

Prepaid Cards an Emerging Threat

Recent ICE investigations have uncovered an emerging trend in the use of prepaid or stored value cards to smuggle illicit proceeds out of the U.S.

Where criminal organizations previously employing bulk cash smuggling or the use of money launderers to wire proceeds out of the U.S. they are now often turning to prepaid cards.

Prepaid cards are issued to customers in two categories, *closed system cards* and *open system cards*. The use of both types involves numerous money laundering vulnerabilities.

Closed System Cards

- Gift cards, phone cards, etc.
- Usually sold in preset denominations.
- Cannot have additional value added.
- Cannot be used at ATMs.
- Limits on the use of closed system cards make them a lesser, but still significant, money laundering threat than open system cards.

Open System Cards

- Most significant money laundering threat.
- Branded by American Express, MasterCard, or Visa operate like traditional credit or debit cards.
- Any prepaid card with ATM access can be a remittance card.
- An estimated \$30 billion in remittance payments go to Latin America from the U.S. each year, with \$10 billion to Mexico alone.
- Remittance cards allow cardholders to use a bank payment



"Prepaid" or "stored value" cards are becoming a preferred method by criminal organizations to move illicit funds out of the country.

network, through ATMs, without requiring a bank account.


- Remittance cards facilitate the cross border movement of funds without a declaration requirement.

Money Laundering Vulnerabilities

- Funds can be loaded anywhere in the world.
- Often no maximum load limit.
- Used at ATMs or as credit cards.
- No bank account needed.
- Can be activated online.
- The Bank Secrecy Act (BSA) Know Your Customer (KYC) policy and other BSA regulations often don't apply.
- Perfect platform for bulk cash smuggling operations.

Recent Scheme

A scheme recently identified through an ICE/IRS investigation involved a criminal organization providing stolen credit card numbers to a co-conspirator operating in Mexico. The co-conspirator used commercially available magnetic encoding devices to encode dummy credit cards.

The co-conspirator was paid by criminal organizations with gift cards issued by U.S. retailers. The gift cards were then used to purchase mobile phone cards, which were smuggled into Mexico and sold at a profit. The investigation resulted in the arrest, indictment and conviction of one foreign national, the seizure of one vehicle and a court ordered \$50,000 fine. 



The Official Newsletter of Cornerstone

U.S. Immigration and Customs Enforcement (ICE) is the largest investigative arm of the Department of Homeland Security (DHS).

ICE's mission is to secure the homeland by enforcing immigration and customs laws and by protecting U.S. commercial aviation and federal facilities. Cornerstone, ICE's comprehensive enforcement initiative focusing on financial and trade fraud investigations, is a key component of that mission.

In addition to financial and money laundering investigations, Cornerstone targets commercial fraud, smuggling and trafficking, export and trade violations and intellectual property crimes. ICE's global reach allows the agency to investigate these crimes around the world.

The Secretary of Homeland Security has determined that the publication of this newsletter is necessary in the transaction of business required by law of U.S. Immigration and Customs Enforcement (ICE).



Safeguarding America through
Financial and Trade Investigations

Volume III: No. 2 • December 2006

Inside This Issue

Demise of the Cali Cartel 2

The E-Cornerstone of Economic Security 3

Prepaid Cards an Emerging Threat 4

Cornerstone is U.S. Immigration and Customs Enforcement's (ICE) comprehensive investigative initiative for fighting financial crime, trade fraud and intellectual property crime.

The Cornerstone Report is a quarterly bulletin highlighting key issues related to ICE financial and trade investigations.



Toll-Free Tip Line:
1-866-DHS-2-ICE

www.ice.gov/cornerstone

ICE Financial Investigation Initiative Combats Illegal Worker Employment



Cash and evidence seized during an investigation into the illegal activities of Pronto Cash, a Florida business, that used mobile check-cashing vans pictured above, indicted for operating an unlicensed money service.

In July 2006, ICE launched Operation Paycheck, a national initiative designed to combat criminal schemes involving the exploitation of the financial industry by businesses to pay the wages of illegal alien workers.

ICE investigators have uncovered schemes throughout the U.S. involving the commission of financial crimes, such as money laundering, structuring funds into and out of financial institutions, and the operation of unlicensed money service businesses (MSBs) to disguise the payment of illegal alien workers.

To combat this criminal activity, ICE investigators are leveraging their combined investigative expertise in financial crimes and worksite enforcement to identify, disrupt and eliminate organizations seeking to exploit our financial industry to facilitate the employment of illegal aliens.

The Scheme

In most cases, many involving the construction industry in the Southeastern U.S., the employer of illegal aliens establishes shell companies that appear to operate as subcontractors of the actual employer.

The employer is then able to pay the shell company for their services, often in the form of one large check or numerous checks. The shell company (the subcontractor) then cashes the checks—frequently through a culpable MSB—and pays the illegal alien workforce in cash. Naturally, the person or persons posing as the subcontractor charge a fee for this service, as does the culpable MSB.

The employer has now successfully laundered the payroll of his illegal alien workforce.

This scheme may also involve other state and federal violations. For example, the use of a shell company and the payment of the illegal alien workers in cash allows employers to avoid withholding state, federal and Social Security taxes from employees' paychecks, in violation of state and federal laws.

Successes

Under Operation Paycheck, approximately 48 criminal investigations have been initiated. These investigations have resulted in the seizure of over \$3 million and the arrest or identification of numerous suspects.

Continued on page 2



Demise of the Cali Cartel

Page 2 of 4

Volume III: No. 2
December 2006

A long-running investigation of the Cali drug smuggling cartel culminated in September 2006, when cartel leaders Miguel and Gilberto Rodriguez-Orejuela pled guilty in the Southern District of Florida to conspiracy to import over 200,000 kilograms of cocaine, and a forfeiture count for \$2.1 billion.

The 15-year investigation under ICE's leadership is a testament to the agents' and prosecutors' tenacity, innovation and good old-fashioned detective work.



Gilberto Rodriguez-Orejuela shown during his arrest and subsequent extradition to the U.S. where he is currently serving a 30-year prison sentence.

The investigation began in 1991 when a drug-sniffing dog at the Miami seaport alerted to a massive shipment of cocaine concealed in concrete posts. Continual surveillance over three months, and several controlled deliveries of drugs in Miami and Texas, resulted in agents executing seven search warrants, seizing 12,250 kilograms of cocaine, and several arrests.

In June 1995, a federal grand jury in Miami issued the first RICO (racketeering) indictment against the Cali cartel, charging 59 defendants, including the cartel's four kingpins (Miguel Rodriguez-Orejuela, Gilberto Rodriguez-Orejuela, Jose Santacruz-Londono and Helmer Herrera-Buitrago), 10 defense attorneys and several hit men.

The indictment charged the Cali cartel with importing 200,000 kilograms of cocaine and laundering \$2 billion from 1983 through 1995. Gilberto and Miguel Rodriguez-

Orejuela were apprehended and jailed in Colombia in 1995. Santacruz and Herrera were later killed.

Although the defendants were imprisoned by Colombia in 1995, they continued to run the cartel from prison by working through Miguel's son, William Rodriguez-Abadia, and others.

In September 2003, ICE agents obtained an indictment against 11 cartel defendants, including the Rodriguez-Orejuela brothers, for their recent drug and money laundering activity. A superseding indictment was obtained in January 2004, with more than \$2 billion in assets being sought.

In November 2004, extradition requests were approved, and several months later the brothers were extradited to the United States, where they were sentenced to 30-year prison sentences, marking the end of the infamous Cali cartel. ❏

Continued from page 1

One of the most successful Operation Paycheck investigations was of Pronto Cash, an MSB in Orlando, Fla. In this investigation ICE uncovered a conspiracy involving construction companies and an MSB involved in the payment of illegal alien workers. In the conspiracy, shell companies posing as construction subcontractors falsely claimed to have workers' compensation insurance on their illegal workers in order to qualify for contracts.

These shell companies cashed checks for the actual employer of the illegal aliens, typically in excess of \$10,000, at Pronto Cash, an MSB

that used mobile check-cashing vans. Pronto Cash promoted this activity by not filing currency transaction reports (CTR) or by filing CTRs with false information.

The construction companies then paid the cash out to their illegal workers. The scheme also permitted the illegal workers to receive their wages without being required to present identification, which could have exposed their illegal status.

In October 2006, a federal grand jury returned an indictment charging the president of Pronto Cash and several employees with operating an unlicensed MSB, money laundering, avoiding or filing false



Red Flag Indicators

- The withdrawal of large sums of cash from business bank accounts for the payment of wages.
- Business bank accounts—alleged subcontractors—that make frequent high-dollar deposits by check and immediate corresponding cash withdrawals.
- Checks written from one business to another for payroll expenses, where checks are cashed rather than deposited.
- Checks written from one business to another for large sums that are then cashed at an MSB.
- Multiple checks issued to the same payee, sequentially numbered, and under the \$10,000 reporting requirement.

CTRs, mail fraud, wire fraud and hiring illegal aliens.

ICE agents seized \$2.8 million, as well as computers, records and other items of evidentiary value. ❏



The Center

The ICE Cyber Crimes Center (C3) in Fairfax, Va., is recognized nationally and internationally as a leader in the investigation of international criminal activities conducted on or facilitated by the Internet.

Created in 1997, the C3 brings the full range of ICE computer and forensic assets together to combat such Internet-related crimes as possession, manufacture and distribution of child pornography; international money laundering; illegal arms trafficking; and intellectual property rights violations.

The Mission

Electronic currencies, or *e-currencies*, can be fundamentally defined as units of value linked to the value of some other item that can represent cash, gold and other precious metals, merchandise or services facilitated via the Internet. The use of e-currency systems by criminals has been well documented by ICE and other law enforcement agencies.

To combat the laundering of e-currencies, ICE C3 developed the E-Cornerstone initiative, an intensified investigative focus on e-currency and Internet money laundering that parallels and augments existing ICE Cornerstone efforts.

ICE C3 has taken a three-pronged approach to the E-Cornerstone initiative—training, outreach and interagency cooperation.



Specially-trained agents at the ICE Cyber Crimes Center investigate Internet-based financial crimes.

Training: To foster the efforts to create a robust and aggressive investigative program, the C3 has provided training to more than 150 ICE field agents in 2006 to specifically focus money laundering investigations on the Internet financial sectors.

Outreach: In an effort to establish reliable points of contact and to develop investigative leads, ICE C3 directs the field in conducting industry outreach with financial institutions that facilitate their businesses on the Internet.

Interagency Cooperation: ICE C3 and the U.S. Secret Service are leading the Global E-Currency Task Force (GETF), which works with other domestic and foreign law enforcement and private sector

entities involved in e-currency to outline strategies to combat online money laundering.

The Goal

Apprehending and bringing violators to justice is one of the best ways to deter and prevent abuse in any system. Investigating and arresting violators who are using the Internet to launder and transfer money is therefore a primary goal of the E-Cornerstone initiative. 