June 24, 2014

The Honorable Tim Johnson
Chairman
Committee on Banking, Housing and Urban Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

We are sending this letter to provide your committee with information regarding Operation Chokepoint, a series of investigations designed to protect consumers from mass-market fraud perpetrated by certain merchants, third-party payment processors, and banks. We appreciate this opportunity to describe our work and to clear up several misconceptions.

Simply put, the Department of Justice (the Department) has made it a priority to hold the perpetrators of consumer fraud accountable. Consumer fraud comes in many forms – from telemarketing fraud to mortgage fraud, from lottery scams to predatory and deceptive on-line lending – and often strips our most vulnerable citizens of their savings and even their homes. While there is seemingly no limit to the kinds of schemes that perpetrators of fraud will come up with, many of these schemes have one thing in common: they employ the banking system to take money from their victims. Once a fraudster can work his way into the banking system, he no longer has to convince unwitting consumers to hand over cash or mail a check. Instead, with the click of a button, he can debit their bank accounts and credit his own, repeatedly, without permission, and in violation of federal law – until somebody does something to stop it.

For decades, the Department, led by the Civil Division’s Consumer Protection Branch, has worked to protect the health, safety, and economic security of the American consumer. After years of combatting fraudulent merchants, we, along with our law enforcement and regulatory partners, have come to understand the role played by certain third-party payment processors – intermediaries between banks and merchants – in allowing fraudsters to gain access to our banking system and consumers’ bank accounts. In some cases, these payment processors open bank accounts in their own names and, for a fee, use these accounts to conduct banking activities on behalf of their customers. While some customers are legitimate businesses, others are fraudulent merchants who either do not or cannot (because banks will not do business with them) open their own bank accounts. At the merchants’ direction, the processor will initiate debit transactions against consumers’ accounts and transmit the money to the fraudulent merchant.
By following the flow of money from fraudulent transactions, we have learned that some third-party payment processors know their merchant clients are engaged in fraud and yet continue to process their transactions - in violation of federal law. Further, we have come to understand that some banks, in violation of the law, either know about the fraud they are facilitating or are consciously choosing to look the other way. As a result, in November 2012, our attorneys proposed a new approach: to pursue the fraud committed by the banks and payment processors. This strategy aims both to hold accountable those banks and processors who violate the law and to “choke off” access to the banking system by the many fraudulent merchants who had come to rely on the conscious assistance of banks and processors in facilitating their schemes. This effort is sometimes referenced as Operation Chokepoint.

Using a variety of public and nonpublic sources, we assembled evidence of fraudulent activity by specific fraudulent merchants, payment processors, and banks. That information included statements of cooperating witnesses; tips and referrals from defrauded consumers and banks whose customers had been victimized; and evidence obtained during investigations of fraudulent merchants identifying third-party payment processors or banks that participated in the merchants’ unlawful conduct.

In addition, we obtained information from the Federal Reserve Bank in Atlanta concerning banks with abnormally high “return rates” - one possible indicator of potential fraud. “Return” or “chargeback” rates refer to the percentage of transactions that are reversed. In addition to “unauthorized” returns, which represent an explicit claim that a consumer did not authorize a debit, a high rate of “total” returns also indicates potential fraud. For example, returns due to insufficient funds may reflect consumers who had money taken from their accounts unexpectedly or repeatedly, without authorization. Returns due to a closed account may reflect consumers who were forced to close their bank accounts as a consequence of unauthorized debits.

Based on these and other sources, between February and August 2013, the Consumer Protection Branch issued civil subpoenas to specific banks, processors, and other entities for which the Department had evidence suggesting possible fraud. We then reviewed the information provided in response to those subpoenas and, depending upon the nature of the evidence, we closed the file, or sought additional information, or determined to pursue a civil or criminal investigation.

One of those investigations has now been resolved, and its resolution demonstrates exactly the type of troubling relationship between a bank and a set of fraudsters that gave rise to the Department’s effort. On April 25, 2014, the U.S. District Court for the Eastern District of North Carolina entered a consent order and approved a settlement resolving the Department’s complaint against Four Oaks Bank. According to the complaint, Four Oaks allowed a third-party payment processor to facilitate payments for fraudulent merchants despite active and specific notice of the fraud, including:

- Four Oaks received hundreds of notices from consumers’ banks - submitted under penalty of perjury - that the people whose accounts were being charged had not authorized the debits from their accounts.
The Honorable Tim Johnson
Page Three

- Four Oaks had evidence that more than a dozen merchants served by the payment processor had a “return rate” over 30 percent – a strong sign the bank was facilitating repeated fraudulent withdrawals. Indeed, one merchant had a return rate of over 70 percent.¹

- Four Oaks had evidence of efforts by merchants to conceal their true identities.

According to the Department’s complaint, despite these and many other signals of fraud, Four Oaks permitted the third-party payment processor to originate approximately $2.4 billion in debit transactions against consumers’ bank accounts, for which the bank received more than $850,000 in fees. As a result, many American consumers were defrauded of their hard-earned savings.

The consent order, agreed to by Four Oaks and approved by the court, requires Four Oaks Bank to pay $1 million to the U.S. Treasury as a civil monetary penalty and to forfeit $200,000 to the U.S. Postal Inspection Service’s Consumer Fraud Fund. It also obligates Four Oaks to take steps to prevent future consumer fraud.

As the Four Oaks Bank case demonstrates, the Department bases its investigations on specific evidence of unlawful conduct. Nevertheless, in recent months, we have become aware of reports suggesting that these efforts instead represented an attack on businesses engaged in lawful activity. Indeed, some media reports claim that the Department has deemed certain industries “high risk.” Our policy is to investigate specific conduct, based on evidence that consumers are being defrauded – not to target whole industries or businesses acting lawfully. Our investigations follow the facts and the law wherever they lead us, regardless of the type of business involved. In fact, we think this endeavor demonstrates the importance of holding financial institutions accountable when they profit from and participate in fraudulent activities, just as we hold accountable any other entity that engages in unlawful conduct.

As with virtually all of our law enforcement work that touches upon highly regulated industries, our work in this area includes communication with relevant regulatory agencies, here including the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and the Federal Reserve Board. Such communication ensures that we understand the industry at issue, that our investigations do not unnecessarily or improperly frustrate regulatory efforts, and that we have all the information needed to evaluate the enforcement options available to address violations that our investigations uncover.

Federal law requires banks to “know their customers” in a variety of ways and to report instances of suspicious activity in order to prevent money laundering, consumer fraud, and other illegal behavior. Banks know this, and most have instituted programs to comply with these longstanding requirements. Indeed, because of these programs, many fraudulent merchants have difficulty engaging directly with banks and have come to rely on third-party payment processors for access to the banking system. Noting this trend, the FDIC – as part of its regulatory

¹ By comparison, the overall return rate for all transactions over the nation’s automated clearing house network is approximately one and a half percent.
responsibilities – has warned banks about the heightened risks to consumers associated with third-party payment processors," and has explained that, "[a]lthough many clients of payment processors are reputable merchants, an increasing number are not and should be considered ‘high risk.’" The FDIC’s list of “high-risk merchants” was developed for purposes relevant to its regulatory mission. The Department’s mission is to fight fraud, and we recognize that an entity’s simply doing business with a merchant labeled “high risk” is not fraud. Indeed, we recognize that most of the businesses that use the banking system – even those in industries that regulators deem “high risk” – are not engaged in fraud, and we are dedicated to ensuring that our efforts to combat fraud do not discourage or inhibit the lawful conduct of honest merchants.

Our efforts to protect consumers by flushing out fraudulent banking activity are not focused on financial institutions that merely fail to live up to their regulatory obligations or that unwittingly process a transaction for a fraudulent merchant. We are fighting fraud. When banks either know or are willfully ignorant to the fact that law-breaking merchants are taking money out of consumers’ bank accounts without valid authorization, and they continue to allow that to happen, that is not just a concern for bank regulators. That is fraud, and it can result in true devastation for consumers. When any entity – whether it is a merchant, a third-party payment processor, or a bank – commits fraud against consumers, the Department will not hesitate to enforce the law.

---

4 According to the Department’s complaint against Four Oaks Bank, many of the fraudulent merchants for which Four Oaks provided access to the banking system were engaged in online short-term lending, one of the “high-risk” activities listed in the FDIC guidance. However, while law enforcement officials and regulators at the federal and state levels have expressed concern about unlawful activity in the online short-term lending industry for several years, Department officials have made clear on numerous occasions that the Department has no interest in pursuing or discouraging businesses engaged in lawful conduct. The Department would only be interested in the conduct of online short-term lenders, or any merchant, to the extent that conduct violates the law.
We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

Peter J. Kadzik
Assistant Attorney General

cc: The Honorable Mike Crapo
    Ranking Member

cc: Members of the Committee