AMERICANS
FOR FINANCIAL REFORM
ACCOUNTABILITY • FAIRNESS • SECURITY

Americans for Financial Reform
1629 K St NW, 10th Floor, Washington, DC, 20006
202.466.1885

July 15, 2014

Representative
United States House of Representatives
Washington, DC 20515

Re: Support Operation Choke Point and other efforts to fight payment fraud; oppose bills to curtail payment fraud work

Dear Representative:

Americans for Financial Reform and the undersigned community, consumer and civil rights groups urge you to support efforts to ensure that banks and payment processors avoid facilitating illegal activity by complying with longstanding due diligence requirements to know their customers, monitor return rates, and be alert for suspicious activity. Please oppose any bills to defund or weaken efforts to fight payment fraud or to insulate banks or payment processors that do not conduct appropriate due diligence or ignore red flags. We need every tool to fight data breaches, identity theft, scams, frauds, money laundering, and other illegal conduct.

Fraudsters Need Banks and Payment Processors to Access the Payment System

Many scams, frauds and illegal activity could not occur without access to the payment system. Banks and payment processors that originate payments play a critical role in enabling wrongdoers to debit victims' bank accounts and to move money around. Examples of unlawful activity that would not be possible without an originating bank include the following:

- A telemarketing scam defrauded seniors of $20 million by lying to them to get their bank account information.[1]
- A lead generator tricked people who applied for payday loans and used their bank account information to charge them $35 million for unwanted programs.[2]
- Bogus debt relief services scammed consumers out of $8 million and made their debt problems worse.[3]
- Wachovia Bank enabled $160 million in fraud by scammers targeting vulnerable seniors.[4]
- After an enforcement action against Wachovia, scammers moved their business to Zions Bank, which allowed it to continue despite spotting suspicious activity. For example, a

telemarketer calling a senior about a purported update to his health insurance card tricked him into revealing his bank account information.[5]

The FBI estimates that mass-marketing fraud schemes causes tens of billions of dollars of losses each year from millions of individuals and businesses,[6] and one study found that fraud drains $2.9 billion a year from the savings of senior citizens.[7] In addition, the data obtained in breaches like the recent Target, Michael's and P.F. Chang breaches would be useless without a bank to use that data to debit bank or credit cards accounts.

Banks are not always aware that they are being used to facilitate illegal activity. But when they choose profits in the face of blatant signs of illegality, they become an appropriate target for enforcement action. Indeed, if regulators do not take action against banks or payment processors facilitating illegal payments, they are left playing an impossible game of 'whack a mole' which makes it much too easy for fraudsters to get away with continuing to break the law, and processing institutions to continue to benefit from law-breaking.

Payment Fraud Hurts Everyone

Wrongdoers who access the payment system inflict harm on everyone. In addition to the *direct victims* of fraud, t*he 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 website or at their store. *Consumers' banks* bear the customer friction and the expense of dealing with unauthorized charges. *The fraudsters' banks and payment processors* may suffer regulatory or enforcement actions, lost customers, private lawsuits, and adverse publicity. *American security* is also 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.

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."[8] The focus is on illegal conduct, not activity that DOJ deems immoral.

The first, and to date only, action that DOJ has brought as a result of Operation Choke Point is U.S. v. Four Oaks Fincorp, Inc., Four Oaks Bank & Trust Co. Four Oaks enabled payments for illegal and fraudulent payday loans; an illegal Ponzi scheme that resulted in an SEC enforcement action;[9] a money laundering operation for illegal internet gambling payments;[10] and a recidivist prepaid card marketing scam that made unauthorized debits for a bogus credit line.[11] DOJ charged that the bank ignored blatant red flags of illegality, including extremely high rates 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.

This type of disregard for know-your-customer requirements and the legality of payments is what led to last month's $8.9 billion penalty against BNP Paribas for concealing billions of dollars in transactions for clients in Sudan, Iran and Cuba,[12] and to a $1.92 billion penalty against HSBC for helping terrorists, Iran, and Mexican drug cartels launder money.[13] It is impossible to read the Four Oaks complaint without concluding that Operation Choke Point is essential work for which DOJ should be applauded, not criticized.[14] Calls to abandon Operation Choke Point are misguided and inappropriate.

Regulators Have Appropriately Warned Banks to be Aware of High-Risk Activities, But Banks Need Not Reject Legal Businesses

Separate from DOJ's Operation Choke Point, bank regulators have asked banks to be aware of higher-risk activities, defined as areas with a "higher incidence of consumer fraud or potentially illegal activities."[15] As with Operation Choke Point, the focus of bank regulators is on areas where fraud or illegal activity is prevalent. For example, telemarketing, credit repair services, and debt forgiveness programs have long been problematic areas plagued with fraud and deceptive conduct. Payday lending is a high-risk activity because it is completely unlawful in 15 states, is unlawful in nearly every other state if the lender lacks a state license, and, especially for online lending, often results in repeated debits that the consumer did not knowingly authorize.

Regulators have also made clear that banks that "properly manage these relationships and risks are neither prohibited nor discouraged" from providing services to lawful customers in high-risk areas.[16] Banks need only be aware of the potential for illegal activities; know their customers, including basic due diligence of high-risk businesses;[17] monitor payment return rates; and be alert for suspicious activity. These are not new obligations, but they are essential ones.

Some recent headlines have drawn sweeping, unsubstantiated conclusions based on individual bank account closures. Banks close accounts every day for a variety of reasons. The bank that closed the account of the adult entertainer, for example, has stated unequivocally that it was unrelated to either Operation Choke Point or any policy concerning her profession.[18] The same is true of a gun dealer who was cut off by its payment processor.[19]

Even the National Rifle Association has said:

> "[W]e have not substantiated that [anti-gun groups' efforts] are part of an overarching federal conspiracy to suppress lawful commerce in firearms and ammunition, or that the federal government has an official policy of using financial regulators to drive firearm or ammunition companies out of business."

Concerns by payday lenders that they are being rejected by some banks go back a decade or longer, long before the 2013 Operation Choke Point or the FDIC's 2011 guidance on payment

processing relationships. For example, in 2006, the Financial Service Centers of America (FiSCA), which represents check cashers, money transmitters and payday lenders, testified:

> "For the past six years [since 2000] banks have been abandoning us - first in a trickle, then continuously accelerating so that now few banks are willing to service us …"[20]

Anecdotes about a few closed accounts do not prove regulatory overreach. The bank could have seen signs of illegality; terminated a problematic processor that had both illegal and legal clients; terminated businesses that lacked adequate controls; made its own business decision to cut ties with payday lenders after the bank suffered adverse publicity from its own payday lending; or misunderstood inflammatory headlines and regulatory signals.

Some bank account closures may also be related to anti-money laundering (AML) and Bank Secrecy Act issues that are separate from whether the business is considered a high-risk business. Some payday lenders with state licenses are also check cashers and money transmitters, areas that require compliance with complicated but important AML rules. Recent money laundering settlements may have drawn more attention to those rules, and the fact that Operation Choke Point is now in the news does not mean that every bank account closure is related.

Regulators are working to clear up any misconceptions created by overreaching headlines or exaggerated lobbyist claims, while also emphasizing the importance of work to prevent payment fraud. As FDIC Vice Chairman Thomas M. Hoenig said recently:

> [I]f the bank knows its customer, takes the necessary steps, has the right controls, then they ought to be able to engage with them…. But you need to do those things like BSA [compliance].… I do believe we have an obligation to say, "If you are following these rules, [you] have to then judge the risk that [you] are willing to take on." That's the process and I'm very comfortable with that.[21]

It is irresponsible and dangerous to halt scrutiny of banks and payment processors that close their eyes when they operate in areas with a high risk of illegality. There are thousands of banks in this country and plenty that will continue to handle high risk but lawful accounts. But the tens of billions of dollars that Americans lose to fraud every year and the harms permitted by money laundering are just too great to abandon all vigilance by banks and payment processors that are in a position to stop illegal activity.

Small Banks are Not a Target But May be Disproportionately At Risk

Banks large and small have received subpoenas and enforcement actions related to payment fraud. But small banks may be disproportionately likely to process illegal payments or be harmed by payment fraud. Some fraudsters target small banks that lack the internal controls to spot suspicious activity or that (like Four Oaks Bank) need capital and look the other way in exchange for fee income. High risk activities without due diligence are also more dangerous to the safety and soundness of a small bank.

Moreover, more small banks are hurt by payment fraud than facilitate it. When the scammer's bank submits an unauthorized charge against a consumer's account, the consumer's bank incurs expenses to deal with the mess. Those costs can be substantial for small banks. When a consumer contests an unauthorized payment, the average bank cost for handling a return is $4.99. But for a small bank the cost is much higher: the average is over $100 and can be as high as $509.90, according to NACHA, the Electronic Payments Association.[22]

The disproportionate impact of payment fraud on smaller banks is a reason to *continue* efforts to stop illegal activity. It is not a reason to halt such efforts.

Conclusion

Fighting payment fraud should not be controversial. Everyone benefits from efforts to stop illegal activity that relies on the payment system. We urge you to support efforts to ensure that banks and payment processors do their part and to hold them accountable when they fail to comply with know-your-customer requirements, conduct due diligence on high-risk activities, or overlook obvious signs of illegality.

Yours very truly,

Americans for Financial Reform
Arizona Community Action Association
Arkansas Against Abusive Payday Lending
California Reinvestment Coalition
Center for California Homeowner Association Law (Oakland, CA)
Center for Economic Integrity (Arizona)
Center for Responsible Lending
Coalition of Religious Communities
Chicago Consumer Coalition
Consumer Federation of America
Consumer Action
Consumers for Auto Reliability and Safety
Consumers Union
Economic Fairness Oregon
Florida Alliance for Consumer Protection
Kentucky Equal Justice Center
The Leadership Conference on Civil and Human Rights
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low income clients)
National Fair Housing Alliance
National People's Action
New Economy Project
NW Consumer Law Center
Public Citizen
Public Justice Center
Reinvestment Partners
South Carolina Appleseed Legal Justice Center

Texas Appleseed
U.S. PIRG
Virginia Citizens Consumer Council
Virginia Partnership to Encourage Responsible Lending
Virginia Poverty Law Center
Woodstock Institute

[1] *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.

[2] *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.

[3] *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.

[4] *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&.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] S.E.C. v. Rex Ventures Group, LLC d/b/a Zeekrewards.com, et al., Civil Action 12-CV-519 (W.D.N.C.).

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

[11] 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.

[12] Danielle Douglass, "France's BNP Paribas to pay $8.9 billion to U.S. for sanctions violations," Washington Post (June 30, 2014), available at http://www.washingtonpost.com/business/economy/frances-bnp-paribas-to-pay-89-billion-to-us-for-money-laundering/2014/06/30/6d99d174-fc76-11e3-b1f4-8e77c632c07b_story.html.

[13] Ben Protess and Jessica Silver-Greenberg, "HSBC to Pay $1.92 Billion to Settle Charges of Money Laundering," New York Times (Dec. 10, 2012), available at http://dealbook.nytimes.com/2012/12/10/hsbc-said-to-near-1-9-billion-settlement-over-money-laundering/.

[14] The complaint, which describes the fraud and the role of the bank and payment processor in detail, is available at http://www.courthousenews.com/2014/01/09/USvFourOaks.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.

[15] FDIC, Payment Processor Relationships, FIL-3-2012 (Jan. 31, 2012), available at http://www.fdic.gov/news/news/financial/2012/fil12003.html.

[16] FDIC, Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities, FIL-43-2013 (Sept. 27, 2013).

[17] For example, it is a simple matter to ask a payday lender in what state it lends and to show that it has licenses in those states.

[18] 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.").

[19] 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.

[20] Gerald Goldman, General Counsel of FiSCA, "Summary Of speech before the U.S. House Committee on Financial Services, Subcommittee on Financial Institutions & Consumer Credit , Regarding Banking Services to MSBs (June 21, 2006), available at http://www.fisca.org/Content/NavigationMenu/GovernmentAffairs/TestimonySpeeches/FiSCAHearingOralStmtGoldman_6_21_06.pdf.

[21] Kate Davidson and Zachary Warmbrodt, Q&A: Thomas Hoenig, Politico Pro (June 13, 2014).

[22] NACHA-The Electronic Payments Association, "Improving ACH Network Quality by Reducing Exceptions" at 6 (Nov. 11, 2013). The NACHA study does not give an average cost for small banks, but the un-weighted average for all banks is $100.52, so the average for smaller banks is undoubtedly higher than that. The weighted average for all banks, taking into account each bank's volume, is $4.99.