Department of Justice

STATEMENT

OF

STUART F. DELERY
ASSISTANT ATTORNEY GENERAL
CIVIL DIVISION

BEFORE THE
SUBCOMMITTEE ON REGULATORY REFORM, COMMERCIAL AND ANTITRUST LAW
COMMITTEE ON JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

FOR A HEARING RELATED TO

“OPERATION CHOKE POINT”

PRESENTED ON

JULY 17, 2014

Statement of Stuart F. Delery
Assistant Attorney General, Civil Division
Before the U.S. House of Representatives
Committee on Judiciary
Subcommittee on Regulatory Reform, Commercial and Antitrust Law
July 17, 2014

Chairman Bachus, Ranking Member Johnson, and Members of the Subcommittee, thank you for inviting me here and for providing the Department of Justice the opportunity to appear at today's hearing to describe our work designed to protect consumers from fraud perpetrated by certain merchants, third-party payment processors, and banks.

As the Attorney General has said, the Justice Department has made it a priority to fight consumer fraud of all kinds and to hold the perpetrators 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 invent, many of these schemes have one thing in common: they employ the banking system to take money from their victims. Once a fraudulent merchant 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.

The Civil Division's Consumer Protection Branch—along with the Criminal Division and United States Attorney's Offices across the country—has worked for decades to protect the health, safety, and economic security of the American consumer. Based on its years of experience in combating fraudulent merchants, the Department, along with our law enforcement and regulatory partners, recognizes the critical role played by a limited number of third-party payment processors—intermediaries between banks and merchants—in allowing fraudulent merchants 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 choose not to open their own bank accounts or cannot do so because banks will not do business with them. At the merchants' direction, the processor will initiate debit transactions against consumers' accounts and transmit the money to the fraudulent merchant.

Guided by the facts and the law, and by following the flow of money from fraudulent transactions, the Department has 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, our experience in these cases has been 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 concentrated effort 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 prevent 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.

To begin the effort, using a variety of public and nonpublic sources, the Consumer Protection Branch 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 that identified third-party payment processors or banks participating in the merchants' unlawful conduct.

In addition, we obtained information from the Federal Reserve Bank of 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 in a transaction account, 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 specific evidence suggesting that those entities might be engaged in fraud or might have evidence of fraudulent conduct by others. We then reviewed the information provided in response to those subpoenas and, depending upon the nature of the evidence, we sought additional information, determined to pursue a civil or criminal investigation, or closed the file.

One of those investigations now has been resolved, and its resolution demonstrates exactly the type of troubling relationship between a bank and a set of perpetrators of fraud 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 agreed to by the Department and Four Oaks Bank. According to the Department's 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.

- 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.

- 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 of the bank's actions, 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's policy is to base 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. I thank you for this opportunity to clear up this misconception. Our policy is to investigate specific conduct, based on evidence that consumers are being defrauded—not to target whole industries or businesses acting lawfully, and to follow the facts wherever they lead us, in accordance with the law, regardless of the type of business involved. We think this endeavor demonstrates the importance of holding financial institutions accountable when they 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 is designed to ensure 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 are aware of these laws, and most have instituted programs to comply with these longstanding requirements. Indeed, it is because of these programs that 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 responsibilities—has warned banks about the heightened risks to consumers associated with third-party payment processors in its Guidance on Payment Processor Relationships first issued in 2008, 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 has provided examples of "high-risk merchants" 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 considered "high risk" is not fraud.

Indeed, we recognize that most of the businesses that use the banking system—even those in industries considered "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. While the Department's complaint against Four Oaks Bank demonstrates that many of the fraudulent merchants for which Four Oaks provided access to the banking system were engaged in illegal online short-term lending, we follow the facts where they lead us. The Department would only be interested in the conduct of an online short-term lender, or any merchant, to the extent that its conduct violates the law.

I thank you for this opportunity to reiterate what I and other Department officials have made clear on numerous occasions: that the Department is seeking to protect consumers from fraudulent practices in all industries and has no interest in pursuing or discouraging businesses engaged in lawful conduct. The Attorney General said this in a recent video posted publicly on the Department website. The Department has said this in response to Congressional inquiries. And the Department has said this many times to industry groups, including in a letter I wrote to the American Bankers Association and the Electronic Transaction Association.

Our efforts to protect consumers by pursuing 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 a bank either knows or is willfully ignorant to the fact that law-breaking merchants are taking money out of consumers' bank accounts without valid authorization, and the bank continues 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. We will continue to pursue our mission to protect honest, hardworking Americans from those who put their financial security in peril.

Thank you, once again, for the opportunity to appear before you today. At this time, Mr. Chairman, I would be happy to address any questions you or Members of the Subcommittee may have.