NCLC®
NATIONAL CONSUMER LAW CENTER®

BOSTON HEADQUARTERS
7 Winthrop Square, Boston, MA 02110-1245
Phone: 617-542-8010 • Fax: 617-542-8028

WASHINGTON OFFICE
1001 Connecticut Avenue NW, Suite 510, Washington, DC 20036
Phone: 202-452-6265 • Fax: 202-463-9462

www.nclc.org

January 13, 2014

The Honorable Eric H. Holder, Jr.
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue
Washington, DC 20530

Re: DOJ's critical payment fraud and money laundering work

Dear Attorney General Holder:

On behalf of our low income clients, I am writing to congratulate you on your action against Four Oaks Bank & Trust and to urge you to continue the critically important work the Department of Justice (DOJ) is undertaking to combat payment fraud and money laundering. There has already been pressure to desist and we expect that there will be more.[1] But at a time when the Target data breach reminds us of the threats to our financial system, your work is essential to protect the security of Americans' bank accounts and indeed American security overall.

The Four Oaks action addresses a bank's complicity in payment fraud, plain and simple, involving not just illegal and fraudulent payday loans but also Ponzi schemes and money laundering for illegal online gambling. Anyone concerned about combatting fraud or money laundering should be applauding vigorous efforts to stop this type of conduct, whether the setting is payday lending, telemarketing scams, senior frauds, or payments that fund terrorism.

The Four Oaks complaint reveals the bank's shocking disregard for its legal obligation to know its customers, comply with the Bank Secrecy Act, and avoid facilitating fraud and illegal payments.[2] The bank gave a payment processor direct access to the ACH system, bypassing bank controls, despite:

- **Extremely high return rates.** The bank knew of the processor's "really high chargebacks" at its former bank, with more than 8,000 unauthorized transactions and merchants that had exceeded NACHA return thresholds in 7 out of 10 months. The bank later ignored unauthorized returns of seven times the level permitted by NACHA. The bank's board of directors authorized total merchant returns of up to 30%, far above the national average of 1.5%, a ridiculously high level tailored to the unscrupulous payment processor and its clients. Yet the bank kept the processor as a client even after some merchants' returns ranged from 31% to 70%.

- **Efforts to hide merchants' identities.** The bank approved ACH processing for merchants despite knowledge that merchants were using a vacant lot as a business address, had changed names to avoid scrutiny, used false Social Security numbers, or claimed to be a United States entity while in fact operating off shore.

- **Offshore entities evading U.S. laws.** Merchants were located in Belize, Costa Rica and other countries in a clear attempt to evade American law. When the bank pointed out that one merchant was unlicensed and was violating state and federal law, the processor replied "Its why lenders choose to be offshore. They don't want to have to deal with each state's laws …." The bank continued providing ACH access to another merchant after discovering that the merchant was owned by a resident of another country despite the processor's representation that it was a

U.S. entity. Returns later topped 70%. In April 2013, 25% of the processor's transactions were purportedly for overseas companies.

- **Disregard for Bank Secrecy Act obligations.** The bank gave ACH access to merchants it could not identify and on whom it could not perform any due diligence. One bank official pointed out that "From a [BSA] perspective, we have a high risk business, owned by a foreign person that we can't due diligence, born in a 'country of concern,' living in a 'county of concern.'" One merchant was "a corporation, owned by a corporation, which is owned by another corporation," and the bank was unable to locate sufficient information about the main company. Other merchants maintained anonymity from the public and the bank itself through corporate layering, sham contractual relationships, fictitious names and other artifices. The bank failed to complete risk matrices for 42 of 68 of the processor's merchants, and then scrambled to re-create them "prior to the examiners arriving."

- **Failure to address NACHA warnings of violations.** NACHA sent the bank several letters about potential ACH rule violations, but the bank ignored those warnings and continued to process transactions against consumer accounts.

- **Illegal and fraudulent conduct concealed through nested payment processors**. The bank permitted the processor to process payments for other payment processors, called "nesting," which can be used to hide a merchant's identity or business. Even after learning about a federal prosecution of one merchant for money laundering of illegal internet gambling payments,[3] with $6 million in the processor's account at the bank connected to illegal conduct, the bank continued to rely on the processor to vet new merchants. Another merchant of a nested payment processor was conducting an illegal Ponzi scheme that resulted in an SEC enforcement action.[4]

- **Fraud against consumers**. The bank ignored hundreds of Requests for Proof of Authorization submitted by the receiving banks in which their customers stated under penalty of perjury that the payments were unauthorized. Eventually the bank stopped even keeping a log of the Requests. Consumer complaints revealed significant problems with consumers being deceived and misled. While conducting due diligence on the proposed fictitious names of one new merchant, a bank employee discovered "many, many" consumer complaints, along with a state cease and desist order. But a senior bank officer overrode those concerns, noting "to deny [the merchant] based on consumer complaints, I think we'd need to look at shutting down the current business …."

- **Deliberate ignorance of the legality of payments**. The processor told a senior bank official: "we do not ask" if the merchant lenders for which it processed payments are licensed. "Asking opens legal issues that are not worth the time or trouble. I want no legal responsibility for whether it is it [sic] legal to lend …. It is irrelevant to the business we do with them …." The official agreed not to push for licensing information, despite observing "You don't think there's huge potential liability for ignoring the fact that certain transactions could potentially be illegal, and not doing the due diligence and monitoring to ensure they aren't?... I'm not sure 'don't ask/don't tell' is going to be a reasonable defense …." The bank ignored complaints from state enforcement authorities and evidence that it was processing payments for illegal loans.

- **Federal law violations.** The bank continued processing payments for merchants despite evidence of violations of the Electronic Funds Transfer Act, the FTC's Credit Practices rule, and unlawful debt collection practices.

These are precisely the elements that are present whenever banks process payments for fraud artists, including scams against seniors and identity thieves. For example, similar problems at Wachovia Bank a few years ago permitted $160 million in fraud against seniors.[5] Banks play a critical role in

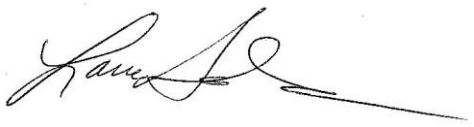
enabling these scams to continue and to inflict immense damages on the American public. It is entirely appropriate for DOJ to target banks that flagrantly ignore their legal obligations and turn a blind eye to fraud.[6]

Efforts to combat terrorism, drug cartels and other threats to American security also depend on banks' complying with their legal obligations to know their customers and their customers' customers. A bank that has lax controls about the legality of payments and oversight over where the money ends up can be a weak link permitting money laundering for criminals of all types.

We applaud your efforts to protect the American public by addressing clear legal violations and payment fraud. Businesses, including payday businesses, that operate within the law have nothing to fear from efforts to stop payments that facilitate illegal transactions. The Department's focus on the banks that shirk their legal obligations will stop fraudsters at the outset, prevent hundreds of millions of dollars of fraud inflicted against consumers, protect the U.S. payment system, and bolster American security.

We thank you for your efforts to protect the public and urge you to continue.

Yours very truly,



Lauren K. Saunders
Managing Attorney

---

[1] *See, e.g.*,Brendan Bordelon, "Issa suspects Eric Holder is illegally targeting online lending," Daily Caller (Jan. 10, 2014), available at http://dailycaller.com/2014/01/10/issa-suspects-eric-holder-is-illegally-targeting-online-lending/.
[2] *See* Complaint for Injunctive Relief and Civil Monetary Penalties, United States v. Four Oaks Fincorp, Inc., and Four Oaks Bank & Trust Company, (E.D. N.C. Jan. 8, 2014), available at http://www.courthousenews.com/2014/01/09/USvFourOaks.pdf.
[3] United States v. Pokerstars, et al., 11-CV-02564 (S.D.N.Y.).
[4] S.E.C. v. Rex Ventures Group, LLC d/b/a Zeekrewards.com, et al., Civil Action 12-CV-519 (W.D.N.C.).
[5] *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&.
[6] A few months ago we sent a letter to DOJ and the bank regulators describing how efforts to address banks' role in payment fraud are critical parts of traditional supervision efforts and a broader federal effort to combat fraud. That letter is available at http://www.nclc.org/images/pdf/high_cost_small_loans/payday_loans/letter_bankinregulators_paymentprocessing.pdf.