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
"Examining Regulatory Relief Proposals for Community Financial Institutions, Part II"

Before the Before the House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit

July 15, 2014

Chairman Capito, Ranking Member Meeks 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 Operation Choke Point and in opposition to H.R. 4986, which would undermine important efforts underway at the Department of Justice and banking regulators designed to ensure that banks do not facilitate illegal activity. I urge you to oppose any bills to weaken the ability of regulators to fight payment fraud or to insulate banks that do not comply with the law or that willfully ignore signs that they are enabling fraud, scams and other illegal conduct. We need every tool to fight data breaches, identity theft, scams, frauds, money laundering, and other illegal conduct.

I will first explain why vigilance by banks is so important to stop illegal activity. I will then discuss H.R. 4986 and will explain why it is inappropriate to immunize banks that fail to conduct due diligence or ignore red flags of illegality merely because the entity holds a state license, is registered as a money transmitter, or can find an attorney to say its conduct is legal.

In brief, merely holding a state license is no guarantee that an entity is acting legally, is not engaged in fraud or deceptive conduct, or is complying with laws designed to prevent money laundering or other illegal activity. Vigilance over money transmitters is essential to prevent fraudsters from concealing themselves and to prevent money laundering and financing for drug cartels and terrorism. Finally, fraudsters have lawyers who are willing to defend them, but the idea that a bank should be able to take a fraudster's attorney's word for the legality of payments and to ignore other signs of illegality is simply astounding.

I also join the testimony of Marcus Stanley of Americans for Financial Reform expressing serious concerns about the discussion draft of The Access to Affordable Mortgages Act of 2014, which would exempt "higher-risk mortgages" of $250,000 or under less that are held on the lender's balance sheet from new appraisal requirements included in the Dodd-Frank Act. The exemption would expose both consumers and financial institutions to the risks of an inflated appraisal.

Fraudsters Need Banks to Access the Payment System

Many scams, frauds and illegal activity could not occur without access to the consumer's bank or credit card accounts through the payment system. Banks 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 rely on an originating bank to process payments include the following:

- A $600 million internet pyramid and Ponzi scheme shut down by the SEC.[1]
- A telemarketing scam defrauded seniors of $20 million by lying to them to get their bank account information.[2]
- A lead generator tricked people who applied for payday loans and used their bank account information to charge them $35 million for unwanted programs.[3]
- Bogus debt relief services scammed consumers out of $8 million and made their debt problems worse.[4]
- Wachovia Bank enabled $160 million in fraud by scammers targeting vulnerable seniors.[5]
- 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.[6]
- Just last week, 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.[7]

The FBI estimates that mass-marketing fraud schemes cause tens of billions of dollars of losses each year from millions of individuals and businesses.[8] A MetLife study found that fraud drains $2.9 billion a year from the savings of senior citizens.[9] In addition, the data obtained in

breaches like the recent Target, Michael's and P.F. Chang breaches would be useless without a bank willing to use that data to debit bank or credit cards accounts.

Even when consumers voluntarily authorize a payment from their account to purchase a product or repay a loan, they may find that their account is repeatedly debited for fees or charges they did not authorize or additional products they did not buy. Just last month, a judge agreed with the FTC that a payday lender had deceived consumers about the cost of their loans by imposing undisclosed charges and inflated fees that were automatically deducted from their bank accounts.[10] Those deductions could not have been made without a bank to process the debits.

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 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 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:

- 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 website or at their store;

- Consumers' banks bear the customer friction and the expense of dealing with unauthorized charges;
- 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.

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."[11] 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;[12] a money laundering operation for illegal internet gambling payments;[13] and a prepaid card marketing scam that made unauthorized debits for a bogus credit line.[14] 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,[15] and to a $1.92 billion penalty against HSBC for helping terrorists, Iran, and Mexican drug cartels launder money.[16]

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.[17] 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."[18] 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. For example, the Four Oaks complaint described how many consumers were defrauded when they authorized a single payment from their bank account but found that the payday lenders debited their accounts repeatedly, without authorization, and would not stop.

Banks are permitted to provide services for entities that operate in high-risk areas as long as the bank undertakes due diligence to obtain reasonable assurances that the entity is operating legally. Regulators have 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.[19] Banks need only be aware of the potential for illegal activities; know their customers, including basic due diligence of high-risk businesses;[20] 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.[21] The same is true of a gun dealer who was cut off by its payment processor.[22]

Indeed, 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 …"[23]

Anecdotes about a few closed accounts do not prove regulatory overreach. Banks close accounts for many reasons that may be unrelated to regulatory pressure or may be an appropriate response to regulatory guidance. Among other reasons, the bank could have:

- seen signs of illegality or fraud, even with a licensed entity, such as high rates of payments challenged as unauthorized;
- terminated a problematic payment processor that had both illegal and legal merchant clients;
- terminated businesses, like a payday lender that also does money transmitting, that lacked adequate controls to prevent money laundering;
- made the bank's own business decision to cut ties with payday lenders after the bank suffered adverse publicity from its own triple-digit deposit advance payday lending;

- eliminated unprofitable accounts in areas where the risks of illegality are not worth the effort to conduct due diligence; or
- misunderstood regulatory signals and inflammatory headlines.

Some bank account closures may 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 to it.

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.[24]

It is irresponsible and dangerous to halt scrutiny of banks 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 vigilance by banks 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, enforcement actions and regulatory guidance related to payment fraud. But small banks may be disproportionately likely to process illegal payments and, even more so, are disproportionately likely to 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 additional revenue and are willing to look the other way in exchange for fee income. High risk activities without due diligence are especially dangerous to the safety and soundness of a smaller bank, particularly one that is undercapitalized.

On the flip side, more small banks are on the receiving end of illegal payments, not the originating end, and are themselves victims of payment fraud facilitated by other banks. When the scammer's bank submits an unauthorized charge against a consumer's account, the consumer's bank incurs expenses to resolve the issue.

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.[25]

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.

H.R. 4986 Would Immunize Banks that Ignore Signs of Illegal Conduct and Would Undermine Essential Efforts to Fight Money Laundering, Payment Fraud and Illegal Activity

H.R. 4986 provides a highly problematic safe harbor for financial institutions that knowingly process payments for unlicensed merchants and fraudsters or willfully ignore signs of illegality. The bill also curtails the Department of Justice's ability to compel the production of important information necessary to determine if banks are facilitating illegal activity.

The bill forbids regulators from prohibiting, restricting or discouraging financial institutions from providing any product or service to an entity that:

- is licensed and authorized to offer such product or service;
- is registered as a money transmitting business; or
- has a "reasoned" legal opinion from a state-licensed attorney that purports to demonstrate the legality of the entity's business under applicable Federal and State law, tribal ordinances, tribal resolutions, or tribal-State compacts.

That is, regulators could not discourage financial institutions from providing processing services to an entity even if the institution observed alarmingly high levels of payments

challenged as unauthorized, was warned by federal or state law enforcement officials that the entity appeared to be engaged in fraudulent or deceptive conduct, knew that the entity had numerous court orders against it, or saw signs that the entity was attempting to conceal unlawful activity.

The fact that an entity holds a state license is no guarantee that it will not engage in unlawful activity. CashCall, Inc. for example, is a licensed lender in many states. But the CFPB has charged that CashCall, acting as a servicer and debt collector on payday loans made by Western Sky, debited consumer checking accounts for money they did not owe and continued debiting accounts even after Western Sky shut down its operations in response to numerous state enforcement actions and court orders.[26] CashCall has also faced prosecution by state attorneys general for its own lending activities, and California is in the process of revoking its license.

Yet, under H.R. 4986, regulators would not be permitted to advise financial institutions of the risks of processing payments for CashCall or from discouraging financial institutions from processing payments for entities facing similar government enforcement activity. The bill would not only permit continued debiting of consumer accounts for unlawful payments, it would also put financial institutions at risk of liability for chargebacks and legal action by consumers and others.

Similarly, even if an entity is registered as a money transmitting business, it could be violating the law or facilitating money laundering, consumer fraud, or other illegal activity. For example, Arizona Attorney General Tom Horne recently obtained a $94 million settlement with

Western Union, which was sending "blood wires" that permitted organized criminal cartels to smuggle money across the Arizona border. Attorney General Horne took the action to protect Arizonans from border violence, gun running, and human and narcotic smuggling along the southwest border.[27]

Under H.R. 4986, if a financial institution was serving a licensed money transmitter that was facilitating similar conduct, regulators could not discourage the activity or advise the financial institution of the risks.

Finally, virtually any criminal can find an attorney to defend its conduct, and sometimes the criminal hides the facts even from its own attorney. A legal opinion by an attorney that an activity is permissible should not absolve a financial institution from its obligation to conduct due diligence on of the third parties with which it does business and to keep its eyes open for suspicious activity. Financial institutions have clear guidance from regulators about how to manage relationships with third parties, including payments processors, and a letter from the third party's attorney cannot trump that guidance.

While this provision will aid any fraudster who has the ability to hire an attorney to write a letter on its behalf, it may have a particular impact on stopping regulators from advising financial institutions of the risks if they process payments for purportedly tribal entities that conduct activities off reservation in violation of state law. The Supreme Court's recent decision in the *Bay Mills* case should have made clear that tribes must obey state law when they act off reservation even if they have a license issued by a tribal entity to conduct business on tribal land.

A state "can shutter, quickly and permanently, an illegal casino," and the same is true of an illegal payday loan operation, by denying a license, obtaining an injunction, and even using the criminal law.[28] Yet even if the legality of unlicensed tribal payday lending is still up for debate, financial institutions that process electronic payments over the ACH system and remotely created checks over the check system provide warranties about the validity of those payments. If the payments turn out to be unlawful, the financial institution is on the hook to the consumer's bank, and a letter from the payday lender's attorney will not help. Regulators are only doing their duty to look out for the safety and soundness of financial institutions when they advise them of these high risk activities designed to evade state law.

H.R 4986 also curtails the Department of Justice's ability 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 – so we cannot tie the hands of the regulators charged with enforcing the law. Regulators must have the ability to examine financial institutions, ensure that appropriate compliance procedures are in place, and when necessary, issue subpoenas, to detect fraud and investigate potential abuses.

Conclusion

Fighting payment fraud should not be controversial. Everyone benefits from efforts to stop illegal activity that relies on the payment system. I urge you to oppose H.R. 4986 and other

measures that would undermine efforts to ensure that banks comply with know-your-customer requirements, conduct due diligence on high-risk activities, 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.

---

[1] *See* 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.

[2] *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.

[3] *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.

[4] *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.

[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] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

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

[14] 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.
[15] 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.
[16] 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/.
[17] 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.
[18] FDIC, Payment Processor Relationships, FIL-3-2012 (Jan. 31, 2012), available at http://www.fdic.gov/news/news/financial/2012/fil12003.html.
[19] FDIC, Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities, FIL-43-2013 (Sept. 27, 2013).
[20] 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.
[21] 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.").
[22] 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.
[23] 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.
[24] Kate Davidson and Zachary Warmbrodt, Q&A: Thomas Hoenig, Politico Pro (June 13, 2014).
[25] 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.
[26] "CFPB Sues CashCall for Illegal Online Loan Servicing," Consumer Financial Protection Bureau (December 13, 2013) available at http://www.consumerfinance.gov/newsroom/cfpb-sues-cashcall-for-illegal-online-loan-servicing/
[27]Arizona Attorney General, "Western Union: CUTTING OFF THE ILLEGAL CASH FLOW: $94 Million Settlement to Aid Law Enforcement in Fighting Border Crime" (Feb. 3, 2014), available at https://www.azag.gov/border-security/western-union.
[28]Michigan V. Bay Mills Indian Community et al., 134 S.Ct. 2024, 2035 (2014).