Testimony of Lauren K. Saunders

Associate Director, National Consumer Law Center

On behalf of

Americans for Financial Reform
National Consumer Law Center (on behalf of its low income clients)
Center for Responsible Lending
Consumer Federation of America
U.S. PIRG

On
"Ongoing Oversight: Monitoring the Activities of the Justice Department's Civil, Tax and Environment and Natural Resources Divisions and the U.S. Trustee Program"

Before the

Committee on the Judiciary
Subcommittee on Regulatory Reform, Commercial and Antitrust Law

May 19, 2015

Chairman Marino, Ranking Member Johnson and Members of the subcommittee:

Thank you for inviting me to testify today on behalf of Americans for Financial Reform, the low income clients of the National Consumer Law Center, the Center for Responsible Lending, Consumer Federation of America, and U.S. PIRG.

I am here today to testify in support of the Department of Justice's Operation Choke Point and to urge the Department to increase its work to deprive fraudsters of access to consumers' bank accounts. I would like to make the following key points:

- Operation Choke Point stops fraud. Many fraudsters rely on banks and third party payment processors to enable them to take money from consumers' accounts. Banks and payment processors can enable fraud, and often they can stop it.

- The three cases that DOJ has brought through Operation Choke Point prove that DOJ is focusing only on banks that willfully ignore blatant signs of illegal activity. No one has defended the egregious conduct of any of the banks targeted.
- Reports that banks have closed the accounts of legal businesses have little or nothing to do with Operation Choke Point. Complaints about account closures go back a decade, since passage of the 2001 Patriot Act with its anti-money laundering rules.
- Bills such as H.R. 766 (Luetkemeyer), the Financial Institution Customer Protection Act of 2015; H.R. 1413 (Schweikert), the Firearms Manufacturers and Dealers Protection Act of 2015; and similar bills would make it harder for DOJ and other government agencies to protect the public.

Fraudsters Use Banks and Payment Processors to Take Money from Consumers

Many scams, frauds and illegal activity could not occur without access to consumers' bank or credit card accounts. Fraudsters who obtain consumers' account numbers can take payments from consumers in several ways. They can submit a "preauthorized" electronic payment through the ACH system; they can create a remotely created check drawn on the consumer's account and deposit it; or they can process a fraudulent charge against the consumer's credit or debit card through the relevant card network (Visa, MasterCard, American Express or Discover).[1]

[1] To my knowledge, none of the Operation Choke Point cases to date have involved card payments, but many scams do. For example, the FTC recently brought a case against a third party payment processor that contributed to a massive $26 million internet scam by helping its fraudster clients evade the credit card networks' fraud monitoring programs. FTC, Press Release, "FTC Charges Payment Processors Involved in I Works Scheme" (Aug. 1, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/ftc-charges-payment-processors-involved-i-works-scheme.

When fraudsters submit a payment against a consumer's account, two different banks are involved: the consumer's bank – which receives the debit (ACH, check, card charge) – and the bank that initiates or submits the debit on behalf of the payee. For simplicity, I will refer to the consumer's bank as the Receiving Depository Financial Institution (RDFI) and the initiating bank as the Originating Depository Financial Institution (ODFI), although different terminology is actually used for payment methods other than ACHs.[2]

Banks play a critical role in enabling payment fraud. Scammers must use an ODFI to gain access to the ACH, check clearing or card network system in order to extract money from a consumer's account.[3]

A payment processor is often used as an intermediary between the payee and the ODFI . The payment processor collects consumers' account information from the payee, formats it, and submits it to the ODFI, which then forwards the debit through the appropriate system. Payment processors enable legitimate merchants and scammers alike to process payments against millions of accounts.

Many scams and other forms of unlawful activity rely on the ability to access the payment system to get the consumer's money. Examples of scams that accessed consumers' accounts include the following:

[2] Those are the terms used for preauthorized payments processed through the ACH system. If a check is involved, the consumer's bank would be the "payor bank" and the bank of the payee or its processor would be the "depository bank." For a card payment, the consumer's bank is the "issuing bank" and the bank of the payee or its processor is the "acquiring bank."

[3] The ODFI is the entry point for each of these payments. In a preauthorized ACH transaction, the ODFI initiates the ACH debit against the consumer's account through the ACH system pursuant to its agreement with NACHA, which writes the rules governing the ACH system. In a check transaction, the ODFI accepts the deposit of the check and then forwards it for collection to the RDFI. In a card transaction, the ODFI is the bank that has the agreement with the card network and provides the merchant with access to the network in order to accept card payments, pursuant to the ODFI's agreement with the network.

- Scammers who cold-called seniors claiming to sell fraud protection, legal protection and pharmaceutical benefits took $10.7 million illegally from consumer accounts using remotely created checks and funneled the money across the border to Canada.[4]
- A telemarketing scam defrauded seniors of $20 million by lying to them to get their bank account information.[5]
- Wachovia Bank enabled $160 million in fraud by processing payments for scammers who targeted vulnerable seniors.[6]
- Some Wachovia scammers then moved to Zions Bank, whose wholly owned third party payment process earned 49% of its revenue from mass market frauds ultimate shut down by the Federal Trade Commission or the Justice Department. Zions ignored suspicious activity and allowed the scammers to continue defrauding seniors.[7]
- A lead generator tricked people who applied for payday loans and used their bank account information to charge them $35 million for unwanted programs.[8]

---

[4] FTC, Press Release, "Court Orders Ringleader of Scam Targeting Seniors Banned From Telemarketing Court Imposes $10.7 Million Judgment" (March 12, 2015), https://www.ftc.gov/news-events/press-releases/2015/03/court-orders-ringleader-scam-targeting-seniors-banned?utm_source=govdelivery.

[5] *See* Federal Trade Comm'n, Press Release, "FTC Stops Mass Telemarketing Scam That Defrauded U.S. Seniors and Others Out of Millions of Dollars" (Mar. 31, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/03/ftc-stops-mass-telemarketing-scam-defrauded-us-seniors-others-out.

[6] *See* Charles Duhigg, "Bilking the Elderly, With a Corporate Assist," New York Times (May 20, 2007), available at http://www.nytimes.com/2007/05/20/business/20tele.html?pagewanted=all&_r=1&.

[7] Jessica Silver-Greenberg, New York Time, "Banks Seen as Aid in Fraud Against Older Consumers" (June 10, 2013), available at http://www.nytimes.com/2013/06/11/business/fraud-against-seniors-often-is-routed-through-banks.html?pagewanted=all&_r=0. Letter from Howard Langer to Rep. Spencer Bachus & Rep. Hank Johnson re Hearing on Operation Choke Point at (July 15, 2014), attached as Exhibit A available at http://judiciary.house.gov/_cache/files/30804b28-f604-4e22-80c5-201db94c0cdc/113-114-88724.pdf (pp. 54-57).

[8] *See* Federal Trade Comm'n, Press Release, "FTC Charges Marketers with Tricking People Who Applied for Payday Loans; Used Bank Account Information to Charge Consumers for Unwanted Programs" (Aug. 1, 2011), available at http://www.ftc.gov/news-events/press-releases/2011/08/ftc-charges-marketers-tricking-people-who-applied-payday-loans.

- Bogus debt relief services scammed consumers out of $8 million and made their debt problems worse.[9]
- The FTC obtained a $6.2 million settlement against a payday loan broker that falsely promised to help consumers get loans and then used consumers' bank account information to make unauthorized withdrawals without their consent.[10]

In each of these scams, the fraudsters' ability to take money out of consumers' accounts depended on access to an ODFI and often a payment processor.

Even when consumers authorize an initial payment from their accounts to purchase products or repay loans, they may find that their accounts are repeatedly debited for fees or charges they did not authorize or additional products they did not buy. For example, the FTC brought an action against a weight loss company that debited consumers' accounts monthly for offers they did not ask for.[11] Online payday lenders have deceived consumers by imposing undisclosed charges and inflated fees that were automatically deducted from their bank accounts.[12]

[9] *See* Federal Trade Comm'n, Press Release, "FTC Charges Operation with Selling Bogus Debt Relief Services; DebtPro 123 LLC Billed Consumers as Much as $10,000, But Did Little or Nothing to Settle Their Debts" (June 3, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/06/ftc-charges-operation-selling-bogus-debt-relief-services.

[10] See Federal Trade Comm'n, Press Release, "Phony Payday Loan Brokers Settle FTC Charges," (July 11, 2014) available at http://www.ftc.gov/news-events/press-releases/2014/07/phony-payday-loan-brokers-settle-ftc-charges.

[11] FTC, Press Release, "At FTC's Request, Court Stops Supplement Marketers From Deceptive Advertising and Illegally Debiting Consumers' Accounts" (Oct. 20, 2014), https://www.ftc.gov/news-events/press-releases/2014/10/ftcs-request-court-stops-supplement-marketers-deceptive.

[12] FTC, Press Release, "U.S. District Judge Finds that Payday Lender AMG Services Deceived Consumers by Imposing Undisclosed Charges and Inflated Fees" (June 4, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/06/us-district-judge-finds-payday-lender-amg-services-deceived.

The FBI estimates that mass-marketing fraud schemes cause tens of billions of dollars of losses each year for millions of individuals and businesses.[13] A MetLife study found that fraud drains $2.9 billion a year from the savings of senior citizens.[14]

How Banks and Payment Processors Can Prevent or Enable Payment Fraud

When an ODFI's customer collects payments through the ACH system, the check system, or a card network, the ODFI has a unique window into the customer's business and the transactions. The ODFI has a corresponding responsibility to undertake due diligence to ensure that the payments it processes are legitimate. Payment processors have similar obligations.

Banks have know-your-customer (KYC) responsibilities under the Bank Secrecy Act (BSA) and the USA Patriot Act amendments. Before agreeing to open an account and process payments for a customer, the bank must conduct due diligence to ascertain the identity of the customer and the purpose of the account. For example, the bank must conduct basic research to establish that a business customer has an actual, legal business; that it has a real address and is truly based in the United States if that is what the business claims; and that the business has not been involved in unlawful or fraudulent activity, such as might be revealed by checking news reports, the Better Business Bureau or internet complaint sites. Additional precautions apply if the customer is located out of the country or intends to process payments internationally. KYC rules are important not only for stopping consumer scams but also for preventing terrorists, drug dealers and other criminals from laundering money and moving it around.

---

[13] Federal Bureau of Investigation, International Mass-Marketing Fraud Working Group, "Mass-Marketing Fraud: A Threat Assessment" (June 2010), available at http://www.fbi.gov/stats-services/publications/mass-marketing-fraud-threat-assessment/mass-marketing-threat.

[14] The MetLife Study of Elder Financial Abuse (June 2011), available at https://www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf.

Banks must also monitor accounts for signs of fraud or unlawful activity. One of the clearest signs of a problem is a high return rate – the percentage of payments that are rejected and are returned by the RDFI to the ODFI because the payment was challenged as unauthorized, was subject to a stop payment order, bounced because of insufficient funds, or was rejected because the account does not exist or was closed. Not every rejected payment is a sign of fraud. But if return rates are high, banks have a duty – both under NACHA rules (governing ACH payments) and under bank regulator supervisory expectations – to determine why and to investigate if the account is being used for improper purposes.[15] If large numbers of consumers are challenging an OFDI's customer's payments as unauthorized, clearly the customer is doing something wrong. If an unusually high number are rejected because the account has been closed, that may reveal that consumers are closing their accounts in response to fraud or that the fraudster is buying lists of bank account numbers that contain older accounts long since closed. Even high rates of payments rejected for insufficient funds, especially when combined with returns for other reasons, may reveal that consumers are not expecting the payments and have been defrauded.

In the ACH system, the average rate of transactions returned as unauthorized is 0.03%.[16] Under upcoming NACHA rules, an unauthorized return rate higher than 0.5% (over sixteen

[15] *See, e.g.*, NACHA, ACH Operations Bulletin #1-2014: Questionable ACH Debit Origination: Roles and Responsibilities of ODFIs and RDFIs (Sept. 30, 2014), https://www.nacha.org/news/ach-operations-bulletin-1-2014-questionable-ach-debit-origination-roles-and-responsibilities; Federal Deposit Ins. Corp., FIL-127-2008, Guidance on Payment Processor Relationships (Revised July 2014), https://www.fdic.gov/news/news/financial/2008/fil08127.pdf ("FDIC Revised Payment Processor Guidance"); Office of the Comptroller of the Currency, OCC Bulletin 2006-39, Automated Clearing House Activities (Sept. 1, 2006), http://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html ("OCC 2006 ACH Bulletin").

[16] NACHA, ACH Network Risk and Enforcement Topics, Topic 1- Reducing the Unauthorized Return Rate Threshold (effective date September 18, 2015), https://www.nacha.org/rules/ach-network-risk-and-enforcement-topics.

times higher than the average rate) will trigger a responsibility to investigate.[17] The average total rate at which ACH debits are returned for any reason is 1.42%, and under new rules, a total return rate of above 15% (over ten times higher than the average rate) will require scrutiny.[18] Legitimate return rates in the check system and card networks are in the same ballpark as the average ACH return rates.[19]

An ODFI's ability to scrutinize return rates can be somewhat more complicated if a payment processor is acting as an intermediary between the payees and the ODFI. The ODFI may not directly see a high return rate for an individual merchant if that merchant's payments are bundled together with those of other merchants. But ODFIs have a responsibility to oversee the payment processors in order to that ensure that each merchant receives KYC scrutiny and return rate monitoring.[20]

The use of "nested" payment processors – a processor that processes payments for other payment processors – can further launder signs of unlawful activity and is itself a warning signal. For this reason, regulators have advised ODFIs to be especially careful of processor customers whose clients include other payment processors.[21]

Other signs of fraud are obvious. The consumer's bank, state attorneys general, or other government officials may complain to or tip off the ODFI. The ODFI also may learn of high rates of consumer complaints when payments are contested.

---

[17] *Id.*
[18] NACHA, ACH Network Risk and Enforcement Topics, Topic 2- Establishing Inquiry Process For Administrative and Overall Return Rate Levels (effective date September 18, 2015), https://www.nacha.org/rules/ach-network-risk-and-enforcement-topics.
[19] *See, e.g.*, FTC, Press Release, "FTC Sues Payment Processor for Assisting Credit Card Debt Relief Scam" (June 5, 2013), https://www.ftc.gov/news-events/press-releases/2013/06/ftc-sues-payment-processor-assisting-credit-card-debt-relief-scam?utm_source=govdelivery (noting that the average credit card chargeback rate is well below one percent).
[20] *See, e.g.*, OCC 2006 ACH Bulletin, *supra*; FDIC Revised Payment Processor Guidance, *supra.*
[21] *Id.*

Efforts to stop payment fraud protect not only consumers but also ODFIs themselves. In all three systems – ACH, check and card network – an ODFI that initiates a payment must extend a warranty to the RDFI that the payment is legitimate. If the consumer challenges it and the payment turns out to be unauthorized, the ODFI must reimburse the RDFI (which in turn reimburses the consumer).

Banks are not expected to verify the legality of every payment they process, and they are not always aware that they are being used to facilitate illegal activity. But financial institutions that take their duties seriously can be an important bulwark depriving criminals of access to the payment system.

DOJ's Operation Choke Point

The Department of Justice's (DOJ) Operation Choke Point is aimed at banks that "choose to process transactions even though they know the transactions are fraudulent, or willfully ignore clear evidence of fraud."[22] The focus is on illegal conduct, not activity that DOJ deems immoral.

Banks that choose profits in the face of blatant signs of illegality are an appropriate target for enforcement action. Cutting scammers off from access to the payment system can be a much more effective way of protecting the American public than playing a game of "whack a mole" by limiting enforcement actions to individual scammers.

The three Choke Point cases that DOJ has brought to date are unassailable. In each of these three cases, banks assisted horrible scams that took millions of dollars out of consumers' bank accounts. Each of the three banks that DOJ targeted ignored overwhelming evidence that its customer was engaged in widespread fraudulent activity.

[22] The U.S. Department of Justice, "Holding Accountable Financial Institutions that Knowingly Participate in Consumer Fraud," The Justice Blog (May 7, 2014), available at http://blogs.justice.gov/main/archives/3651.

Four Oaks Bank & Trust

The first case, brought in January of 2014, was against Four Oaks Bank & Trust Co. and its holding company, Four Oaks Fincorp, Inc. Four Oaks enabled payments for an illegal Ponzi scheme that resulted in an SEC enforcement action;[23] a money laundering operation for illegal internet gambling payments;[24] illegal and fraudulent payday loans; and a prepaid card marketing scam that made unauthorized debits for a bogus credit line.[25]

Four Oaks ignored blatant red flags of illegality, including:

- extremely high rates – *up to 70%* -- of payments returned as unauthorized;
- efforts to hide merchants' identities;
- offshore entities clearly violating U.S. laws;
- disregard for Bank Secrecy Act obligations by foreign entities;
- hundreds of consumer complaints of fraud; and
- federal and state law violations, including warnings by NACHA and state attorneys general.[26]

I am not aware of a single criticism of the Four Oaks case itself. The bank's conduct was indefensible. But because some of the payments being processed were for illegal and fraudulent

[23] SEC, Press Release, "SEC Shuts Down $600 Million Online Pyramid and Ponzi Scheme" (Aug. 17, 2012), available at http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171483920#.U8P2rpRdX9Z.

[24] United States v. Pokerstars, et al., 11-CV-02564 (S.D.N.Y.).

[25] Federal Trade Comm'n, Press Release, "FTC Sends Full Refunds to Consumers Duped by Marketers of Bogus '$10,000 Credit Line'" (May 12, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/05/ftc-sends-full-refunds-consumers-duped-marketers-bogus-10000.

[26] Complaint for Injunctive Relief and Civil Monetary Penalties, United States v. Four Oaks Fincorp, Inc., and Four Oaks Bank & Trust Company, No. 5:14-cv-00014-BO (E.D. N.C. filed Jan. 8, 2014), https://www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/BankingLaw@manatt/7-U.S.-v-Four-Oaks-Fincorp.pdf. A summary of the key allegations is available at http://www.nclc.org/images/pdf/banking_and_payment_systems/letter-doj-payment-fraud.pdf.

payday loans, it spawned a cottage industry of critics claiming that the hidden purpose of Operation Choke Point was to target legal industries that the Obama Administration dislikes.

However, the Four Oaks case was merely about a bank that was knowingly processing illegal and fraudulent payments that just happened to involve payday loans. The loans were made in states where payday loans are prohibited, rendering both the loan and the payment authorization invalid.[27] The complaint also described many consumers who were defrauded when they authorized a one-time payment from their bank account but found that the payday lenders debited their accounts repeatedly, without authorization, and would not stop.

In March of this year, DOJ brought two additional cases through Operation Choke Point. Both fit the model of clearly fraudulent activity and banks that looked the other way.

CommerceWest Bank

CommerceWest Bank allowed V Internet Corp LLC, a third-party payment processor, to make unauthorized withdrawals from consumers' bank accounts. CommerceWest facilitated over 1.3 million unauthorized remotely created checks for telemarketing scams, medical benefit discount card scams, and payday loan finder scams. The merchants included a fraudulent telemarketing company and a company that charged victims $15 million in payday loan referral fees they never authorized.

CommerceWest ignored clear warning signs indicating that V Internet and its merchants were defrauding consumers, including:

- return rates *exceeding 50%*,
- thousands of complaints from consumers to the Better Business Bureau and in other venues, and

[27] *See* discussion in footnote 47, *infra*.

- multiple complaints from other banks whose customers had been victims of these fraud schemes.[28]

When CommerceWest received complaints from other banks, it blocked access to banks that complained but allowed transactions to continue against consumers' accounts at other banks.[29]

The conduct at CommerceWest was so egregious that DOJ brought a criminal action, charging CommerceWest with willfully failing to file Suspicious Activity Reports required by the Bank Secrecy Act. CommerceWest Bank admitted its wrongdoing and gave up any claim to more than $2.9 million seized by the U.S. Postal Inspection Service from the processor's accounts at the bank.

Plaza Bank

The third Operation Choke Point case to date was against Plaza Bank. The bank's chief operating officer (COO), who was secretly the part-owner of a payment processor, brushed aside warnings from the bank's compliance officer and allowed fraudsters unfettered access to steal from tens of thousands of consumers.[30]

For three years, fraudulent merchants acted through a third-party payment processor to illegally withdraw tens of millions of dollars from the bank accounts of consumers who owed them nothing.[31] Scams included internet telemarketing schemes, fraudulent "identity theft

[28] U.S. DOJ, Press Release, "CommerceWest Bank Admits Bank Secrecy Act Violation and Reaches $4.9 Million Settlement with Justice Department" (Mar. 10, 2015), http://www.justice.gov/opa/pr/commercewest-bank-admits-bank-secrecy-act-violation-and-reaches-49-million-settlement-justice.
[29] *Id.*
[30] Press Release, Department of Justice, Justice Department Announces Settlement with California Bank for Knowingly Facilitating Consumer Fraud (March 12, 2015), *available at* http://www.justice.gov/opa/pr/justice-department-announces-settlement-california-bank-knowingly-facilitating-consumer-fraud.
[31] Complaint at 11–12, U.S. v. Plaza Bank, No. 8:15-cv-00394 (C.D. Cal. Mar. 15, 2015).

protection insurance," misusing consumer financial information from payday loan applications, and false offers of free credit cards, airline tickets, and other products to the public.[32]

Plaza's chief compliance officer had raised concerns in response to a flood of warning signs. Thousands of consumers complained that money was withdrawn from their accounts without their authorization. Other banks and law enforcement officials expressed concern that the payment processor's transactions were fraudulent. Approximately *half* of withdrawals from this payment processor were rejected as fraudulent or unauthorized by consumers' banks.[33]

The compliance officer's concerns were dismissed by Plaza's COO. Unknown to the compliance officer, the COO was one of two Plaza officials who also held an ownership stake in the payment processor.[34]

The bank was also affirmatively making money from fraud. Each time a scammer's fraudulent withdrawal was rejected, Plaza collected a fee from the payment processor, including over $83,000 in fees resulting from over 160,000 rejected withdrawals just in September 2009. Even when new management realized the scope of the fraud, management spent months debating whether the revenues outweighed the risk to the bank.[35]

DOJ Pursues Scammers Directly, But Cutting Off Access to Bank Accounts is a Critical Tool

One of the criticisms of Operation Choke Point is that DOJ should be going after scammers directly and that it is unfair to expect banks to be accountable for fraud committed by their customers or their customers' customers. But as described above, the only banks that DOJ has targeted are ones that have willfully participated in scams by flagrantly violating their duties

[32] *Id.* at 18, 22, 28.
[33] *Id.* at 15.
[34] *Id.* at 10.
[35] *Id.* at 22–25.

to know their customers, monitor return rates, and pay attention to other signs of unlawful or fraudulent activity.

The Department of Justice does go after scammers directly. Here are just a few examples of scams that the Department has stopped recently:

- DOJ shut down a call center in Peru that targeted US Spanish-speakers, telling them that they owed thousands of dollars and threatened to sue those who didn't pay. DOJ secured a sentence of over 10 years in prison for the perpetrators of the scheme and seized related assets.[36]
- A Jamaican man who preyed on elderly victims in the US through an international lottery scam pleaded guilty to conspiracy to commit wire fraud after being extradited from Jamaica. He faces up to 30 years in prison, and over $90,000 dollars has been recovered in connection with the scheme.[37]
- DOJ filed complaints against the perpetrators of a multi-million dollar mail-fraud scheme in which thousands of people received letters supposedly written by world-renowned psychics. The letters, which were allegedly made to appear personalized to their recipient, targeted the elderly, the ill, and those in perilous financial condition, and defrauded victims out of tens of millions of dollars.[38]

[36] U.S. DOJ, Press Release, "Peruvian Man Sentenced for Defrauding and Extorting Spanish-Speaking U.S. Residents through Fraudulent Call Centers" (Jan. 27, 2015), http://www.justice.gov/opa/pr/peruvian-man-sentenced-defrauding-and-extorting-spanish-speaking-us-residents-through.
[37] U.S. DOJ, Press Release, "First Jamaican Man Extradited to the United States in Connection with International Lottery Scheme Pleads Guilty" (April 10, 2015), http://www.justice.gov/opa/pr/first-jamaican-man-extradited-united-states-connection-international-lottery-scheme-pleads.
[38] U.S. DOJ, Press Release, "Justice Department Files Enforcement Actions to Shut Down 'Psychic' Mail Fraud Schemes" (Nov. 19, 2014), http://www.justice.gov/opa/pr/justice-department-files-enforcement-actions-shut-down-psychic-mail-fraud-schemes.

- DOJ shut down a business opportunity fraud scheme in which scammers based in Costa Rica fraudulently induced purchasers in the US to buy into fake business opportunities, usually costing at least $10,000. The perpetrator faces a maximum sentence of 25 years in prison, fines, and restitution of profits.[39]
- Two men were sentenced to more than eight years in prison for defrauding Spanish-speaking consumers into buying knockoff products and then threatening to arrest or deport consumers who complained. DOJ seized assets related to the scheme, including around 20 pieces of real property.[40]

These types of direct prosecutions of scammers are an important part of DOJ's work. But the Department should not limit itself in the tools it uses in the never-ending fight against fraud. Individual criminals are often hard to find. Scammer-by-scammer prosecutions take time and can have a limited impact, often popping up again somewhere else.

It can be a much more efficient and effective use of limited government resources to stop a bank or payment processor that has developed a business of processing payments for multiple fraudsters. For example, in the Four Oaks case, the bank and payment processor helped to process payments for an illegal Ponzi scheme, a money laundering operation for illegal internet gambling payments, numerous illegal online payday lenders, and a bogus prepaid card marketing scam. The CommerceWest action stopped numerous scams including telemarketing scams, medical benefit discount card scams, and payday loan finder scams.

[39] Press Release, Department of Justice, U.S. Citizen Extradited from Costa Rica in Connection with International-Based Business Opportunity Fraud Ventures (February 12, 2015), *available at* http://www.justice.gov/opa/pr/us-citizen-extradited-costa-rica-connection-international-based-business-opportunity-fraud.
[40] Press Release, Department of Justice, Florida Residents Sentenced for Defrauding and Threatening Spanish-Speaking Consumers (January 9, 2014), *available at* http://www.justice.gov/opa/pr/florida-residents-sentenced-defrauding-and-threatening-spanish-speaking-consumers.

Indeed, some banks and processors specialize in companies that have been banned from the ACH system or card networks, or were rejected by more careful financial institutions. Discovery in lawsuits against Wachovia and Zions Bank revealed:

> The very same persons who operated the NHS fraud through Zions had operated a similar fraud through Wachovia. Several of the frauds involved in the T-Bank and First Bank of Delaware cases had simply migrated to Zions. Had the banks engaged in the most rudimentary due diligence they would have turned up these migrating frauds. Wachovia and Zions both obtained the fraudulent customers through what are known as account brokers. The account broker who brought PPC to Wachovia testified that four other banks had refused to open accounts for PPC before Wachovia accepted it. The perpetrator of the NHS fraud testified that he was approached by an account broker who brought his account to Zions within twenty-four hours of losing his prior access to the banking system, through a court order freezing PPC's accounts at Wachovia.[41]

That is, basic due diligence would have denied those fraudsters access to the bank accounts of their elderly victims.

Prosecuting banks and payment processors that willfully participate in fraud also has benefits beyond the individual cases. Operation Choke Point has served as an important reminder to all financial institutions and payment processors about the importance of taking their due diligence duties seriously. Since DOJ's work began, numerous financial industry conference sessions, webinars, white papers and consulting efforts have helped the industry to be more vigilant against fraud.

[41] Letter from Howard Langer to Rep. Spencer Bachus & Rep. Hank Johnson re Hearing on Operation Choke Point at (July 15, 2014), attached as Exhibit A available at http://judiciary.house.gov/_cache/files/30804b28-f604-4e22-80c5-201db94c0cdc/113-114-88724.pdf (pp. 54-57).

The vast majority of financial institutions and payment processors have no desire to help scammers. These institutions are important partners with law enforcement when they deny criminals access to the payment system. It is much better to deny fraudsters access to consumers' accounts in the first place than to prosecute them after the fact.

Closures of Pawnbroker or Gun Dealer Accounts are Unrelated to Operation Choke Point

It is virtually impossible to read the three Choke Point complaints to date without concluding that this is essential work for which DOJ should be applauded, not criticized. Yet the two new cases brought this year – clear evidence of what DOJ is actually doing – have not quelled critics from making baseless claims that, behind the scenes, Operation Choke Point is actually about pressuring banks to cut off legal businesses. Bills continue to be introduced to de-fund Operation Choke Point.

The primary "evidence" used against Operation Choke Point is reports that some pawnbrokers, money transmitters, gun dealers and even cigar stores have had their bank accounts closed. The banks generally did not discuss the reasons.

However, complaints about bank closures go back a decade, long before Operation Choke Point, which began in 2013. Bank account closures have much more to do with the Bush Administration USA Patriot Act passed in 2001 after 9/11 than with any current DOJ activity.

The current complaints are just the continuation of an old gripe. Pawn brokers, check cashers, remittance providers and others have been complaining about "bank discontinuance" for years. In 2006, FiSCA, the trade association of neighborhood financial service providers, testified:

"For the past six years banks have been abandoning us - first in a trickle, then continuously accelerating so that now few banks are willing to service us …."[42]

Also in 2006, the National Pawnbroker Association complained to FinCEN:

"Pawn industry members have lost longstanding lines of credit as well as demand deposit relationships in most parts of the country since 2004."[43]

Cash-intensive businesses and accounts used for international transactions can be impacted by enforcement of anti-money laundering laws. Payday lenders and pawnbrokers are often involved in check cashing and remittances.

Gun dealers may also be impacted indirectly by Patriot Act enforcement – not because they are selling guns, but because they may be cash-intensive businesses.

Anti-money laundering rules can lead to account closures if:

- A regulator finds that a bank or credit union lacks the controls required by the BSA and orders the institution to stop serving cash-heavy businesses until the failures can be remedied.
- The bank makes an individual business decision to simplify compliance by not handling certain types of accounts.
- The bank has concerns about the level of cash transactions.
- The bank cannot confirm the ownership or use of the account.

[42] Gerald Goldman, General Counsel of FiSCA, "Summary Of speech before the U.S. House Committee on Financial Services, Subcomm.on Fin'l Inst'ns & Consumer Credit , Regarding Banking Services to MSBs (June 21, 2006), http://www.fisca.org/Content/NavigationMenu/GovernmentAffairs/TestimonySpeeches/FiSCAHearingOralStmtGoldman_6_21_06.pdf.

[43] Letter from Fran Bishop, President, National Pawnbroker Association to Robert W. Werner, Director, Financial Crimes Enforcement Network (FinCEN) (May 9, 2006), http://www.fincen.gov/statutes_regs/frn/comment_letters/71fr12308_12310/msb_51_bishop.pdf.

None of these issues have anything to do with Operation Choke Point. The idea that Operation Choke Point is a moral crusade against gun sales is pure conspiracy theory. Not one of the voluminous DOJ documents produced in the House of Representatives' inquiry about Operation Choke Point mentioned a focus on gun dealers.[44] DOJ's focus is entirely on banks that are complicit in payment fraud.

Banks Close Accounts for a Wide Variety of Reasons

Anti-money laundering efforts are not the only reasons why a bank account may be closed. There are a wide variety of reasons, and it is important not to leap to conclusions based on one-sided anecdotes. Other reasons that a financial institution may close an account include:

- *The bank shuts down a payment processor account used for fraudulent activity.* When that happens, the legal clients of that processor can also be disrupted.
- *Signs of suspicious activity, or indications of financial difficulties such as a pattern of overdrafts, default on another loan held by the bank, or a deteriorating credit rating.* Privacy concerns may prevent banks from explaining why an account was closed,[45] but the customer's side of the story is not always complete.[46]

[44] The only supposed link between Operation Choke Point and gun dealers is DOJ's use of the FDIC's former guidance on third party payment processors, which in one footnote listed online firearm sales among the businesses that had been associated by the payments industry with higher-risk activity. But there is no indication that DOJ (or the FDIC) has ever shown any interest in the bank accounts of gun dealers, and the FDIC later amended the guidance to remove the list of specific merchants.

[45] Dana Liebelson, "Is Obama Really Forcing Banks to Close Porn Stars' Accounts? No, Says Chase Insider," Huffington Post (May 8, 2014), available at http://www.motherjones.com/politics/2014/05/operation-chokepoint-banks-porn-stars(quoting Chase source as saying: "This has nothing to do with Operation Choke Point … we have no policy that would prohibit a consumer from having a checking account because of an affiliation with this industry. We routinely exit consumers for a variety of reasons. For privacy reasons we can't get into why.").

[46] Red Wing Ammunition Co. "isn't sure why he was cut off" by First Data, which stated: "First Data processes transactions for merchants selling firearms and ammunition, so long as they meet our longstanding credit/risk management policy requirements… These policies were implemented before the DOJ's Operation Choke Point and are unrelated." Jennifer Bjorhus, Star Tribune, "Federal antifraud initiative goes too far, banks say" (June 7, 2014), available at http://www.startribune.com/business/262167821.html.

- *Business decisions to avoid areas with high rates of illegal activity or predatory lending.* Regulators have clarified that financial institutions that are aware of the risks and have appropriate controls are not discouraged from serving entire categories of businesses. But some banks choose to exit areas like debt settlement and online payday lending where there are high rates of complaints and illegal activity. Banks may also choose not to be associated with predatory lending even if it is legal.
- *Unprofitable business areas.* Banks make strategic decisions to exit areas unrelated to regulator pressure.

There is one area where Operation Choke Point deserves some credit for bank account closures: accounts used for scams and other illegal activity. For example, some online payday lenders operate unlawfully without state licenses. Operating offshore or through a tribe does not exempt lenders from state laws, contrary to their claim.[47] Banks may close the accounts of lenders that cannot show state licenses, and some banks may choose to stay away from payday lending, simply because it is unlawful in many states.

But the mere fact that Operation Choke Point has a catchy name and makes for good headlines does not mean that every business that has suffered a bank account closure is related to DOJ's work. A few anecdotes about individual businesses drawn from the thousands of accounts that are closed every year do not prove a pattern. The proof of what DOJ is doing is in the cases it has brought – against those rare institutions that choose to enable fraud.

[47]The Supreme Court repeated last year its longstanding view that tribes must obey state law when they act off reservation even if they cannot be sued directly. A state "can shutter, quickly and permanently, an illegal casino" – or an illegal payday loan operation – by denying a license, obtaining an injunction, and even using the criminal law. Michigan v. Bay Mills Indian Community et al., 134 S.Ct. 2024, 2035 (2014).

H.R. 766, the Financial Institution Customer Protection Act of 2015, Would Limit DOJs Ability to Address Fraud.

H.R. 766 (Luetkemeyer) would eliminate the authority that DOJ used to investigate and bring the cases against CommerceWest Bank, Plaza Bank and Four Oaks Bank & Trust for helping scammers to debit consumers' bank accounts. The bill would amend the Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA) to eliminate penalties for and investigative authority into unlawful conduct "affecting" federally insured financial institutions. Instead, agencies could only penalize or investigate illegal conduct "against" a financial institution or "by" the institution against a third party. In other words, DOJ could not use FIRREA authority to look into signs that a bank is knowingly helping scammers to take money out of the accounts of seniors, because the scammers are not targeting the bank and the bank is not targeting the senior.

The bill would frustrate efforts to protect not only the public but also insured financial institutions. Payment fraud poses risks to ODFIs, which by law warrant the legality of payments when the bank serves as an intermediary between payors and payees.[48] Thus, ODFIs that overlook signs of fraud are on the hook for illegal payments when they are challenged. The bill also imposes new procedural hurdles to investigations into FIRREA violations of any kind and makes it more difficult and burdensome for banking agencies to discourage a financial institution from maintaining a banking relationship with a customer that shows significant signs of being involved with fraud or illegal activity.

[48] *See* Testimony of Adam J. Levitin, Professor of Law, Georgetown University Law Center, Before the United States House of Representatives, Judiciary Committee, Subcommittee on Regulatory Reform, Commercial, and Antitrust Law, "Guilty Until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point" at 9-10 (July 17, 2014), http://judiciary.house.gov/_cache/files/f6210f6f-68eb-49b6-b617-167eecfdfe3b/levitin-testimony.pdf.

H.R 766 also makes it more cumbersome for the Department of Justice to issue subpoenas in connection with its investigations of financial fraud. A subpoena is merely a request for information. If a financial institution is potentially facilitating illegal activity, a subpoena is an important tool to determine the facts. Abusive practices, especially in cases of payments fraud, are hard to detect. For fraudsters, this is by design – the best scams are those that go undetected for as long as possible. We should not deprive investigators of the information they need to determine if a financial institution is willingly enabling financial fraud.

H.R. 1413, the Firearms Manufactures and Dealers Protection Act 2015, Would Cut off Critical Funding to Prevent Fraud.

H.R. 1413 would prohibit federal agencies from using any funds to carry out Operation Choke Point – no matter what illegal conduct is targeted – or any program designed to discourage financial institutions from providing credit or payment processing for firearms or ammunition dealers. As discussed above, Operation Choke Point has nothing to do with gun dealers. Yet H.R. 1413 would completely defund DOJ's payment fraud activities, such as the cases described above against fraudsters who targeted seniors and others.

H.R. 1413 would also inhibit federal agencies from enforcing the Bank Secrecy Act and the Patriot Act if a financial institution's noncompliance or lax money-laundering controls happened to involve an account held by a firearm or ammunition dealer. Criminals could hide money laundering in the guise of gun sales. The bill could also restrict efforts to stop a bank account from being used for illegal activity if the owner of the account is a firearm or ammunition dealer.

DOJ Must Do More to Stop Payment Fraud, Which Hurts Everyone

Wrongdoers who access the payment system inflict harm on everyone. In addition to the direct victims of fraud:

- The general public spends millions of dollars on identity protection products and loses faith in the security of the payment system;
- Retailers and online merchants lose business if consumers are afraid to shop on their websites or at their stores;
- Consumers' banks bear the customer friction and the expense of dealing with an unauthorized charge – at an average cost of $100 and up to $509.90 for a smaller bank, according to NACHA;
- The fraudsters' banks may suffer regulatory or enforcement actions, lost customers, private lawsuits, and adverse publicity; and
- American security is put at risk when banks and processors that lack know-your-customer controls are used for money laundering for drug cartels, terrorist groups, and other criminals.

Operation Choke Point targets few but protects many.

Indeed, my only concern about Operation Choke Point is that it has not brought enough actions. The three cases that the Justice Department has brought in the last two years are just the tip of the iceberg. We have heard a regular litany of payment fraud cases, with new cases coming out every day. In some cases, fraudsters manage to hide their fraud from the financial institutions or payment processors who process the payments. But it is hard to believe that at least some of the banks that enabled the scams described earlier in my testimony did not know what was going on.

Conclusion

Fighting payment fraud should not be controversial. Everyone benefits from efforts to stop illegal activity that relies on the payment system. The tens of billions of dollars that Americans lose to fraud every year are just too great to abandon vigilance by banks that are in a position to stop illegal activity. I urge you to support DOJ's Operation Choke Point and other efforts to ensure that banks comply with know-your-customer requirements, conduct due diligence, and keep an eye out for signs of illegality. Everyone must do their part to protect the integrity of the payment system and to prevent illegal activity that harms millions of Americans, businesses and American security.

Thank you for inviting me to testify today. I would be happy to answer any questions.