The Cornerstone Report

Safeguarding America through Financial Investigations

Volume VI: No. 3 • Summer 2009

Inside This Issue



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

*The Cornerstone Report* is a quarterly bulletin highlighting key issues related to ICE financial, narcotics and public safety investigations.

U.S. Immigration and Customs Enforcement

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

www.ice.gov/cornerstone

# A Study in Money Laundering

## The Oropeza Family and Drug Smuggling at the Southwest Border

A joint investigation by U.S. Immigration and Customs Enforcement (ICE) and the Drug Enforcement Administration (DEA) into drug trafficking at the Southwest border revealed a multi-million dollar money laundering organization, utilizing multiple companies, and numerous bank accounts, to launder narcotic proceeds. This case study demonstrates methodologies used for laundering criminal proceeds.

In 2004, ICE agents in Brownsville, Texas, received information that Oscar Oropeza, along with his wife Tina, daughter Paulina and son Juan, were using various businesses they owned to launder proceeds derived from narcotic sales. The Oropeza family owned substantial assets in both Brownsville and Harlingen, Texas, including a car wash, landscaping business, trucking company, a large house, and numerous vehicles valued between $60,000–$120,000 each.

One of the first developments linking the Oropeza family to narcotics occurred in April 2004. Juan Hernandez and other defendants were arrested by local police in Harlingen, Texas, after they were linked to a narcotic smuggling operation utilizing truck lines to ship marijuana out of the Rio Grande Valley, to Florida. As a result of this arrest, Hernandez received more than three years in a state penitentiary. DEA agents in West Palm Beach, Florida, learned of Hernandez's arrest and asked ICE for additional information about his drug operation. This information linked Milton Oquendo to the narcotic smuggling in Florida. DEA subsequently arrested and charged him in Florida for his role in the organization. Hernandez and Oquendo were each sentenced to ten years as a result of this indictment. The money laundering activities being conducted by the Oropeza family were directly linked to Hernandez and Oquendo.

U.S. currency discovered in safe deposit box and seized by ICE.

In July 2006, investigators caught a break in the case when Tina Oropeza was stopped and questioned by Harlingen police officers while riding on a north-bound bus headed out of the city. Officer's discovered she was carrying approximately $90,000 in cash, which they seized.

Subsequent financial records checks showed that the Oropeza family had more than 20 accounts with several banks. Personal bank accounts connected to the money laundering activity were held by all four Oropeza's. Account statements from these personal accounts reflected cash deposits

continued

# Oropeza Family et al., Investigation, continued

well in excess of $1 million in just over two years. Of these cash deposits, the vast majority consisted of cash deposits of less than $10,000, and often involved multiple cash deposits on the same date.

Statements for the multiple business accounts reflected cash deposits well in excess of $2 million in just over two years. The business accounts had over $3.6 million in deposits for 2006 alone. A large portion of the cash deposits also consisted of amounts less than $10,000, and often involved multiple cash deposits on the same date. These numerous cash deposits were conducted by all four Oropeza family members.

Prior to opening an investigation, ICE learned that Oscar Oropeza paid for a building connected to his landscaping business with two cash payments. The first payment was $221,000, and the second was for approximately $120,000, both of which consisted of primarily $20 bills.

The case saw another critical development on May 31, 2007, when Oscar and Tina Oropeza were stopped for traffic violations by local police in Mobile, Alabama. Oscar Oropeza gave verbal consent to search their van, which revealed a hidden compartment in the floor area. The officers discovered four aluminum containers concealed within the compartment containing 84 packages wrapped in plastic wrap and duct tape. The packages contained a white powdery substance that field tested positive for cocaine; Oscar and Tina Oropeza were arrested on state charges for transporting cocaine.

Seized luxury jewelry discovered during execution of search warrants.

In May and June 2007, ICE agents served search warrants on seven properties owned by the Oropeza family in Brownsville, Texas. The search warrants resulted in the seizure of several vehicles, luxury jewelry items, and currency. ICE agents also served seizure warrants on 13 bank accounts and three safety deposit boxes connected to the Oropeza family, resulting in the seizure of more than $310,000.

The amount of currency, funds, property, and vehicles seized by ICE agents in Brownsville totaled more than $2.1 million. Five real properties valued in excess of $1 million were also forfeited.

In March 2008, Tina Oropeza pled guilty to federal charges related to narcotics smuggling and to money laundering conspiracy. Paulina Oropeza pled guilty to federal charges because of her knowledge of the money laundering activities. In November 2009, Tina Oropeza was sentenced to 10 months prison, five years probation, and a $25,000 fine. Paulina Oropeza was sentenced to five months in prison, five years probation, and a $5,000 fine.

Oscar Oropeza was sentenced to 180 months in the federal penitentiary for conspiracy to possess more that 1,000 kilograms of marijuana, and 180 months for conspiracy to posses more that five kilograms of cocaine. Oropeza was also sentenced to 180 months for conspiracy to possess with intent to distribute approximately ninety kilograms of cocaine. All of the sentences are to run concurrently for a total of 180 months. Oropeza was also ordered to serve five years of supervised release and to be deported to Mexico.

Vehicles seized by ICE that were purchased with illicit proceeds from narcotics smuggling.

## Red Flag Indicators

- Various reported occupations (attorney, owner of Green Wealth Group, financial analyst, etc.) by the same individual on BSA filings.
- The acquisition or purchase of high-value ticket items (real estate) with cash.
- Large number of business and personal accounts at different financial institutions.
- Numerous structured cash deposits into both personal and business bank accounts.
- Deposits made in different bank branches on the same day, and deposited into the same account.

The Cornerstone Report
Page 3 of 4
Volume VI: No. 3
Summer 2009

# Financial Fraud and Cross-Border Crimes

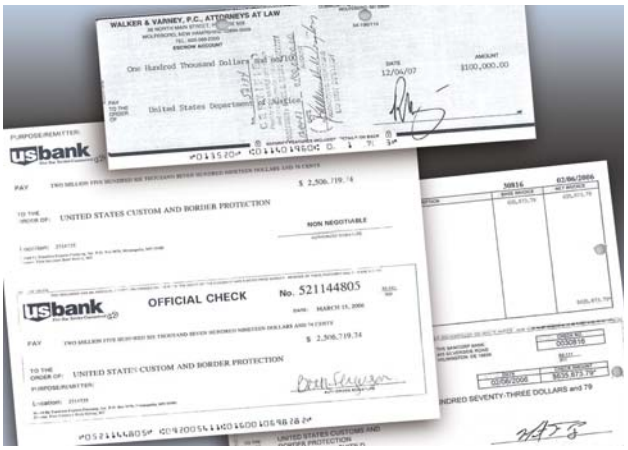
## Automated Clearing House Transactions

In 2006, the ICE Special Agent in Charge Office in Buffalo, N.Y., initiated an investigation into Integrated Check Technologies Inc. (ICT), a payment processor linked to a previous financial fraud investigation involving telemarketing activities. The investigation revealed ICT had knowledge that the telemarketers for whom they provided payment processing services had been committing fraud and were involved in a complex money laundering scheme exploiting the U.S. financial system through telemarketing.

ICE learned the state of Ohio's Attorney General's Office had an on-going civil investigation of ICT for processing payments for fraudulent telemarketing companies, and other states were pursuing or had pursued action against the company. A review of 57 telemarketing companies that ICT processed payments for revealed that each had a high return rate for unauthorized debit transactions, and the majority of those companies had complaints filed against them for fraud.

The international telemarketing fraud ring included Thomas J. Cimicato from Columbus, Ohio. Cimicato was the president, secretary, treasurer, director and primary shareholder of Check Free Recovery, Inc. d/b/a ICT. This financial fraud scheme involved the use of U.S. bank accounts to launder millions of dollars in fraudulently obtained wire transfers and was designed to extract money from victims' bank accounts on false pretenses or without authorization.

Individuals located in Canada and the United States, opened U.S. bank accounts in order to debit unsuspecting U.S. bank account holders' checking accounts by either Automated Clearing House (ACH) transactions or by depositing fraudulent draft checks through demand drafts. ICT, in business since 1998, began processing payments for telemarketing companies in March 2005. A review of the bank records indicated that the deposits by ICT substantially increased after ICT began processing payments for telemarketing companies.




An ICE investigation into questionable practices at a payment processing company uncovered a multimillion dollar telemarketing scheme.

Between March 2005, and January 2006, ICT deposits totaled more than $54.3 million. The bank where the deposits were made contacted a number of the account holders who were listed on the draft checks and inquired whether the debits on the draft checks were authorized. All the account holders who were contacted informed bank representatives that they did not authorize the withdrawals and the majority of the account holders who were contacted were elderly, living on limited incomes. In addition, some of the account holders were debited more than once, via draft checks, without their authorization by ICT and by other payment processors. Through a variety of fees for services rendered, ICT retained approximately $19.9 million of the $54.3 million total.

Using victims' bank account information, ICT printed (or caused to be printed) demand drafts, drawn from victims' accounts. ICT deposited the demand drafts into their bank account, causing debits to victims' bank accounts, and corresponding credits to ICT's bank account. Based upon a review of multiple telemarketing companies that ICT processed transactions for, ICE learned that more than half of the transactions processed were reversed or returned due to various reasons, including insufficient funds, account closed, stopped payments and unauthorized/fraudulent transactions. ICT willfully ignored countless complaints lodged against ICT and/or its clients by victims of telemarketing fraud.

ICT generated fees from this type of activity by generally charging a business the following recurring fees: a monthly minimum charge per account, a monthly administrative fee, a debit item origination fee, a credit item origination fee, a return fee for all items that did not clear, charge back fees, continued

# Financial Fraud and Cross-Border Crimes, continued

an item upfront decline fee, a reversal file created fee, a reversal file item origination fee, wire fees, and other fees, including a discount rate based on underwriting criteria and a risk management fee for settlement reserve.

The fraudulent telemarketing schemes, included unsolicited telephone calls, commonly known as "cold calls", made by foreign and domestic telemarketers to vulnerable consumers residing throughout the United States. During the cold calls, victims were induced, through misrepresentations and false promises of goods and services of value, to provide the telemarketer with personal bank account information. The telemarketer then transmitted the personal bank account information, using the United States mail and/or wires, to ICT.

Fraudulent telemarketers and their accomplices often trade in lists of prospective victims, including repeat victims who are likely to become a victim of another fraudulent scheme. These telemarketers also have been known to use these lists in order to debit victims' financial accounts without ever contacting the individual or offering a service or product. This is commonly known as "slamming a list" or "running a database".

ICE was able to obtain seizure warrants for monies in two third party payment companies' bank accounts, resulting in the seizure of eight U.S. bank accounts totaling approximately $3.1 million dollars, more than $2 million of which was from ICT. Only after Cimicato was contacted by law enforcement and consumer protection agencies did he take action against some of the telemarketing companies his company had processed payments for. To date, numerous State Attorney Generals have filed civil actions against various companies previously identified by ICE to impede these businesses from doing business within their respective jurisdictions.

## Red Flag Indicators

- The bank of initial deposit for draft checks shows many draft checks deposited followed by wire transfers out of the account to both foreign and domestic bank accounts, with a large number of the transactions returned as unauthorized or fraudulent.
- Accounts set up to receive wire transfers from the payment processor have many wires for large amounts of money that are deposited and subsequently wired out in a relatively short period of time.
- Wire transfer of funds to commercial accounts with no logical relationship or connection to the sender of the funds.
- Third-party service providers have a history of violating Automated Clearing House (ACH) network rules, generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.
- ACH transactions for larger amounts of money often originate from non-bank customers for which the bank has no or insufficient due diligence.

# Second Annual European Serious Organised Crime Conference

In March 2009, Deputy Assistant Director Janice Ayala, of the ICE Financial, Narcotics and Public Safety Division, delivered the international keynote address at the 2nd Annual European Serious Organised Crime Conference, sponsored by the Merseyside Police and Merseyside Police Authority in the United Kingdom.

The conference focused in part on the link between terrorism and organised crime and looked at harm reduction measures. Additionally, the conference also showcased major successes in the fight against organized crime and encouraged the facilitation of partnerships between police forces, border control services, immigration enforcement agencies and other key stakeholders.

Unit Chief David Eoff from the Asset Forfeiture Section at ICE headquarters, also participated in a group panel discussion about the use of forensic accountants during asset forfeiture investigations.