBT ISSUED BY JPMORGAN EFS  DEBIT  PERSONAL  UNITED
STATES
507704  INDIANA EBT ISSUED BY JPMORGAN EFS  DEBIT  STANDARD  UNITED
STATES
507711  MICHIGAN EBT  DEBIT    UNITED STATES
600760  PENNSYLVANIA EBT  DEBIT    UNITED STATES
610098  TEXAS EBT ISSUED BY AFFILIATED COMPUTER SERVICES  DEBIT
STANDARD  UNITED STATES
507680  ALABAMA EBT ISSUED BY EFUNDS  DEBIT  PERSONAL  UNITED STATES
507681  COLORADO EBT ISSUED BY JPMORGAN EFS  DEBIT  PERSONAL  UNITED
STATES
507683  MISSOURI EBT ISSUED BY EFUNDS  DEBIT  PERSONAL  UNITED STATES
507693  OREGON EBT ISSUED BY EFUNDS  DEBIT  PERSONAL  UNITED STATES
507695  ALASKA EBT ISSUED BY JPMORGAN EFS  DEBIT  PERSONAL  UNITED
STATES
507700  OHIO EBT ISSUED BY AFFILIATED COMPUTER SERVICES  DEBIT
PERSONAL  UNITED STATES
507702  TENNESSEE EBT ISSUED BY JPMORGAN EFS  DEBIT  PERSONAL  UNITED
STATES
507709  KENTUCKY EBT ISSUED BY JPMORGAN EFS  DEBIT  STANDARD  UNITED
```

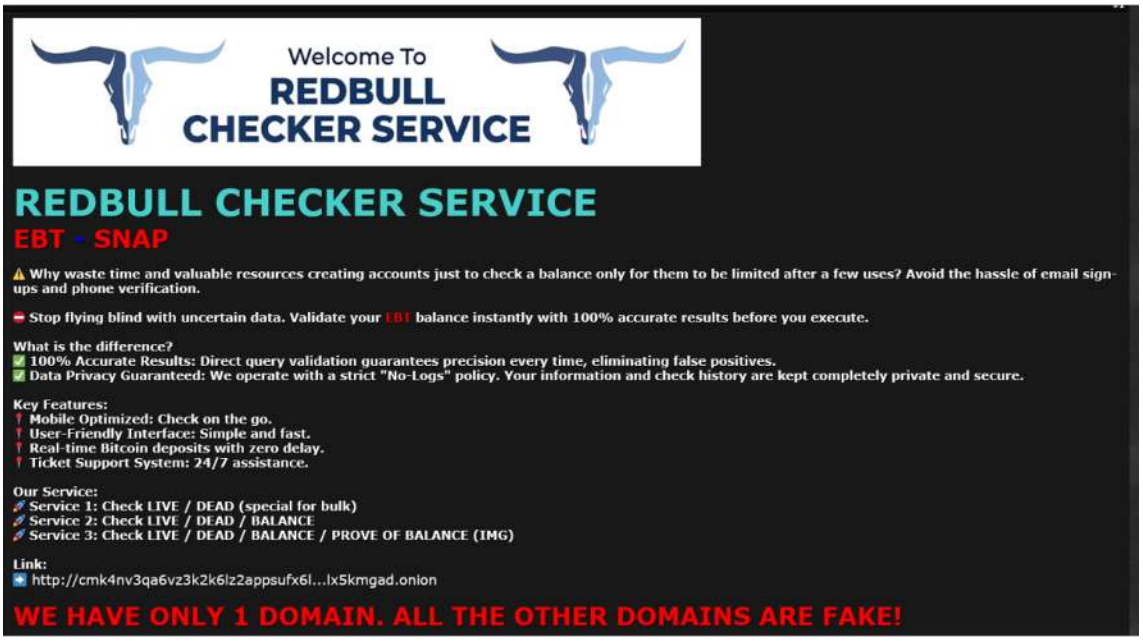
SNAP EBT Cards For Sale on a Darkweb Market

Once the information is purchased, criminals may encode the stolen data onto cloned payment cards and use them to drain victims' accounts. SNAP benefits can be used to purchase high-demand goods, such as baby formula and other products that can be resold for cash. When the compromised account also contains cash assistance or disability benefits, criminals may withdraw those funds directly from ATMs. Fraudsters also sell step-by-step tutorials -- sometimes marketed as the "EBT method" -- that explain how to steal, transfer, and monetize benefits, including through online grocery and delivery platforms.

In a recent development, fraudsters have begun offering services that allow criminals to verify the status and available balance of stolen EBT cards before attempting to use them. For example, the screenshot below shows an underground service advertised as **"**Redbull Checker**,"** which claims to determine whether an EBT account is active and, for an additional fee, reveal the remaining balance or provide visual proof of that balance. The service is promoted through an online site and emphasizes bulk checking, privacy, and immediate results.

The platform operates through a credit-based payment system funded with Bitcoin. Users purchase credits and then spend those credits to check stolen EBT account information. This type of service reduces uncertainty for criminals by allowing them to identify which compromised

cards still contain benefits before cloning the cards, making purchases, or reselling the account information. In effect, it adds another specialized layer to the SNAP fraud ecosystem: one criminal steals or acquires the card data, another service validates its value, and a separate actor monetizes the benefits.



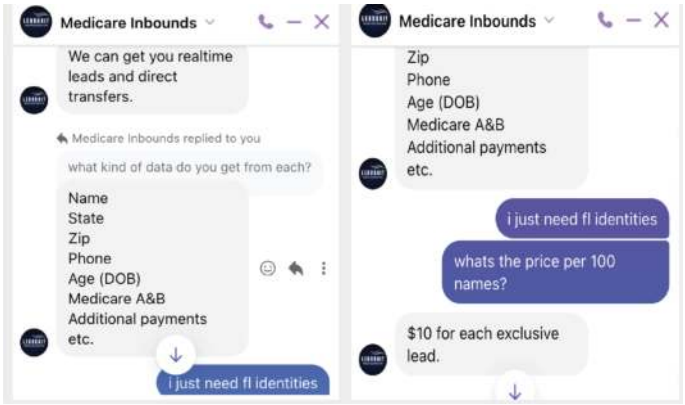
EBT Balances checking services

This activity has a particularly severe effect on victims because SNAP recipients often discover the theft only after attempting to purchase food for their families. Unlike consumers whose bank-issued credit or debit cards generally include mature fraud controls, EBT recipients have historically relied on cards and systems with fewer protections, limited real-time alerts, and inconsistent reimbursement processes. The result is that criminals can drain an account shortly after benefits are deposited, leaving the intended recipient without money for basic necessities.

Medicaid and Medicare Fraud

Another trend my teams and I are observing is the development of an online market for Medicare and Medicaid beneficiary information. Criminals often first obtain this information through data breaches of healthcare facilities and scams designed specifically to harvest beneficiaries' identities. They send fraudulent enrollment notices, text messages, emails, and telephone solicitations that impersonate Medicare, Medicaid, insurers, pharmacies, or medical-equipment providers and suppliers. Victims are told that they must confirm their eligibility, activate a new benefit, avoid an interruption in coverage, or complete a health survey. In reality, these communications are designed to collect Medicare or Medicaid numbers, Social Security numbers, dates of birth, addresses, and medical information.

The stolen information is then packaged into structured beneficiary profiles and advertised for sale through Telegram, Facebook, encrypted messaging applications, and other online channels. During my research, I observed vendors selling profiles that included the beneficiary's name, age, address, telephone number, Medicare coverage information, and other personal identifiers. Some sellers offered these records individually, while others advertised access to hundreds or thousands of beneficiaries at a time. The purchasers may include lead brokers, telemarketing operations, laboratories, home-health agencies, and durable medical equipment companies seeking identities that can be used to generate reimbursable claims.



Medicare patient data offered for sale by online vendor on Facebook

Leaked Patient Registration Forms Exposing Personal Identifiers

The scam that initially targets the beneficiary is therefore only the first stage of the fraud. The person who collects the information may not be the same person or company that ultimately bills the government. Instead, beneficiary data moves through a supply chain: one group conducts the scam, another packages or brokers the information, and a provider or shell company uses it to bill Medicare or Medicaid for equipment, testing, treatments, or services that were unnecessary, unauthorized, or never provided. Stolen beneficiary information alone cannot easily produce reimbursement; criminals also need a billing entity that appears legitimate. Medical supply companies, laboratories, clinics, and home-health agencies can provide that institutional front.

My investigation of "Sunshine Senior Solutions," a Florida durable medical equipment supplier, illustrates how this process can manifest in the physical world. Beneficiaries in several states publicly reported charges associated with the company for medical equipment they said they had neither requested nor received. When I visited the company's listed address in Delray Beach, I found the office closed and indications that its occupants had vacated the space abruptly. The property's leasing manager later confirmed that the company had left under those circumstances. The contrast between the company's limited physical presence and the volume and geographic reach of the reported billing activity underscores the importance of verifying that providers receiving federal reimbursements maintain operations consistent with the services they claim to deliver.

Website of Florida medical supply provider associated with repeated medicare fraud allegations

This location has since become relevant to a major federal enforcement action. According to the Department of Justice, Sunshine Senior Solutions and another company allegedly submitted at least $3.76 billion in claims to Medicare, Medicaid, and other insurers. Federal authorities recently returned a defendant associated with the alleged scheme to the United States following his apprehension abroad. These remain allegations, and the litigation is ongoing.

This case demonstrates why Medicare and Medicaid fraud should not be viewed solely as a billing problem detected after a claim is submitted. It often begins much earlier -- with scams targeting beneficiaries, trafficking in stolen health identities, the creation or acquisition of billing companies, and the construction of an infrastructure capable of converting stolen identities into government payments. To reduce losses, the federal government must disrupt that entire supply chain rather than waiting until fraudulent claims have already reached the payment system.

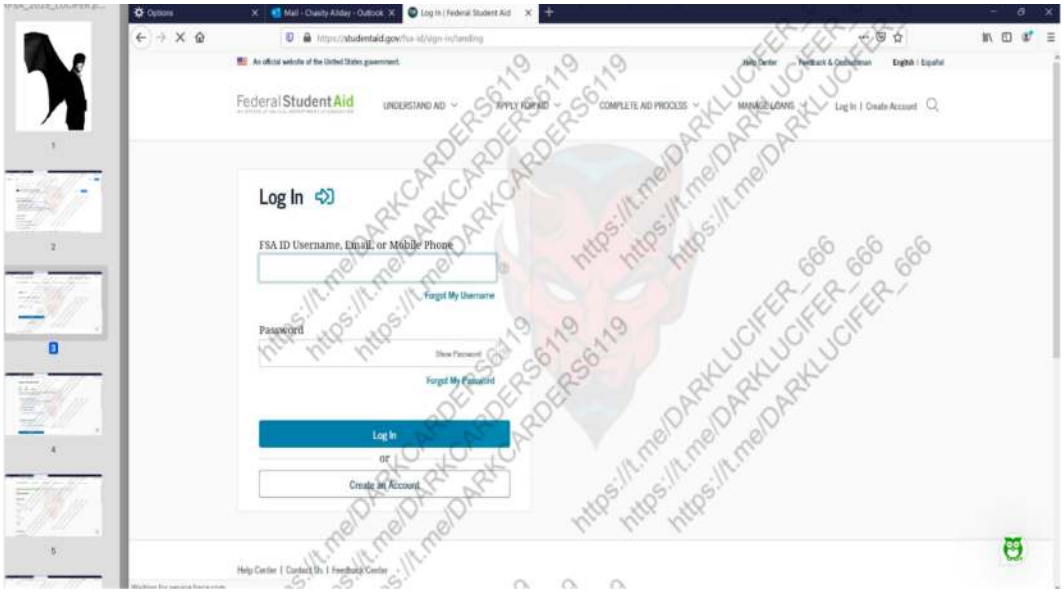
Federal Student Aid Fraud

Another trend I would like to highlight is the rapid growth of organized fraud targeting the federal student aid system, particularly Pell Grants. Within online fraud communities, this scheme is commonly referred to as "Pell Running." Criminals acquire stolen or synthetic identities over online fraud markets, use them to enroll in colleges -- often community colleges -- and submit fraudulent Free Application for Federal Student Aid (FAFSA) applications. Once the aid is approved, they collect the living-expense disbursement, which can reach several thousand dollars per student, and disappear without ever attending a class.

Telegram Post Advertising Complete Identity Packages for FAFSA Fraud

What makes this trend particularly concerning is that it has evolved into a mature fraud-as-a-service ecosystem. My team's research has documented Telegram channels openly advertising identity packages specifically tailored for FAFSA fraud, often bundled with fabricated high school transcripts. Criminals also sell step-by-step tutorials explaining how to complete fraudulent applications, offer cash-out services to convert federal aid into usable funds, and even maintain customer reviews to build credibility and attract new buyers. This is no longer isolated fraud committed by individuals; it is an organized underground economy designed to systematically steal taxpayer dollars.

While The Department of Education has recently required new safeguards, which are an important step forward, the online fraud ecosystem continues to adapt. As we have observed across multiple government benefit programs, fraudsters are already discussing methods for bypassing stronger identity verification requirements, including the use of artificial intelligence and deepfake technology. This underscores a broader lesson: protecting taxpayer-funded programs requires not only stronger identity verification, but also continuous monitoring of the online criminal ecosystem to identify emerging attack methods before they become widespread.



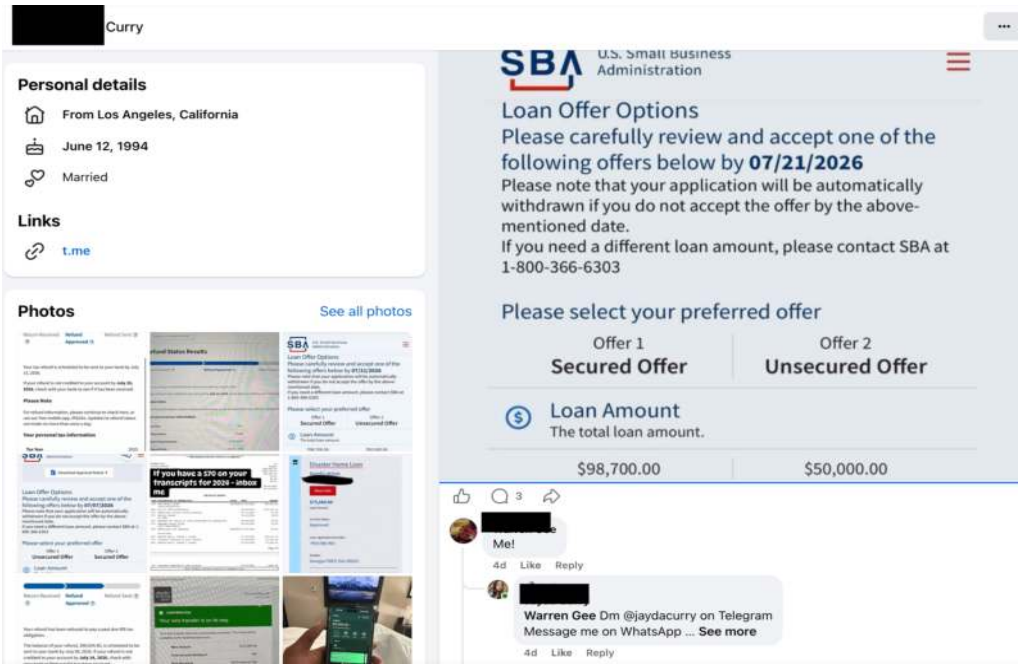
Screenshot of a PDF Tutorial Explaining How to Commit FAFSA Fraud

SBA Loans

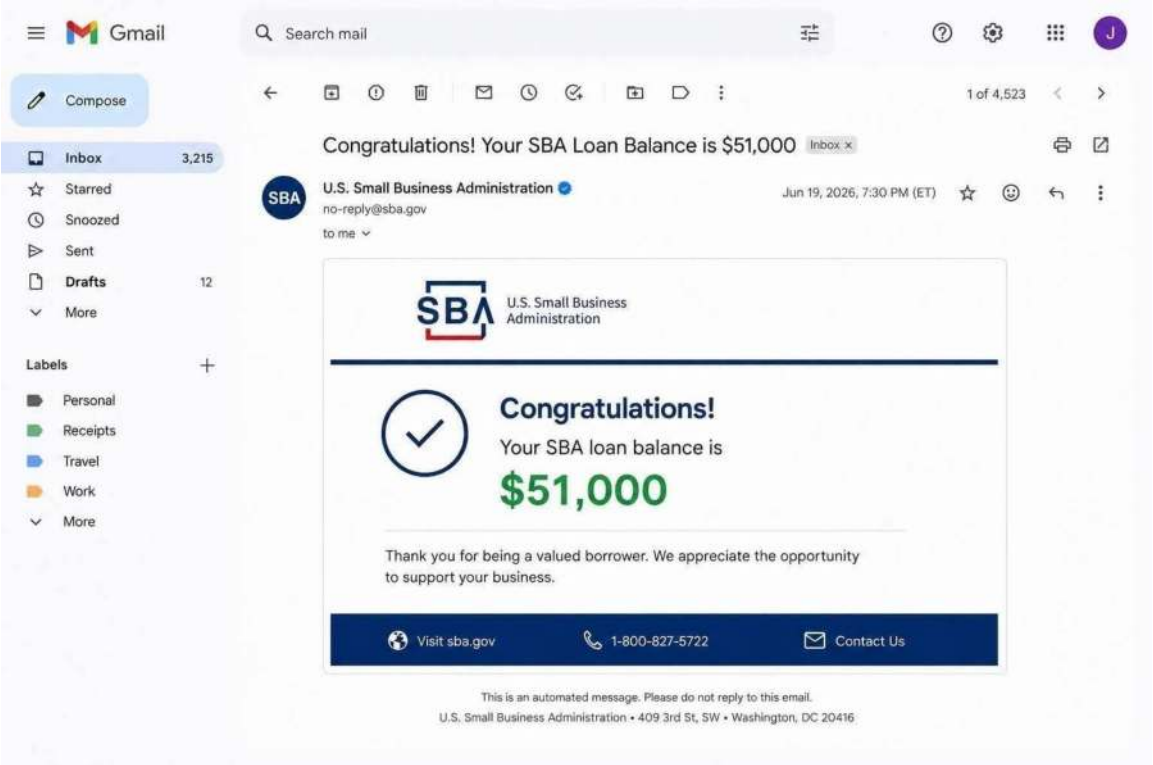
The final and most recent trend my teams and I have started to observe in May of this year is the promotion of fraudulent Small Business Administration loan schemes across social media. Criminals commonly advertise what they call **“**SBA sauce” -- a slang term for instructions, templates, documents, or assistance intended to help applicants obtain government-backed business loans through deception. Public posts have promoted these methods with claims that recipients will not have to repay the money, while some groups have bundled SBA schemes with stolen identities, document services, bank-account opening, and other fraud methods.

These offerings typically include guidance on creating or acquiring a business, fabricating revenue or payroll records, selecting industry classifications, preparing false financial statements, and submitting applications using stolen or synthetic identities. Some promoters sell step-by-step tutorials, while others offer a more complete service in which they prepare the application, provide supporting documents, or take a percentage of any funds received. In this way, SBA loan fraud has become another fraud-as-a-service product that lowers the level of knowledge required for individuals to participate.

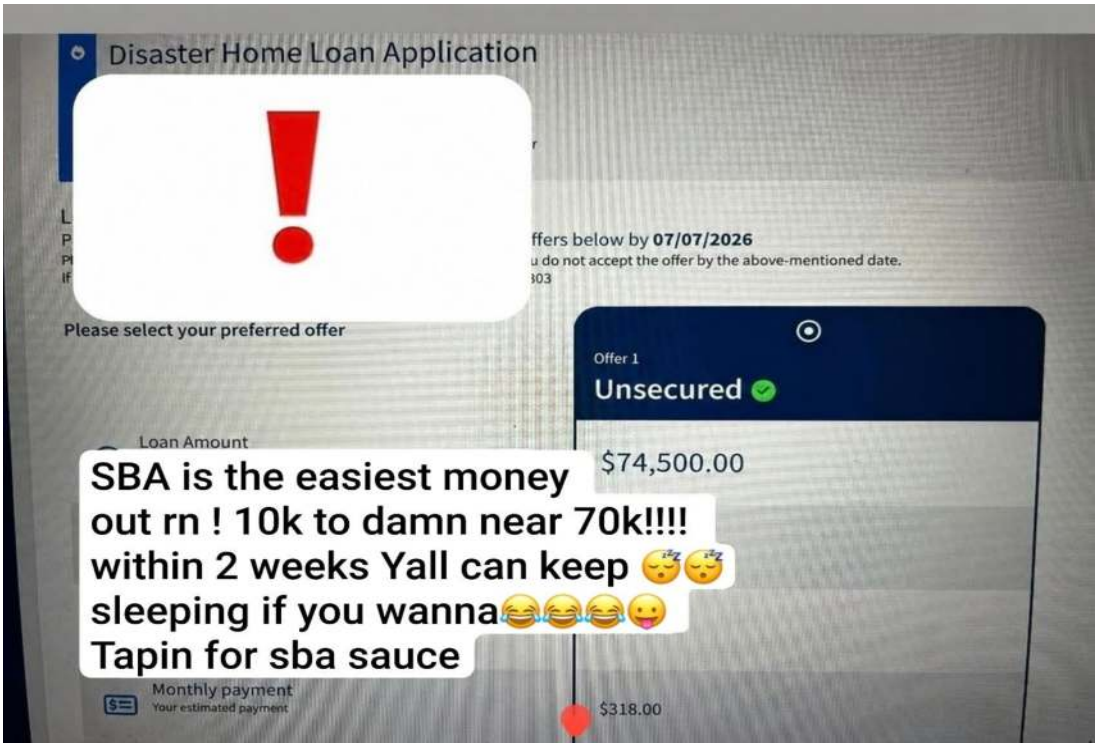
The continued use of the phrase “SBA sauce” is significant because it shows that fraud techniques developed during the pandemic remain part of the online fraud ecosystem. During the emergency-relief period, offenders learned how to form companies quickly, obtain employer identification numbers, generate false business records, open commercial bank accounts, and navigate government loan applications. Those capabilities did not disappear when the Paycheck Protection Program and COVID-19 Economic Injury Disaster Loan programs ended. They can now be redirected toward other SBA-backed lending products and future emergency programs.



Facebook Post Advertising Fraudulent SBA Loan Offers and Directing Applicants to Telegram and WhatsApp



Proof of a Successful SBA Loan Application Advertised Online



Online Promotion of "SBA Sauce" Using a Purported $74,500 Loan Offer as Proof of Success

Key Actions the Federal Government Can Take to Reduce Fraud

The trends described above reveal that fraud against government programs is not confined to individual agencies or benefit systems. Although tax refunds, SNAP, Medicare, student aid, and government-backed loans are administered separately, criminals often rely on the same identities, businesses, bank accounts, devices, addresses, and online service providers to exploit them. Effective prevention therefore requires a government-wide strategy focused on the shared infrastructure that allows fraud to move across programs.

Several cross-cutting themes emerge from my discussion above:

- **First, fraud has become increasingly specialized.** Rather than one offender carrying out every stage of a scheme, online ecosystems now connect dedicated service providers that sell stolen identity profiles, verify compromised EBT balances, produce fraudulent documents, generate deepfake images and videos, prepare applications, and facilitate the movement of funds. This division of labor lowers the technical barriers to fraud and allows criminal operations to scale rapidly.
- **Second, compromised and synthetic identities are rarely used only once.** The same personal information may be used to seek a tax refund, obtain SNAP benefits, submit Medicare claims, apply for federal student aid, or secure a government-backed loan. Fraud prevention systems that examine each program in isolation may therefore miss the broader pattern of repeated identity misuse.
- **Third, the fraud ecosystem is platform-agnostic.** Criminal actors, stolen data, and fraud tools move fluidly among Facebook, Telegram, encrypted messaging services, and darknet marketplaces. Disruption efforts focused on a single platform are unlikely to eliminate the underlying market because vendors and customers can quickly relocate elsewhere.
- **Fourth, artificial intelligence is accelerating these threats.** Generative AI now allows criminals to create realistic identity documents, synthetic photographs, face-swapped videos, and talking avatars that can be used to defeat identity-verification and liveness controls. These capabilities were once expensive and technically difficult to obtain; they are now widely accessible and increasingly offered as services.
- **Finally, fraud networks migrate from one government program to another.** When pandemic-specific relief programs ended, the knowledge, identities, shell companies, financial accounts, and technical tools developed to exploit them did not disappear. The same infrastructure shifted toward standing programs such as Medicare, SNAP, federal student aid, tax refunds, and SBA-backed lending. For this reason, the federal government should focus not only on closing vulnerabilities within individual programs, but also on identifying and disrupting the reusable infrastructure that enables organized fraud across the public sector.

These cross-cutting themes point to a clear conclusion: because modern fraud networks operate across programs, platforms, and stages of the fraud lifecycle, the federal response must be equally coordinated, preventive, and focused on disrupting the shared infrastructure that

enables fraud to scale. Below I offer my recommendations regarding key actions the Federal Government can take to reduce fraud.

1. Replace Self-Attestation with Verified Data

Too many benefit, loan, and reimbursement programs still let applicants report their own income, employment, or identity with little independent verification. That gap was the single biggest vulnerability exploited in unemployment insurance and Paycheck Protection Program fraud: criminals could submit false information at scale because agencies lacked the time or authority to check it before releasing funds.

Self-attestation has a place when speed matters, but it should not be the primary control on high-value or high-risk payments. Income and employment claims should be checked against IRS records, payroll systems, or state wage databases instead of relying on applicant-uploaded documents. Identity proofing should move past document checks and single-point database matches toward identity intelligence that looks at historical consistency: how long a phone number, email, address, or device has been tied to an identity, whether those attributes have appeared together before, and whether the identity shows patterns consistent with synthetic creation. Those relational signals are far harder for criminals to fabricate than a selfie or a document scan. Agencies should also run systematic cross-checks against the Social Security Administration's Death Master File and incarceration records, so payments stop going to fictitious, deceased, or ineligible people before they start.

2. Expand Real-Time Data Matching, and Modernize the Legal Authorities Behind It

Tax, Social Security, unemployment, student aid, healthcare, and lending systems are administered separately, and fraudsters count on that. The same identity, business, address, or bank account can appear across multiple programs without anyone connecting the dots. Agencies need stronger cross-program matching against IRS, SSA, state unemployment, DMV, and correctional records to catch duplicate claims and reused financial instruments before payment, not in a batch run weeks later after the money is gone.

The Treasury Department's Do Not Pay system is the right model, but its reach is limited by statute, not just technology: it doesn't cover every federal payment, program, or data source it should. Congress should expand its scope and modernize the authorities behind it so agencies can conduct real-time matching of narrowly defined data elements with real safeguards -- access controls, audit logs, data-minimization, retention limits, and a clear path for applicants to correct errors. The goal isn't unrestricted government access to personal data. It's a legal framework that lets agencies use information they already have before funds leave the building, instead of after.

3. Strengthen Pre-Payment Screening and Build Fraud Prevention into Program Design

Most programs still lean on post-payment investigation and recovery, and by the time a fraudulent payment is caught, the money has usually already moved through mule accounts or shell businesses, making recovery expensive and often futile. Anomaly-detection tools can flag

spikes from a single device or IP address, reused bank accounts across identities, and payment instructions that change abruptly, and those signals should drive lower manual-review thresholds for claim types with known fraud exposure — regardless of dollar amount, since criminals often test controls with small claims before scaling up.

This has to be built into programs at the design stage, not bolted on after losses mount. New programs should undergo a fraud-risk assessment before launch: likely attack vectors, required verification data sources, and pre-payment controls tested against synthetic identities, shell companies, and AI-generated documents or biometrics. For large one-time payments especially, staggered disbursement -- an initial payment for immediate need, subsequent payments tied to verification -- preserves speed for legitimate applicants without handing criminals the full amount up front. Speed and integrity are not competing goals; they should be designed together.

4. Reconsider Reporting Thresholds and Strengthen Oversight and Transparency

Programs generally get scrutiny only after improper payments cross a set dollar or error-rate threshold. That works for mature fraud vectors, but it lets emerging ones grow underneath the radar. This is particularly true in newer or fast-expanding benefit categories, where by the time a program crosses the formal threshold, criminals have already found the hole, published the method, and built the infrastructure to exploit it. Policymakers and program managers should add a risk-based layer to reporting: rapid year-over-year growth, evidence of organized fraud, and repeated identity misuse should trigger early risk assessments even below the dollar threshold.

The same principle applies to public reporting. GAO high-risk designations and Payment Integrity Information Act reporting should function as accountability tools, not annual paperwork -- dashboards that show loss trends, causes, and recovery by program, and that separate administrative error from suspected fraud rather than blending them into one number that obscures what's actually happening.

5. Strengthen Enforcement, Recovery, and Deterrence

Inspectors general overseeing high-risk programs need dedicated resources for data analysis and investigation, and faster, more standardized referral pipelines to DOJ, the Secret Service, and other law enforcement partners, escalated on strong fraud indicators, not held until losses hit an arbitrary threshold. Referrals should include structured network analysis so prosecutors can see the organization behind what looks, claim by claim, like isolated fraud.

Recovery audits still matter, but they complement pre-payment controls, they don't replace them; recovery gets harder the moment money crosses into mule accounts, cryptocurrency, or overseas channels. Enforcement should weight organized, high-dollar networks over isolated low-level claimants, since concentrating resources on small cases leaves the identity brokers, document forgers, and cash-out operators who enable fraud at scale untouched. And Congress should look at whether False Claims Act qui tam protections still fit a fraud landscape where

contractors, data brokers, and financial intermediaries often hold the first evidence of a scheme, before a single claim is paid.

6. Invest in Fraud Research and Build a Proactive, Rapid-Response Capability

Fraud research and analytics should be a standing government capability, not something stood up after a scandal. Agencies running high-risk programs need dedicated fraud-intelligence units, modeled on what Treasury and CMS have already built, with multi-year funding, because the value of this work -- schemes that never scale, losses that never happen -- doesn't show up in an arrest count and competes poorly for budget against work that does.

Those units should do two things well. First, measure accurately: current improper-payment estimates likely understate fraud designed specifically to dodge audits and sampling, so agencies need better estimation methods and consistent ROI methodology to justify continued investment. Second, move fast: continuous monitoring of program data alongside social media, Telegram, and darknet intelligence should feed directly into operational authority to update screening rules, alert other agencies, pause suspicious payment patterns, and refer organized activity to law enforcement in days, not after an annual audit. Fraud rings don't respect agency boundaries, and the response infrastructure that tracks them can't either — funding tied to a single program guarantees the government sees only the piece of the pattern that program happens to touch.

Conclusion

The central lesson of this testimony is that fraud against government programs is no longer a series of isolated schemes. It is a durable, specialized, and highly adaptive criminal infrastructure, and the pandemic gave it the opportunity and the capital to build out: stolen identities, shell companies, fabricated documents, money mules, all distributed and refined across online platforms. When pandemic-relief programs ended, none of that capability disappeared. It migrated into SNAP, Medicare, Medicaid, federal student aid, tax refunds, and government-backed loans.

That migration works because criminals no longer need to possess every skill a scheme requires. They can buy each piece from a specialized provider, and the same compromised identity can be reused across several programs at once, which makes agency-by-agency detection increasingly inadequate. Generative AI is accelerating the problem further: a document, a selfie, or a single database match may confirm that information looks valid, but it does not confirm that the applicant is a real person, controls the identity, or has a credible history.

The federal government already has some of the tools it needs to change this picture. What is missing is the authority, coordination, and sustained investment to use them before fraudulent payments leave the government, not after criminals have already moved the money. Fraud prevention is not an administrative burden. It is a core responsibility of effective government,

and every dollar protected is a dollar that stays available for the people Congress intended to help.

Thank you for the opportunity to testify. I look forward to answering the Subcommittee's questions.

References

Fisher, D., Maimon, D., & Berenblum, T. (2022). Examining the crime prevention claims of crime prevention through environmental design on system-trespassing behaviors: A randomized experiment. *Security Journal*, *35*(2), 400-422.

Kamar, E., O'Malley, R. L., Howell, C. J., Maimon, D., & Shabat, D. (2025). “Cutie, click on the link”: A forensic analysis of URLs. *Computers in Human Behavior*, *162*, 108454.

Kamar, E., Maimon, D., Weisburd, D., & Shabat, D. (2024). The Relevance of Targets’ Sexual Knowledge in the Progression of Online Sexual Grooming Events: Findings from an Online Field Experiment. *Justice Quarterly*, *41*(3), 452-473.

Kaur, M., Maimon, D., Kubek, M. M., & Bourgeois, A. G. (2026). Telegram as a transformative criminal marketplace: Analyzing identity theft dynamics on surface-accessible platforms. In *2026 14th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1–6). IEEE.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33-59.

Maimon, D. (2022, January 6). *How cybercriminals turn paper checks stolen from mailboxes into bitcoin*. The Conversation. https://theconversation.com/how-cybercriminals-turn-paper-checks-stolen-from-mailboxes-into-bitcoin-173796

Maymoni, L., Kamar, E., & Maimon, D. (2026). Dude, where’s my check? An OSINT-based analysis of the link between check theft and identity theft. *Crime & Delinquency*, 00111287261441231.

Ouellet, M., Maimon, D., Howell, J. C., & Wu, Y. (2022). The network of online stolen data markets: How vendor flows connect digital marketplaces. *The British Journal of Criminology*, *62*(6), 1518-1536.