IMMIGRATION POLICY CENTER
AMERICAN IMMIGRATION COUNCIL

PERSPECTIVES

HOW TO FIX A BROKEN BORDER:
FOLLOW THE MONEY

PART III OF III

By Terry Goddard

MAY 2012

HOW TO FIX A BROKEN BORDER:

FOLLOW THE MONEY

PART III OF III

BY TERRY GODDARD

MAY 2012

ABOUT PERSPECTIVES ON IMMIGRATION

The Immigration Policy Center's *Perspectives* are thoughtful narratives written by leading academics and researchers who bring a wide range of multi-disciplinary knowledge to the issue of immigration policy.

ABOUT THE AUTHOR

Terry Goddard completed his second and final term as Arizona's Attorney General in January 2011 and has reentered the private practice of law. A native of Tucson, Arizona, and graduate of Harvard College, he was first elected Arizona Attorney General in 2002. Over eight years in office, he focused on protecting consumers and fighting the organized criminal activities of the drug cartels. He made significant progress in attacking cartel money laundering, seizing approximately $20 million and culminating in an historic $94 million settlement with Western Union in February 2010. He received the Kelly-Wyman Award for 2010, the top recognition given by his fellow Attorneys General. Terry's first job out of ASU law school in 1976 was prosecuting corporate fraud. During his legal career, he has handled a wide variety of cases, from a challenge to a federal highway route to election law matters before the state Supreme Court. Before law school, he served on active duty in the Navy, retiring as a commander after 27 years in the Reserves. Mr. Goddard is currently teaching at Columbia Law School in the Attorney General Project. He also teaches a graduate course entitled "The Art of Public Decision Making" at Arizona State University School of Public Affairs. He has been selected a Wasserstein Fellow at Harvard Law School and is a Senior Fellow at the American Immigration Council. Terry lives in Phoenix with his wife Monica and teenage son.

ABOUT THE IMMIGRATION POLICY CENTER

The Immigration Policy Center, established in 2003, is the policy arm of the American Immigration Council. IPC's mission is to shape a rational conversation on immigration and immigrant integration. Through its research and analysis, IPC provides policymakers, the media, and the general public with accurate information about the role of immigrants and immigration policy in U.S. society. IPC reports and materials are widely disseminated and relied upon by press and policymakers. IPC staff regularly serves as experts to leaders on Capitol Hill, opinion-makers, and the media. IPC is a non-partisan organization that neither supports nor opposes any political party or candidate for office. Visit our website at www.immigrationpolicy.org and our blog at www.immigrationimpact.com.

Introduction

For all the political rhetoric and chest pounding about border security in recent years, the U.S. has done very little, and politicians have said almost nothing about, the need to cut off the funds flowing illegally across the southwest border and feeding the drug cartels. The most basic, the most effective approach to fighting organized crime has always been to cut off their funds. But this is not being done in the case of the cartels. Billions of dollars in illegal revenue from the sale of drugs and other contraband continues to flow into cartel pocketbooks, as well as to criminals within the U.S. The money pours over the border by many means, from bulk cash shipments and wire transfers to funnel bank accounts and stored value instruments. Most of these transactions clearly violate anti-money laundering laws. Yet, rather than disrupting this flow of cash, the U.S. government expends almost all of its border security resources building more fences and chasing would-be workers through the desert.

By letting so much illegal cash literally flow through its fingers, the United States is making sure that the cartels have the resources they need to attack and defeat our border defenses.

Only recently has the Department of Homeland Security been making substantial seizures of bulk currency headed south. The totals are impressive—over $150 million in bulk currency seized in fiscal year 2011 (up from $7.3 million in 2005).[1] However, compared to the billions headed to Mexico, this is a drop in the bucket. The National Drug Intelligence Center has estimated the amount of money flowing from the United States to Mexico from the sale of illegal drugs in this country at between $19 billion and $39 billion per year.[2] That number is four years old and undoubtedly low. Revenue from the total sale of drugs in the United States was estimated last year to be $64 billion.[3] More recently, the number was placed at "over $85 billion by a Justice Department official."[4] Human smuggling into the United States, according to a United Nations estimate, brings in over $6 billion more.[5]

Although some cartel funds are used to purchase guns and other products and services in the United States, most of the cartel revenues must be moved back across the border. And, because of changes in Mexican law in 2010 restricting the holding of dollars by Mexican citizens, the dollars must be converted to pesos. This torrent of cash pays for the highly trained personnel who are killing Mexican police and public officials, and who are so expert at smuggling drugs, guns, and people across the U.S. border. The money also encourages corrupt officials to look the other way and pays for the sophisticated technology and weapons that the cartels use to such deadly effect.

By letting so much illegal cash literally flow through its fingers, the United States is making sure that the cartels have the resources they need to attack and defeat our border defenses. But, some say, the cartels are not terrorists and cutting off terrorist funds must be our main international objective. However, there is no way to distinguish between illegal money transfers to the cartels and similar transactions to terrorist organizations. Once the guards against money laundering are down, the money corridors and criminal money brokers are impartial. Leave open the door for one, and it is open for all.

Over the past decade, Arizona has occupied a front-row seat for the dramatic increase in smuggling of people, drugs, guns, and contraband across the southwest border. Frustrated by the lack of federal response, law enforcement in the Grand Canyon State attacked what they knew to be the most vulnerable point in the massive smuggling organizations—their access to cash. As one state, working virtually alone, Arizona could not stop the criminal monster. But we did learn some valuable lessons, discover some cartel vulnerabilities, and develop important investigative resources that, if aggressively deployed in federal hands, could prove decisive in the effort to protect the southwest border.

Wire Transfers

Wire transfer has been, and in some places may still be, the payment vehicle of choice for human smugglers. The reasons are obvious. Human smugglers have a one-time contact with their "cargo." Once the person being smuggled is released in the United States, it is likely that the smuggler will never see them again. Payment must be fast, close in time to the moment the cargo is safely deposited at a drop house, and as anonymous as possible. The cartel agent must be able to collect many individual payments at the same time without arousing official suspicion. Once the wired funds are received by the smuggler, or *coyote*, the smuggled person is released from the drop house or escorted on the rest of his or her journey.

Arizona: A Case Study in Enforcement

More than 10 years ago, under the expert leadership of Cameron (Kip) Holmes,[6] the Arizona Attorney General's Office started to go after smuggler money. At the time, and until a few years ago, hundreds of millions of cartel dollars were being wired illegally into Arizona. As the Arizona Attorney General from 2003 to 2011, I made targeting these practices a top priority.

Our investigators with the Arizona Financial Crimes Task Force looked for financial anomalies; mismatches that did not correspond to business reality. They immediately saw that Arizona was a huge net importer of wired funds. At the top-ten Arizona wired-funds locations, over $100 were coming in for every dollar wired out. Wire transfers into Arizona from other states, in amounts over $500, totaled more than $500 million per year. Since there was no apparent business reason for this imbalance, the investigators took a closer look.

Arizona investigators posing as drug dealers picked up wired payments at telegraph offices.[7] After receiving wires totaling almost $10,000—the threshold at which transactions in a single day under one name must be reported to the federal government—the agent would pull out identification for someone else and attempt to continue receiving wire transfers under the new name, so as to not trigger a report. Far from being astonished by this miraculous change in identity, desk clerks routinely accepted multiple IDs—as many as six at a time. In one case, the clerk examined the freshly produced ID and told the agent that it was not a very convincing forgery and that her cousin a few doors away would do a much better job. In other cases, the clerk would just give the customer a new ID from a stack kept behind the counter.

At the top-ten Arizona wired-funds locations, over $100 dollars were coming in for every dollar wired out.

Beginning in June 2003, Arizona started issuing Geographic Targeting Orders (GTOs)[8] by which the state required additional identification or required additional reporting from the wire-transfer agents for certain types of financial transactions in an identified geographical area.[9] Under a GTO, Arizona could, for example, require all high-volume money transmitter locations in the southern part of the state to obtain the fingerprints and signatures from all persons who received person-to-person wire transfers in amounts over $500. Based on analysis of the transaction data produced by the GTOs, as well as other evidence gathered through more traditional law-enforcement actions, the Task Force obtained 25 court-ordered warrants from the summer of 2001 through 2006 permitting seizure of wire transfers it had probable cause to believe were intended to pay for human smuggling or narcotics trafficking.

These "damming warrants" described the type of wire transfers the Task Force determined were most likely to be used for payment to human smugglers. At first, the descriptions were pretty simple. When we first used damming warrants, passage across the border cost around $2,000, and an identifiable set of smugglers picked up most of the money at a few high-volume locations on the Arizona side of the border. The damming warrant therefore described transactions of approximately $2,000, picked up by one of several specified *coyote* agents at specified locations. Later in the process the courts accepted a detailed description of the transaction—such as the amount of the wire, location of the pick-up, and number of similar transactions—but without naming the pickup operators, as sufficient grounds to issue a warrant.

Under the warrant, the money transmitter was ordered to electronically divert into a holding account wire transfers that matched the court-targeted criteria. When the *coyotes*' runners, called "pick-up operators" by law enforcement, tried to obtain the funds, they were told that the money was being held by the Attorney General. The money transmitter company provided a number to call if the frustrated recipient wished to pursue the money. That number was answered by specially trained, bilingual police officers who tried to determine if there was a legitimate purpose for the wire payment. Many of the callers were very frank, saying the money was to pay a *coyote* for illegally bringing someone into the country. Others made up elaborate stories, almost all of which fell apart when questioned.

The police officers handling the calls were instructed to let even semi-plausible explanations pass and, in those cases, to release the money. But if the caller admitted an illegal purpose for the funds, or the story was too improbable to believe, the money remained in official detention. All detained funds were taken before a court for a final seizure proceeding. At that hearing, the state had to demonstrate to the court's satisfaction why it believed that the funds were the proceeds of illegal acts. Anyone whose money was held could appear at that hearing to make their case that a particular seizure was improper. About $17 million was detained by the damming warrants and processed for court seizure. In almost six years of court actions and 25 warrants, no party successfully challenged a money seizure for forfeiture.

No damming warrant was effective for very long. As soon as the smugglers got word that money was being held at their usual pick-up points, they figured out the criteria being used and quickly

changed their payment procedures. If a certain dollar amount was being targeted, the next payments would be broken into smaller amounts. If certain locations were targeted, the pick-up operators went elsewhere. The money detained by each warrant reached its highest point shortly after initiation and within three days fell to almost zero as the smugglers adapted to law-enforcement's initiative.

As the damming warrants became more successful, the disproportionate volume of inbound wires to Arizona began to shrink. By 2006, the peak month of incoming transactions over $500 had fallen from a high a year earlier of over $36 million per month to less than $2 million per month. Especially steep declines in early 2005 and early 2006 came after damming warrant interdictions. At the same time, the receive-to-send ratio of transactions at the 10 highest volume wire-transfer locations fell from about 100 to one to about three to one.

There is no accounting for such a dramatic change apart from the conclusion that a substantial amount of illegal funds were being wired into Arizona. Unfortunately, the drying up of the Arizona wire-transfer business by no means meant that human smuggling through Arizona had stopped. The cartel agents simply changed their payment procedures and smuggling continued. Smugglers started "triangulating"—having their payments wired to a confederate just south of the border, who would pick up the money and phone the drop house operator in Arizona to confirm that payment had been received, allowing the release of the smuggled person. Although having tens of millions of dollars in cash flooding small Mexican border communities had undoubted risks, it kept the funds away from Arizona authorities.

...the drying up of the Arizona wire-transfer business by no means meant that human smuggling through Arizona had stopped. The cartel agents simply changed their payment procedures and smuggling continued.

Continuing to go after the money, Arizona law-enforcement officials obtained a damming warrant to seize wire transfers sent from specified "corridor states" to locations in northern Mexico, just south of the Arizona border. The seizure order was only in effect for three days, but took in $200,000 of suspect transactions before an Arizona judge shut it down. The Arizona Supreme Court eventually ruled that a state court did not have jurisdiction to issue a warrant for seizures outside the territorial limits of the state.

By the fall of 2009, the Arizona Attorney General's Office and Western Union, by far the largest volume transmitter of cash by wire in the world and into Mexico, began to seek a way to stop multiple ongoing legal actions between them. In February 2010, an agreement was reached. All lawsuits were dismissed and Western Union agreed to make sweeping changes to increase adherence to federal requirements and to more aggressive reporting of suspicious transactions by their agents. A fund was established to pay for the changes and a monitor appointed by the court to make sure the new procedures would go into effect. Perhaps most important, all the data involving unusually large wire transfers for the past five years and going forward would be made available to law enforcement—state, local, and federal.

Finally, and the capstone to this effort to increase border security, Western Union contributed $50 million to a fund which would make competitive grants to local and state law-enforcement efforts to attack money laundering and other border-related crimes. The Southwest Border Anti-Money Laundering Alliance was established with this money and the Executive Board selected Kip Holmes as its executive director. The wire-transfer data has been flowing to the Alliance since November 2010 and is being analyzed by their agents. Promising information is passed on to the appropriate law-enforcement agencies (state, federal, and the PGR in Mexico) for further investigation. Significant improvements in border security are being funded by the Alliance.

Beyond Arizona: Next Steps

Arizona has done about all a single state can on the anti-money laundering front. We identified a serious criminal problem, developed a successful investigation/prosecution technique, and changed smuggler behavior, at least in Arizona. But the next step must be national. Using the same leads Arizona derived from wire-transfer data, federal authorities are in an ideal position to coordinate among the states and with Mexican law enforcement to close down the criminal exploitation of the wire-transfer system. Nothing of the kind has happened, yet.

I testified several times before Congress urging increased action to fight money laundering, most recently in July of 2010. The U.S. Governmental Accountability Office (GAO) that same month recommended that the Department of Homeland Security should study the Arizona successes in tracking and seizing wire transfers:

> A second opportunity involves assessing the financial investigative techniques used by an Arizona Attorney General task force. The task force seized millions of dollars and disrupted alien smuggling operations by following cash transactions flowing through money transmitters that serve as the primary method of payment to those individuals responsible for smuggling aliens. By analyzing money transmitter transaction data, task force investigators identified suspected alien smugglers and those money transmitter businesses that were complicit in laundering alien smuggling proceeds.[10]

In spite of this strong GAO endorsement, there has been no adoption of the Arizona model. After almost two years, no convictions. No indictments. Just rumors of investigations and hints in SEC filings give hope that something may be changing. Considering the treasure trove of new data is available to facilitate these investigations and better track organized criminal activity and seize their money, the lack of action is very disappointing.

It is especially frustrating because the federal government has an opportunity to use the wire-transfer data in ways that state officials never could. They can “up stream” an investigation. When a suspect wire transfer came to our attention in Arizona, we could seize it and prevent the cartels from getting the money. We could not go up stream to check out the sender in another state to find out what other criminal enterprises that person or enterprise might be conducting. The federal government, however, can do exactly that and cast a wide net against criminal behavior.

Unfortunately, not only is there little positive movement by federal authorities in combating illegal wire transfers, but some money transmission agents appear to be actively evading federal rules.

These companies collectively processed billions of dollars in wire transfers last year to Mexico. The companies require very little identification from senders of wire transfers under $1,000, just a name. Other specific identifiers such as a birth date, driver's license, or address are not required. Furthermore, these companies do not seem to be particular about the qualifications of the subagents in Mexico who receive their wire transfers. Subagents may not even be known to the U.S. transmitter. They could be criminals with long records and the U.S. company would not know.

Hypothetically, under such lax oversight, a cartel operative could set up as a receiving subagent in Mexico and then wire funds from the United States illegally by "structuring"—that is, breaking large payments into multiple small transmissions. If the receiving agent is a money launderer, the names of real people would not be needed. Any list of fictitious names would do. The receiving agent could divide the amount of money that has to be moved out of the United States among a list of names in varying amounts. The names and corresponding amounts would then be sent to a confederate in the U.S. who would send the requested wire transfers to the receiving agent, all in small, apparently legitimate, and facially unrelated transactions. By structuring the transmission, and with the cooperation of the sending agent, the sender can avoid the $10,000 reporting requirement, even if the total amount sent is in the hundreds of thousands of dollars. The receiving agent reaggregates the funds and passes them to the cartel.

…not only is there little positive movement by federal authorities in combating illegal wire transfers, but some money transmission agents appear to be actively evading federal rules.

Such techniques can effectively disguise the movement of large amounts of cash. The hypothetical money laundering situation described above is further exacerbated because, although Western Union subagents are exclusive to that company, other wire-transfer companies allow their subagents to represent many different money transmitters. Thus, a single operator could be a subagent for several transmission companies, allowing a large transaction to be split not only among a large number of recipients, but among several different carriers, structuring the money transfer even more effectively. When a sender can coordinate with the receiving agent, effective control over international wire transfers virtually disappears. Eventually, one hopes that FinCEN, a division of the Department of the Treasury, would notice a large flow of funds to a mysterious location that had little or no economic reason to receive so much money. But FinCEN has been planning to monitor international wire-transfer data for about eight years and the system is still not operational.

Most international wire-transfer activity is made up of millions of legitimate transactions. The money launderers are tiny needles in a huge haystack. But without careful identification requirements on each transmitter and pick-up agent, and alert action by the transmission agents in spotting suspicious activity and filing Suspicious Activity Reports (SARs), human smugglers and other criminals are able to hide their cash transfers amid the forest of legitimate wires. Companies that operate outside the anti-money laundering rules present a huge challenge, not only to the effectiveness of the 2010 Western Union settlement with the border states, but to whether this country can enforce its anti-money laundering laws at all.

Money Laundering Technologies and Techniques

Currency Brokers

More and more, illicit cross-border money transactions are done by currency brokers—specialists who can divide a large sum into numerous small amounts that are virtually unnoticeable and can be aggregated at the receiving end. The currency broker has far more options for money laundering than the wire-transfer agent, including bank accounts set up in fictitious names and trade accounts of companies that either do export/import activity and can hide laundered transactions among many legitimate ones, or shell corporations set up to look as if they are involved in cross-border trade.

According to a GAO report, alien smugglers increasingly use "funnel accounts," deposit accounts opened to receive payments for smuggled goods and services. Federal officials in Arizona report large-scale money laundering through major U.S. banks that have a nationwide branch and automated teller machine (ATM) network. A deposit account opened by smugglers in Arizona would receive payments from the sponsors of smuggled aliens through an ATM or bank office from anywhere in the United States. The alien smuggler then quickly withdraws the money and closes or abandons the account, leaving virtually no trace.[11]

Trade-Based Money Laundering and the Black Market Peso Exchange

Cross-border businesses have always been tempted to disguise currency smuggling amid the flow of legitimate commerce. Booking an extra cost for the purchase of goods in Mexico can move dollars across the border and reduce taxable income. A more sophisticated version of the money-brokering process is found in the current evolution of the Black Market Peso Exchange (BMPE). Starting out as the market for illegal currency in Columbia, the original BMPE was taken over by Colombian drug cartels to repatriate drug proceeds in the 1990s. The Peso Exchange has become the default description of almost any procedure that uses product shipments to avoid currency restrictions and reporting, whether it touches an actual Exchange or not.

The pesos paid for U.S. goods (a tractor trailer truck, for example) sold in Mexico can take some surprising turns in the currency conversion process. Instead of converting pesos to dollars through a legitimate currency exchange with formal reports of the transaction, direct payment is sometimes made to the truck seller by third parties, unrelated to the purchaser—payments which are the dollar proceeds of illegal drug sales in the U.S. The pesos needed to purchase the product in Mexico are paid to the cartel's money broker (usually at a discount from the legal exchange rate) and the purchased truck crosses the border to complete the transaction.

Sometimes, such transactions take place without moving any goods at all. A warehouse north of the border issues an invoice to someone wishing to convert drug dollars to pesos. The invoice shows a "purchase" of a Mexican product (perfume, for example) and the dollars to be converted are paid to the writer of the invoice who then "purchases" product in Mexico and receives a receipt in pesos for the alleged "import" goods. The pesos are paid to the cartel's money broker by a third party who needs dollars in the U.S. and is looking for a good discount. No goods change hands, only cash

and paperwork. The business in the U.S. keeps some of the invoiced product on hand in case of inquiry. It looks like a lot of perfume has crossed the border. But in reality, only cash does.[12]

Stored Value Instruments or Prepaid Access Cards

One particularly mystifying failure of our nation's border defense is the inability or unwillingness to monitor and control the cross-border movement of "stored value" devices. These are innocent-looking plastic cards that can contain thousands if not millions of dollars and are not covered by any currency disclosure requirements at the border. They resemble credit cards, but have access not to a credit account at a financial institution, but to a specific amount of cash "stored" on the card in a microprocessor chip or in an account accessible through the card. Along with other digital devices, these cards are the currency of the future. Throughout the economy, more and more payments are being made with stored value cards. From a volume of only $6.2 million 10 years ago, the use of prepaid access cards exploded to over $800 billion in 2008, with projections as high as $1.3 trillion for the current year.[13] One large user of these cards is the United States government, which uses them for a wide variety of payments, including virtually all public assistance.

There are several types of stored value devices. The least sophisticated contain a fixed amount and are activated by a merchant. The funds on the card are drawn down as purchases are made until the card is empty. This type of card is not rechargeable. Commonly known as gift cards, they are available at every supermarket checkout counter. This version is not a problem (unless a smuggler is carrying hundreds of them). More problematic are the cards that can be refilled from a computer or ATM. These are, in effect, little bank accounts and the balances stored on them are not apparent without a scanner equipped with the appropriate software. These cards can carry a large balance that can be downloaded after crossing the border. The cards can be passed easily from hand to hand, making them essentially anonymous.

Stored value devices are not listed as monetary instruments or otherwise subject to declaration at the border, even though they could contain many times the $10,000 disclosure threshold.

Under U.S. law, no traveler may take over $10,000 in cash or cash equivalents, called "monetary instruments," into or out of the United States without declaring that money at the border. The definition of "monetary instruments" is evolving. It includes travelers' cheques, bearer bonds, some letters of credit, and other documents readily convertible to cash. Stored value devices are not listed as monetary instruments or otherwise subject to declaration at the border, even though they could contain many times the $10,000 disclosure threshold. This loophole, clearly identified by federal authorities over six years ago, provides smugglers with a massive opportunity to evade anti-money laundering security at the border. Since there is no obligation to disclose, border officials have no authority to even inquire how much value is stored on a stored value instrument, and no way to read any cards they happen to spot.

A third type of prepaid access device provides access to an account through its magnetic strip (or other electronic mechanism) and a password. These are readily transferable and can be used with participating financial institutions on both sides of the border. Presumably, it takes a higher degree

of identification to open the original account than is the case with a rechargeable card, making these instruments somewhat less desirable to smugglers. However, the low level of identification that has been required by some financial institutions does not pose an obstacle for money launderers. These cards have recently been renamed "prepaid access" devices by federal regulators to emphasize the fact that they usually do not actually store value on the device, but more often provide access to an account.

Attempts to Control Money Laundering Technologies

The huge hole that stored value devices pose to our anti-money laundering efforts cannot be a surprise. In 2006, the National Drug Intelligence Center (NDIC) in its Assessment of stored value cards warned that prepaid access devices constituted a significant loophole in our border defenses.

Key judgments from the NDIC Assessment include:

- Prepaid stored value cards—a product experiencing explosive growth—provide an ideal money laundering instrument to anonymously move monies associated with all types of illicit activity, without fear of documentation, identification, law enforcement suspicion, or seizure. Therefore, it is very likely that drug traffickers and criminals alike are exploiting and will increasingly exploit the convenience and anonymity of prepaid stored value cards to launder and move funds associated with their illicit enterprises.

- Prepaid stored value cards cannot be seized for Report of International Transportation of Currency or Monetary Instrument (CMIR) violations; are loosely regulated; function as remittance cards; frequently provide cardholder anonymity when individuals are obtaining cards or adding value to cards; often have liberal daily limits on total card value, reloading, withdrawal, and spending of funds; and feature fees that are generally consistent with or lower than the normal "cost" of laundering money.
- Prepaid stored value cards are, in many ways, superior to established methods of money laundering and money movement—specifically, the use of money transmitters and bulk cash smuggling—and may replace these methods under certain conditions.
- Drug traffickers and other criminals will most likely use prepaid stored value cards in lieu of electronic money transfers because the fund-transfer processes are similar and use of the cards provides additional benefits.
- Prepaid stored value cards are an advantageous alternative to bulk cash smuggling via package delivery services or couriers on board commercial conveyances (airplanes, buses, trains)—methods that carry a significant risk of detection by law enforcement.
- It is much less likely that prepaid stored value cards will replace traditional bulk cash smuggling by private or commercial vehicle—methods that currently appear to be adequate to fulfill traffickers' needs.
- U.S. regulatory action alone will not be sufficient to suppress the money laundering threat posed by prepaid cards, since cards issued by non-U.S. banks or other institutions

> can be used domestically to transfer funds, make purchases, or access cash at automated teller machines (ATMs).[14]

Among other conclusions, the Assessment recommended specific regulatory changes:

> The U.S. Department of the Treasury has acknowledged the need to modify and clarify existing regulations related to the prepaid stored value card industry; in fact, FinCEN recently announced that it will issue new regulations designed to clarify the roles and obligations of issuers of prepaid cards. Although it is not yet clear what actions will be taken, **there is an obvious need** {emphasis added} to implement several changes to existing regulations. In order to enable seizure of prepaid stored value cards with a monetary value of more than $10,000, stored value should be included in the definition of monetary instruments for CMIR purposes. Because it is often difficult to distinguish between traditional debit cards and network-branded prepaid stored value cards, a requirement designed to distinguish the appearance of open and semi-open system prepaid stored value cards would enable law enforcement agencies to better identify suspicious cards. Due diligence procedures required of financial institutions under the USA PATRIOT Act—such as identity verification and comparison of customers' identities against names of known terrorists—should be applied to prepaid stored value cards because open and semi-open system prepaid stored value cards are used in a manner that approximates a traditional checking account. Additionally, the imposition of compliance programs such as those that apply to money transmitters—including customer identification, recordkeeping, and SAR-MSB reporting requirements—would empower law enforcement investigations by allowing agencies to access information such as cardholders' identities, to track transactions, and to identify patterns of suspicious activity.[15]

In spite of the above dramatic conclusions, FinCEN did not act in 2006. As part of credit card reform, Congress ordered Treasury to write regulations for prepaid access devices by February 2009. Nothing happened. When regulations were finally drafted in 2010, they failed to cover the international movement of the cards. The final rule took effect on September 27, 2011. It changed the official name of the cards to "prepaid access devices" and made some long-overdue changes in how the cards are reported by the issuer and monitored, but the rule did not close the international money laundering loophole. Only now is the rule change for international transportation of such devices being officially proposed.

Retired U.S. Representative Gabrielle Giffords introduced legislation to close the prepaid access loophole in May 2010.[16] That proposed legislation defined prepaid access devices to include developing technologies for money transfers such as cell phones; established a disclosure requirement for prepaid access devices transported out of the country when they, or they in combination with cash or monetary instruments, total more than $10,000; required registration of prepaid access programs; mandated that law-enforcement officers have the software needed to determine the value accessible with devices they encounter; subjected non-conforming prepaid access devices to forfeiture; and established criminal and civil penalties for violations. Although the bill died at the end of the 111th Congress, some of its provisions were included in the September 2011 final rule from Treasury. The broader objectives of the bill, however, including the need to control international movement of prepaid access devices and provide meaningful penalties for

abuse, remain undone. Senators Grassley, Levin, and Feinstein have introduced a less comprehensive effort to control the international transport of prepaid access devices in the 112th Congress.[17] But no action has been taken on that legislation, either.

The prepaid access industry has fought any attempt to require disclosure of card balances, to allow official examination of the cards with scanners, or even to identify the cards visually in a way that makes clear that they are different from debit and credit cards as was recommended by the Department of Justice Assessment. Since credit-card companies such as Visa and MasterCard are the primary issuers of prepaid access cards, there is no way to tell by observation what type of cards a cartel courier is carrying. I have spoken to Treasury officials on this subject and testified before Congress to urge the elimination of the stored value or prepaid access card loophole. In 2009, the 18th annual Southwest Border Money Laundering Conference in Phoenix was dedicated solely to the threat posed by prepaid access devices. Treasury agents attended this and other anti-money laundering conferences where the urgent need to fix this problem has been discussed.

The federal government has been stubbornly unwilling to patch the hole that prepaid access devices create in our anti-money laundering regulations.

The federal government has been stubbornly unwilling to patch the hole that prepaid access devices create in our anti-money laundering regulations. Federal inaction is very hard to understand. True, the ideal fix is statutory and not regulatory, making it more complicated and time consuming. Statutes would have to be passed to impose the obligation on travelers crossing the border to declare any prepaid access devices in their possession or face criminal consequences. Border agents must be supplied with card readers able to verify the amount contained on the cards or in accounts accessible through the cards. But, surprisingly, the agency in charge of preventing money laundering has not pushed legislation and has conspicuously dragged its feet on regulating the international transportation of these cards, even in the face of urgent law-enforcement demands and Congressional mandate.

What Next?

Some long overdue efforts to tighten up the criminal laws against money laundering began in 2011. The Administration has put forward an anti-money laundering and forfeiture legislative package which it calls the Proceeds of Crime Act (POCA). In hearings on February 8, 2012, before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, officials from the Departments of Justice and Treasury testified in support of the POCA provisions, saying they are needed to combat transnational organized crime and international money laundering. Their analysis indicating that money laundering is a major threat to our financial system was thorough, but their suggestions for remedy were not.

The Administration proposed the following changes to the criminal statutes under POCA:

- harmonizing the definition of money transmitting businesses (including more *casas de cambio* and check cashers).
- extending wiretap authority to schemes reliant on electronic communications (wiretaps are often the most productive information sources in money laundering investigations).
- confronting the problem of commingled funds (reversing the tendency of courts to assume that in a commingled account the dirty money comes out last).
- promoting corporate transparency (requiring proof of beneficial ownership when opening bank accounts).
- extraterritorial application of the RICO and VICAR statutes (increasing the predicate offenses overseas that would prevent the proceeds being invested in the U.S.).

While these are worthwhile improvements, at best they are on the margins, tightening up definitions and expanding the list of predicate offenses. Plus, most of the suggested changes involve cutting down on dirty money coming into the United States, not keeping it from flowing out. If all the POCA reforms were enacted tomorrow, big holes in the anti-money laundering fabric would remain. Although representatives of Justice and Treasury both testified at a recent Congressional hearing that prepaid access cards were a significant smuggling problem, neither suggested doing anything about it. Especially surprising is that the Department of Justice, which so clearly identified the threat in 2006, has not included reform of prepaid access cards in POCA.

Generally speaking, the failures of the anti-money laundering effort are not because of inadequate statutes, but a failure of enforcement.

Prosecutors in federal court today operate under tight restrictions on when they can seize the cash they believe to be part of a criminal scheme. Under Arizona law, it is far easier to hold suspected funds pending further examination of their source.[18] Giving this authority to federal agents would put important teeth in their anti-money laundering efforts. However, POCA contains no recommendations concerning the lack of effective authority to detain and ultimately seize funds when there is a reasonable suspicion that they are the proceeds of a crime.

Another area in which state law could be a model for federal law relates to the consequences for giving false information in connection with a financial transaction. In Arizona, if you give a false name when you open an account at a financial institution, the money is subject to forfeiture.[19] If you give a false social security number when you use a money transmitter, the money is forfeitable.[20] In both cases, the depositor and the sender have committed money laundering under state law. If someone tries to bribe a money transmitter or other employee to ignore a reporting requirement, he or she has committed money laundering and the money is forfeitable.[21] If a money transmitter or an employee accepts false personal identifying information from any person or incorporates false personal identifying information into any report, it is a money laundering violation and the money is forfeitable.[22] The same clear forfeiture authority is not contained in

federal law. These statutory changes would be very valuable to a federal prosecutor battling money laundering.

Time to Clamp Down on Money Laundering in All Its Forms

The *Manchester Guardian* reported in April 2011 how hundreds of billions of dollars in "wire transfers, traveler's cheques and cash shipments" were moved illegally through Wachovia Bank and across the U.S.-Mexico border in 2005 and years preceding. These funds undoubtedly paid for murder and mayhem in Mexico, yet an investigation into Wachovia Bank's procedures resulted in a fine of less than 10 percent of the money laundered and no criminal prosecutions.[23] As one commentator rightfully observed, the best way to end these insidious practices is the "rattling of hand cuffs in some bank boardrooms." Yet one of the consistent factors in money laundering prosecutions is the lack of penal consequences. Major financial institutions continue to be less than diligent in enforcing anti-money laundering regulations and some respond to law-enforcement subpoenas in ways that undercut the investigations by closing out the subject account and sending the deposited funds back to the depositor.

Until government agencies, especially Treasury, get more serious about cutting off the illegal international flow of funds, we can never say we have a "secure" border.

Generally speaking, the failures of the anti-money laundering effort are not because of inadequate statutes, but a failure of enforcement.[24] Again and again, huge amounts of funds flowing illegally out of this country could be stopped, if financial institutions and government agencies focused on the problem. But the prevailing attitude is permissive of violations and reluctant to sanction violators. Of course, there will always be sophisticated nuances and complex trade relationships which can be exploited to move money illegally, but the billions of dollars going to the drug cartels are not flowing through nuances. They are going through the front door of the financial system, through bank accounts, large trade transactions, prepaid access devices, and wire transmissions. As opponents, the cartels have not made the problem any easier, proving to be extraordinarily innovative and opportunistic. They have mastered the international financial system and exploited it to their great advantage.

The U.S. government must enforce existing anti-money laundering provisions and quickly close the identified loopholes to stop (or at least slow down) the cash flowing to the cartels. Until government agencies, especially Treasury, get more serious about cutting off the illegal international flow of funds, we can never say we have a "secure" border. Stopping less than one percent of the opponent's cash smuggling transactions should never be considered a good job. Especially when the money pouring across the border is wreaking such havoc in Mexico and making a mockery of the U.S. border defenses.

With the Calderon Administration in Mexico in its last months in office, the best chance to strike back against the cartels is rapidly disappearing. The United States should be making every effort to strengthen Mexico's hand right now. The most effective means available is to stop the cash that

makes the cartels so strong. We can fix the "broken" border and stop the bloodshed in Mexico—by just following the money.

Endnotes

[1] Eric Tucker, "Cash Smuggling from Mexico Presents US With Challenge," Huffington Post, February 12, 2012.
[2] National Drug Intelligence Center, *National Drug Threat Assessment 2009*, December 2008.
[3] United Nations Office on Drugs and Crime, *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, October 2011, p. 21.
[4] Testimony of Jennifer Shasky Calvery, Chief, Asset Forfeiture and Money Laundering Section, Criminal Division, Department of Justice, before the Subcommittee on Crime, Terrorism and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, February 8, 2012.
[5] United Nations Office on Drugs and Crime, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*, 2010, p. 66.
[6] Mr. Holmes, a Harvard-educated former Portland cop, has focused his career in law enforcement on detection and prosecution of money laundering. He drafted the Arizona money laundering laws, among the toughest in the nation, and led the Financial Crimes Task Force at the Arizona Attorney General's Office. Today, Kip is the Director of the Southwest Border Anti-Money Laundering Alliance.
[7] At the beginning of these investigations, agents did not pose as human smugglers, or *coyotes*, because being a *coyote* was not yet a state crime.
[8] The 1991 money transmitter regulation statutes, 6-1201 through 6-1242, and—in particular—6-1241(J), relating to GTOs, and the 2002 amendments to it adding (K).
[9] The GTO provisions are 6-1241(J) and (K).
[10] U.S. Government Accountability Office, *Alien Smuggling: DHS Could Better Address Alien Smuggling along the Southwest Border by Leveraging Investigative Resources and Measuring Program Performance*, GAO-10-919T, July 22, 2010, p. 6.
[11] U.S. Government Accountability Office, *Alien Smuggling: DHS Needs to Better Leverage Investigative Resources and Measure Program Performance along the Southwest Border*, GAO-10-328, May 2012 p. 35.
[12] See, for example, Juan Aguilar, "In Laredo, Was A Criminal Enterprise Bathed in Sweet Perfume?" *Texas Tribune*, November 12, 2011.
[13] This information is from the materials prepared for the 2009 Southwest Border Money Laundering Conference.
[14] U.S. Department of Justice, National Drug Intelligence Center, *Assessment: Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods*, Product No. 2006 R0803-001, October 31, 2006, p. 1.
[15] Ibid., p. 7.
[16] H.R. 5127, 111th Congress, 2d Session.
[17] SB1731.
[18] This is because ARS 13-4304 defining property subject to forfeiture applies to property subject to forfeiture under in personam causes of action such as ARS 13-2314 (D) and 13-4312 and property subject to forfeiture as substitute assets under ARS 13-4313(A) and/or ARS 13-2314(D)(6)(d) and (E), or under a special treble substitute assets provision relating to money laundering under ARS 13-2317(D), and because all property subject to forfeiture is subject to seizure for forfeiture under ARS 13-4305.
[19] ARS 13-2317(A)(6-8).
[20] ARS 13-2317(A)(7)..
[21] ARS 13-2317(C)(1).
[22] ARS 13-2317(B)(4),(5) & (9).
[23] Ed Vulliamy, "How a big US bank laundered billions from Mexico's murderous drug gangs," *Manchester Guardian*, April 3, 2011.
[24] Except for the failure to include prepaid access cards among the funds which must be disclosed at the border and the difficulty seizing cash assets in federal actions.