

Investigative Programs



*Protecting America's
Financial Systems*



**Homeland
Security**

Contents

I.	<i>Press Release</i>	1
II.	<i>Fact Sheet and Case Examples</i>	3
III.	<i>A snapshot of successful ICE financial investigations since the creation of the Department of Homeland Security on March 1, 2003</i>	10
IV.	<i>A snapshot of successful Secret Service financial investigations since the creation of the Department of Homeland Security on March 1, 2003</i>	12
V.	<i>Graphics:</i>	14
	<ul style="list-style-type: none">• <i>Examples of How Money is Laundered Through Life Insurance Policies</i>• <i>Example of How Money is Laundered Through Global Trade</i>• <i>Features of the new \$20 Bill</i>	

U.S. DEPARTMENT OF HOMELAND SECURITY

Office of the Press Secretary

FOR IMMEDIATE RELEASE

July 8, 2003

**SECRETARY RIDGE ANNOUNCES
NEW FINANCIAL INVESTIGATIONS INITIATIVES**

***Unveils Comprehensive New Programs to Protect U.S. Financial Systems from
Criminal Exploitation***

NEW YORK, NY – In a speech at the New York Federal Reserve, the Secretary of Homeland Security, Tom Ridge, today announced programs to safeguard the nation's financial systems against criminal exploitation. Two of the many actions being taken by the Department of Homeland Security (DHS) include the creation of a new financial crimes investigative initiative and an expansion of already successful electronics crime task forces. Secretary Ridge also announced a groundbreaking initiative designed to share specific information with the nation's top financial institutions, about financial systems weaknesses discovered through the Department's criminal investigations.

Secretary Ridge announced *Operation Cornerstone*, a new financial investigations initiative that will not only prosecute money laundering crimes but will initiate a new approach of working with the private sector to shore up potential weaknesses in financial systems.

In short, *Operation Cornerstone*, run by the Bureau of Immigration and Customs Enforcement (ICE), is a new financial investigations program that will identify vulnerabilities in financial systems through which criminals launder their illicit proceeds, bring the criminals to justice and work to eliminate the vulnerabilities. Through a working partnership with industry representatives, ICE will share information learned from these investigations to eliminate industry-wide security gaps that could be exploited by money launderers and other criminal organizations.

Secretary Ridge also announced that the Secret Service is expanding its highly successful Electronic Crimes Task Forces to four additional cities. The Secret Service currently runs task forces in 9 cities. The four new cities are Cleveland, Houston, Dallas and Columbia, South Carolina. The 9 existing task forces are operating in New York, Los Angeles, Miami, Charlotte, San Francisco, Las Vegas, Boston, Chicago, and Washington, D.C.

These task forces investigate a wide range of computer-based criminal activity. Examples include e-commerce frauds, identity crimes, telecommunications fraud, and a wide variety of computer intrusion crimes that affect a variety of infrastructures. Since its inception in 1995, the New York Electronic Crimes Task Force alone has charged over 800 people with electronic crimes valued at more than \$500 million.

Earlier in the day Secretary Ridge toured the Secret Service's Electronic Crimes Task Force in New York, as well as ICE's El Dorado Task Force. The El Dorado Task Force has investigated numerous money laundering and other financial crimes since its inception in 1992. In eleven years El Dorado Task Force agents have arrested 1,753 individuals and seized nearly \$560 million in criminal proceeds.

"Safeguarding the integrity of America's financial systems is a key part of homeland security," said Secretary Ridge. "Criminal organizations are seeking new ways to finance their operations, and the Department of Homeland Security is moving aggressively to identify vulnerabilities within U.S. financial systems that could be exploited to those ends."

To aid the financial industry in its own efforts to shore up vulnerabilities in its systems, Secretary Ridge announced a new program jointly run by ICE and the Secret Service. Under this new program called SHARE (Systematic Homeland Approach to Reducing Exploitation), officials from the Secret Service and ICE will jointly conduct semi-annual meetings with executive members of the financial and trade communities impacted by money laundering, identity theft, and other financial crimes. In these meetings special agents and analysts from the two Homeland Security agencies will share data on specific investigative outcomes from investigations into money laundering, identity theft, and other financial crimes.

By taking the Secret Service's long experience with investigating crimes like counterfeiting, identity theft and credit card fraud, and ICE's long experience with investigating illegal efforts to launder or mask the true source of criminal proceeds – and sharing that experience with the financial community, American pocketbooks and bank accounts will be far safer, Secretary Ridge explained in his remarks.

Before his speech, Secretary Ridge met with leaders from the top financial institutions to brief them on the new initiative. "It's critical we work in partnership with the financial community," Secretary Ridge told the financial leaders. "Unless we share the specific findings of our investigations, we run the risk that our nation's financial systems will remain vulnerable to exploitation. We can't let that happen."

Secretary Ridge announced that the first meeting under the SHARE program will take place by mid-October.

###

U.S. DEPARTMENT OF HOMELAND SECURITY

Office of the Press Secretary

July 2003 – Fact Sheet

Financial Investigations and Financial Infrastructure Protection

The Department of Homeland Security plays a critical role in the government's efforts to investigate financial crimes and to help the financial community identify and eliminate potential weaknesses in our nation's financial infrastructure. DHS is drawing on the expertise of the Bureau of Immigration and Customs Enforcement (ICE) – a part of the Border and Transportation Security Directorate – and the U.S. Secret Service – to expand their existing capabilities in an effort to better protect America's financial service systems from illegal money laundering, insurance schemes, identity theft, bulk cash smuggling, counterfeiting, credit card fraud and similar financial crimes.

Initiatives:

Expanding Electronic Crimes Task Forces from 9 to 13:

Under the USA Patriot Act of 2001, the U.S. Secret Service was authorized to establish a nationwide network of electronic crimes task forces, drawing on its successful New York task force. Thus far, the Secret Service has established nine task forces in New York, Los Angeles, Miami, Charlotte, San Francisco, Las Vegas, Boston, Chicago, and Washington, D.C. Four additional electronic crimes task forces are being established in Cleveland, Houston, Dallas and Columbia, South Carolina

The Thirteen Electronic Crimes Task Forces will -

- Focus primarily on computer-based crimes involving the theft of funds, credit information, identities, and network intrusions.
- Investigate identity crimes, telecommunications fraud, and computer intrusion crimes (such as credit card fraud).
- Identify weaknesses in key systems through which criminals could steal funds, credit card information or individual identities.
- Partner with federal, state and local law enforcement agencies, as well as key segments of the private sector (e.g., the telecommunications industry) and academic community to understand and eliminate systemic weaknesses.

Launching Operation Cornerstone, A New Financial Investigations Program:

The Bureau of Immigration and Customs Enforcement (ICE) is launching Operation Cornerstone – a new financial investigations program to identify vulnerabilities in financial systems through which criminals launder their illicit proceeds, bring the criminals to justice, eliminate the vulnerabilities, and develop a working partnership with industry representatives to share information and close industry-wide security gaps that could be exploited by money launderers and other criminal organizations.

Cornerstone will

- Identify and assess the means and methods used by criminals to exploit financial systems in order to transfer, launder and otherwise mask the true source of criminal proceeds.
- Work with specific private sector industries to gather new information and reduce vulnerabilities found within existing financial systems.
- Assign a dedicated special agent to each of the 25 ICE field offices to liaison with the private sector.
- Investigate and prosecute criminal organizations exploiting emerging traditional and non-traditional financial systems.

- Work with financial institution security teams to help them understand how criminal organizations exploited financial systems in their industry.
- Provide the private sector with a quarterly report that details specific examples of how certain U.S. financial systems are being exploited by criminal organizations to transfer, launder or mask the true source of criminal proceeds. The report will provide recommendations to industry on how to detect and prevent such exploitation.

Launching the SHARE program:

Under the SHARE (Systematic Homeland Approach to Reducing Exploitation) program, officials from the Secret Service and ICE will jointly conduct semi-annual meetings with executive members of the financial and trade communities impacted by money laundering, identity theft, and other financial crimes, to share data on specific investigative outcomes from investigations into money laundering, identity theft, and other financial crimes. The first meeting under the SHARE program will take place by mid-October.

Historic Expertise

Protecting Against Computer-based Crime:

- Since 1984, the Secret Service has been the primary authority for the investigation of access device fraud, including credit and debit card fraud.
- Today, the vast majority of financial transactions are electronic. Billions of dollars are moved through financial payment systems each day.
- Identity crime includes identity theft, credit card fraud, bank fraud, check fraud, false identification fraud, and passport/visa fraud (See Appendix A for case examples).
- Identity crimes are almost always associated with other crimes such as narcotics and weapons trafficking, organized crime, mail theft and fraud, money laundering, immigration fraud, and terrorism.
- Last year the Secret Service arrested 1143 people for violations involving credit card or access device fraud.
- In FY 2002, the Secret Service opened 1833 new cases involving credit card fraud, with a potential dollar loss totaling \$565 million.

Protecting Against Money Laundering:

- Agents from the former U.S. Customs Service have investigated money laundering and similar financial crimes since the 1970's. This expertise is now vested in the Department's Border and Transportation Security Directorate, within ICE.
- Drug organizations and other criminal groups have used many methods to launder their illegal proceeds. ICE agents have investigated thousands of cases that used these various schemes. They are now using that expertise to not only investigate criminal organizations, but through the newly announced SHARE program, to also alert financial institutions about the methods – or typologies – they uncovered.
- ICE agents have become expert at investigating the complete range of systems exploited by money launderers and other criminals to cleanse or mask the source of their illicit proceeds, including banking systems, money services businesses, bulk cash smuggling systems, trade-based money laundering systems, illicit insurance schemes, and illicit charity schemes. (See Appendix A for case examples.)
- Billions of dollars in criminal proceeds each year flow through the nation's financial systems. In one case alone in the mid-1990's, ICE agents discovered a scheme that funneled more than \$1 billion in drug proceeds from New York to Colombia through wire remitters.

Protecting Against Counterfeiting:

The U.S. Secret Service was founded in 1865 expressly to fight the counterfeiting that had become rampant during the Civil War – nearly one third of all currency was fake. For 138 years, the Secret Service has

worked to protect the integrity of our nation's currency. Today the Secret Service fights counterfeiting in new ways.

- New Color of Money - On May 13, 2003, the new design for the latest \$20 Federal Reserve Note was unveiled. The Secret Service worked closely with Treasury officials to develop features that make the bill more difficult to counterfeit. It's the first time that the U.S. dollar has been printed with colors other than green and black since the early 1900s, and the first time that offset printing – for the background colors – will appear on U.S. currency (**See Graphic**).
- New Features – The new design also contains improved features to deter counterfeit notes produced using home computers, office copiers, and similar technology. These include:
 - *Watermark* -- the faint image similar to the large portrait, which is part of the paper itself and is visible from both sides when held up to the light.
 - *Security thread* -- also visible from both sides when held up to the light, this vertical strip of plastic is embedded in the paper. "USA TWENTY" and a small flag are visible along the thread.
 - *Color-shifting ink* -- the numeral "20" in the lower-right corner on the face of the note changes from copper to green when the note is tilted. The color shift is more dramatic and easier to see on the new-design notes.

Partnering With the Law Enforcement and the Financial Community

- The Department of Homeland Security is launching the SHARE (Systematic Homeland Approach to Reducing Exploitation) program to provide private sector executives with progress updates on its financial investigations and information on new trends and vulnerabilities discovered during these investigations. The SHARE program is a joint ICE / Secret Service initiative that provides data on specific investigative outcomes to executive members of the financial and trade communities impacted by money laundering, identity theft, and other financial crimes. The first meeting will be convened by mid-October.
- DHS is also conducting joint studies and training programs for members of the financial and trade communities:
 - As part of the *Cornerstone* Program, ICE has created a unit solely dedicated to providing training to the private sector on how to identify and prevent exploitation by criminal organizations.
 - The Secret Service and the Computer Emergency Response Team Coordinating Center (CERT/CC) of Carnegie Mellon University have embarked on an analysis of network, system and database compromises committed by malicious insiders. The results of the "Insider Threat Study" will help the partnering agencies develop accurate information about insider intrusions that can help efforts to identify and prevent future intrusions before they occur.

Leading Task Forces

El Dorado Task Force:

- The El Dorado Task Force (EDTF) was started in 1992 as a joint initiative between the former Customs Service and the Internal Revenue Service. The mission of the El Dorado Task Force is to dismantle and disrupt money-laundering and criminal financing organizations operating in the New York/New Jersey area utilizing the tools and resources of all participating agencies. The EDTF, the largest money-laundering task force in the nation, has seized over \$557 million dollars and arrested 1,753 individuals since its inception.
- The EDTF is made up of two components, an operational component and intelligence component. The operational component is housed in 7 offices and consists of 263 members from 37 agencies. The EDTF intelligence unit consists of 39 members from 12 agencies with participating liaisons from 5 agencies.

- The EDTF is comprised of representatives from the IRS, NYPD, New York State Police, FBI, Manhattan and Queens District Attorney Office.

Electronic Crimes Task Forces:

- Since its inception in 1995, the New York Electronic Crimes Task Force has charged over 800 people with electronic crimes valued at more than \$500 million. The task force has also trained over 13,000 law enforcement personnel and private representatives in the criminal abuses of technology and how to prevent them.
- With the passage in October 2001 of the USA PATRIOT Act, a direct response to the September 11th terrorist attacks, the U.S. Secret Service was authorized by Congress to expand beyond the New York City task force, and establish a nationwide network of similar electronic crimes task forces.
- The types of investigations handled by the task forces encompass a wide range of computer-based criminal activity. Examples include e-commerce frauds, identity crimes, telecommunications fraud, and a wide variety of computer intrusion crimes that affect a variety of infrastructures.

APPENDIX A

Case Examples

- **Credit Card Network Intrusion** - In early February 2003, a Credit Card processing company reported a potential network intrusion to the Secret Service. A computer forensic examination by Secret Service agents determined that the company's computer system had been compromised, and over 10 million credit card numbers, with corresponding expiration dates had been stolen. A computer forensic investigation of the Internet Service Provider (IP) addresses traced the intrusion to a number of web servers in the United States, Europe, and Southeast Asia. The Secret Service worked in conjunction with the company to prevent losses due to this theft and to date, no fraud loss has been associated with these stolen credit card numbers. The investigation is continuing.
- **Money Laundering Through Insurance Schemes** –During a long-term drug trafficking investigation in the 1990s, ICE agents in Miami learned that Colombian drug cartels were laundering large quantities of money through the purchase of life insurance policies in Europe, the United States, and offshore jurisdictions. Based on this information, ICE agents launched Operation Capstone in 2000. The probe soon revealed the Colombian cartels, using a small number of insurance brokers, were purchasing investment-grade life insurance policies with cartel associates as the beneficiaries. The policies were purchased with drug proceeds sent to the insurance companies via wire transfers and checks by third parties around the globe. The investigation revealed that the cartels were then cashing out these policies after short periods of time, despite the financial penalties invoked for early liquidation. The cartel beneficiaries would then receive a check or wire transfer from the insurance company that, on its surface, appeared to be legitimate insurance/investment proceeds. The cartels could use these “clean” funds virtually without question. Agents determined the cartels had used this scheme to purchase at least 250 life insurance policies and launder some \$80 million worth of drug proceeds. In December 2002, ICE announced the seizure of nearly \$30 million, the arrest of nine individuals, and charges against five additional individuals as a result of this joint probe by authorities in the United States, the Isle of Man, the United Kingdom, Colombia, and Panama. (See Graphic)
- **Treasury Securities Fraud** – In early 2002, the Secret Service was notified by the Bureau of Public Debt of a scheme to defraud the government of \$1.3 billion in Treasury Securities. This scheme was perpetrated using the popular electronic system, TreasuryDirect, which sells Treasury securities through an auction-style bidding process. TreasuryDirect was initiated in 1986 to allow individuals to buy bills and bonds at a noncompetitive auction without having to receive paper certificates. In 1997, electronic access was added to the system to allow bids over the telephone and the Internet. A discrepancy of involving improper bids first attracted the attention of Treasury officials after an investor failed to submit payment for the Treasury securities. A computer forensic investigation of the bid by agents of the Secret Service revealed that an individual established a TreasuryDirect account and placed orders for approximately \$1.3 billion in Treasury Bills and Treasury Notes. This bid was backed by funds allegedly held in California bank account. Investigation of that bank account revealed that it held a zero balance. Further investigation by agents of the Secret Service resulted in the arrest and conviction of one individual for violation of federal wire fraud statutes.
- **Commodities-Based Money Laundering: Gold & Diamonds** – On June 5, 2003, ICE agents arrested 11 individuals at seven different jewelry stores in Manhattan's diamond district on charges of participating in an international money laundering scheme. The arrests were the culmination of a long-term investigation which began when ICE agents received information that Colombian drug cartels were laundering substantial amounts of money through the purchase, smuggling, and resale of gold and diamonds. Intelligence indicated that Colombian drug organizations were instructing their U.S. employees to purchase precious stones in New York with drug proceeds, then smuggle these items to Colombia, where they

were resold to refiners for “clean” pesos that the traffickers could use risk-free. Based on this information, ICE agents launched an investigation in 1999 into several New York jewelers alleged to be involved in the money laundering scheme. According to the charges, the New York jewelers were approached by undercover agents posing as drug dealers. The undercover agents informed the jewelers they were looking to buy gold and diamonds with their illicit funds so they could smuggle these precious metals to Colombia and resell them to refiners in exchange for “clean” cash. According to the charges, the jewelers willingly accepted some \$1 million in drug funds from undercover agents. They also offered to smelt the gold into small objects, such as belt buckles, screws, and wrenches, in order to facilitate the smuggling of these goods to Colombia

- **Money Laundering Through the Banking Industry** – On November 27, 2002, a Manhattan bank pleaded guilty to a three-count information charging it with failure to file required reports on \$123 million in suspicious cash deposits, failure to implement an anti-money laundering program, and helping to “structure” \$76 million in bulk cash deposits. The event marked the first time that a U.S. bank had ever pled guilty to the first two charges. The plea came as a result of a four-year investigation by ICE’s El Dorado Task Force in New York. The investigation disclosed that this bank had become a bank of choice for criminal organizations seeking to conceal their illicit financial activities from the government. One drug money laundering organization made \$46 million worth of cash deposits at the bank. In many cases, members of the organization literally brought duffel bags full of cash into the bank for deposit. According to details of the plea agreement, the bank almost never filed the required reports on such deposits, which were promptly wired to locations in Latin America. The cash deposits were so large that bank tellers complained to managers about having to count the cash during their lunch breaks. Another example of the bank’s disregard for anti-laundering laws occurred when it opened new accounts for an individual whose account at the bank had just been frozen by the government for money laundering activity. The individual promptly began structuring cash deposits into his new account. Once again, the bank failed to file any of the required reports on these structured cash deposits. As part of its guilty plea, the Manhattan bank agreed to pay a \$4 million fine.
- **Black Market Peso Exchange** – In March 1997, ICE agents launched an undercover investigation into a Colombian drug smuggling / money laundering organization. Over the next two years, undercover ICE agents posed as money launderers for this organization. Agents routinely picked up drug cash from employees of this organization in various U.S. cities, and deposited these funds into undercover bank accounts. The Colombian organization then instructed the agents to wire these drug funds to specified bank accounts around the globe. As it turned out, many of these accounts belonged to major U.S. companies. In one example, undercover agents were ordered by the Colombian organization to pick up a suitcase full of drug cash in New York. They next day, they were ordered by the organization to wire transfer \$335,800 of these funds, in five separate payments, to an account belonging to a major U.S. company. ICE agents later determined that these wire transfers (of drug proceeds) to the U.S. company constituted partial payment for a helicopter that the company was exporting to Colombia. The investigation further revealed that this U.S. company had received a total of 31 different wire transfers from individuals completely unrelated to the buyer as payment for the \$1.5 million helicopter. In July 1999, ICE agents froze the funds they had wired to this company’s account, as well as funds they had wired to the accounts of many other U.S. companies, on grounds that the monies constituted drug proceeds. The investigation revealed that many of these U.S. companies had been paid in drug money for products that they were exporting to Colombia. Ultimately, in August 2000, the helicopter in question was seized in Panama on grounds that it had been paid for with drug money. The case highlighted how U.S. firms can become entangled in the Black Market Peso Exchange, a vast trade-based money laundering system that frequently results in major U.S. companies being paid in drug money for their exports. On an annual basis, an estimated \$5 billion worth of drug funds are laundered through the Black Market Peso Exchange. The Black Market Peso Exchange operates in the following manner. Colombian cartels accumulate vast sums of

cash from drug sales in major U.S. cities. The cartels then sell these U.S.-based drug dollars to Colombian money brokers and, in return, receive “clean” pesos in Colombia. The money brokers then place these dollars into the U.S. banking system through a variety of methods and offer them for sale to Colombian importers. After receiving pesos from the Colombian importers, the money brokers route the drug dollars to U.S. firms to pay for goods ordered by the Colombian importers. Ultimately, American firms receive payment in drug dollars for goods they ship to Colombian importers. **(See Graphic)**

Selected Financial Investigations by
The Bureau of Immigration and Customs Enforcement (ICE)
Since March 1, 2003

- **11 Charged in Baby Formula Theft Scheme That Sent Funds to Middle East** – On June 20, a federal grand jury in Dallas returned three indictments charging 11 individuals with felony violations relating to an organized theft scheme in north Texas that routed its proceeds to the Middle East. The charges resulted from a joint investigation by ICE and the Fort Worth Police Department, with assistance from other law enforcement agencies. The probe revealed that a retail theft organization in north Texas purchased stolen baby formula and other products, then resold these stolen products to wholesalers around the United States. Millions of dollars in proceeds from this scheme were allegedly routed to Jordan, Egypt, and Palestinian Territories.
- **6 Arrested for Illegally Transmitting \$70 Million to Pakistan** – On June 17, agents from ICE and the IRS arrested six individuals on charges of illegally transferring roughly \$70 million to Pakistan via unlicensed money transmittal businesses in New York and New Jersey. Agents from ICE and the IRS also executed three search warrants, seizing \$57,000 in currency and many boxes of evidence.
- **Guilty Plea in Wire Transfer Scheme that Routed \$12 Million to Iraq** – On June 12, Hussein AlShafei, an individual in Washington state, pleaded guilty to a federal money laundering charge in connection with the illegal transfer of more than \$12 million to Iraq. The ICE investigation revealed that AlShafei employed a nationwide network of money transfer agents who collected funds for AlShafei to illegally transfer to Iraq, via Jordan, the United Arab Emirates, and other nations.
- **31 Charged with Laundering Millions Through Wire Remitting Firms** -- On June 5, a federal grand jury in New York charged 31 individuals with money laundering violations as a result of an ICE/El Dorado Task Force investigation which disclosed that several money remitting businesses in the New York metropolitan area were illegally wiring millions of dollars worth of drug funds to Colombia.
- **11 Charged in Laundering Scheme Involving Purchase and Resale of Gold** -- On June 5, ICE agents arrested 11 individuals in New York who had been charged money laundering as a result of an ICE/El Dorado Task Force probe which found that Manhattan jewelry stores were helping Colombian drug cartels launder millions through the purchase, smuggling, and resale of gold. In many cases, the jewelry store owners smelted the gold into small objects to facilitate international smuggling. ICE seized \$860,000 in U.S. currency, gold, and diamonds in the raids.
- **\$5.4 Million in Texas Lottery Winnings Forfeited** – On June 4, a federal jury in Texas determined that \$5.4 million worth of Texas lottery winnings by Jose Betancourt would be forfeited to the government. An ICE investigation had disclosed that Betancourt, a convicted narcotics trafficker, had purchased the winning lottery ticket with drug proceeds. Betancourt was assessed an additional \$76,000 penalty.
- **Credit Card Fraud Proceeds Routed to Lebanon**– On June 4, a federal grand jury in the District of Massachusetts charged four individuals with conspiracy, credit card and access device fraud violations after an ICE investigation revealed that the individuals were exporting to Lebanon non-bearer checks and gift cards purchased with the proceeds of a complex credit card fraud scheme.
- **Guilty Plea in Scheme to Illegally Wire \$5 Million Abroad** – On May 28, Ahmed Abdu, a Sudanese national, pleaded guilty in New York to charges that he conspired to operate an unlicensed money transmitting business that wired more than \$5 million abroad. During this prosecution, ICE agents utilized Section 319 of the Patriot Act to seize funds from five interbank accounts of foreign banks. This represented the first time this law enforcement tool had been used in the Southern District of New York.

- **Alternate Remittance Network Charged with Illegally Sending \$32 Million Abroad --** On May 21, federal prosecutors in New York unsealed charges against nine individuals accused of participating in an unlicensed money transmittal business that had transmitted more than \$32 million abroad since January 2001. The ICE investigation also disclosed that members and associates of this business were involved in a large-scale document fraud scheme involving the creation of fake driver's licenses and the falsification of Indian passports to smuggle illegal aliens into the United States.
- **\$21 Million Fine Against Individual Who Defrauded Elderly Investors –** On May 6, an individual was sentenced in Cleveland to nine years federal imprisonment and ordered to pay \$21 million restitution. Best had pleaded guilty to money laundering wire fraud, and conspiracy to commit securities fraud as a result of his involvement in an organization that defrauded elderly investors of more than \$41 million.
- **Guilty Plea in \$12 Million Counterfeit Check Scheme –** On April 19, Omar Shishani pleaded guilty in Detroit to possessing \$12 million worth of counterfeit checks. Shishani was arrested in July 2002 at the Detroit Metropolitan Airport after arriving on a flight from Indonesia. Subsequent investigation by ICE and the Secret Service linked Shishani to two other violators who have been indicted for conspiracy to distribute and/or manufacture counterfeit securities.
- **\$33 Million Illegally Funneled to Pakistan –** On March 20, 2003, ICE agents and FBI agents in New York arrested 4 individuals, seized \$71,400, and executed multiple bank seizure warrants in connection with an investigation into a Pakistani money remittance business called Manhattan Foreign Exchange. The 18-month ICE/FBI probe revealed that Manhattan Foreign Exchange moved more than \$33 million to Pakistan during a three-year period, much of which constituted proceeds of illegal activity. The joint investigation also revealed that associates of this business sold fake (U.S., Pakistani, Canadian, and British) passports and travel documents.

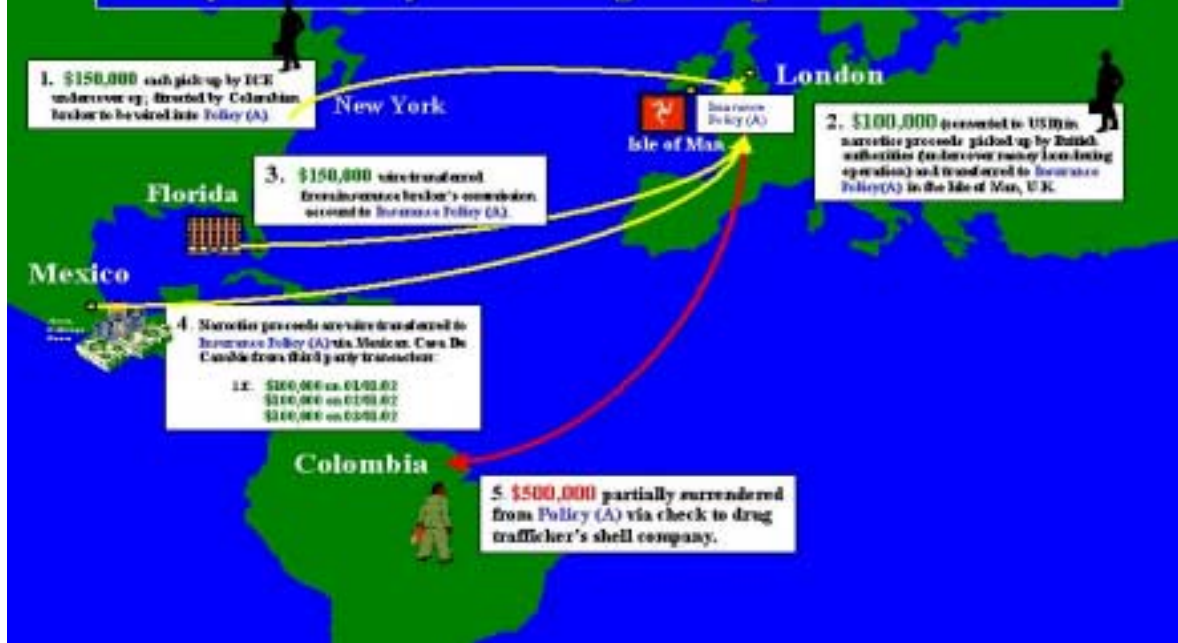
Selected United States Secret Service
Financial Crimes and Financial Infrastructure Investigations
Since March 1, 2003

- **Suspect Arrested in \$800,000 Identity Theft Ring** - On June 27, U.S. Secret Service agents arrested an individual suspected of being the mastermind behind counterfeit credit card/identity theft ring in the Detroit area. Working in conjunction with the Detroit Metro Identity Fraud Task Force, agents identified the individual – known by the alias “Frank” – as the person behind the operation, which involved the skimming of credit card numbers from area retailer and the production of counterfeit credit cards and false identification cards. In the last four years, the suspect and his associates are responsible for nearly \$800,000 in losses to area merchants.
- **Two Indicted and Arrested for Stealing Millions of Dollars Worth of Satellite TV Transmissions**– Secret Service agents from the Detroit Field Office recently arrested two individuals indicted of conspiracy charges stemming from the sale and manufacture of illegal decryption devices. The suspects sold \$127,000 worth the devices used to intercept Direct TV Satellite Signals over the internet. Direct TV estimates the losses to exceed several million dollars as a result of stolen transmissions. Agents also seized 1,300 decryption devices either assembled or in the assembly stage.
- **Million-Dollar Credit Card Fraud Scheme Stopped** – On June 26, Agents of the Houston Field Office arrested two individuals for violation of 18 USC 1029 - Access Device Fraud and 18 USC 371 Conspiracy to commit Access Device Fraud. The suspects had conspired to commit numerous types of credit fraud to include instant credit fraud, account takeover, re-encoding credit cards, identity theft and the production of counterfeit identification. They had committed these crimes continuously over a period of two years, netting nearly \$1 million. Information was obtained through one of the suspects, who worked in the billing department of a local doctor’s office and would provide copies of credit card receipts. To date, 828 credit card account numbers have been uncovered by agents investigating the case, though it is believed that over 2,000 credit card numbers may have been obtained.
- **“Cash Money Boys” Arrested for Counterfeit Commercial Checks** - A leaders of a Detroit area fraud ring, known as the “Cash Money Boys,” were arrested by the Secret Service after the discovery of more than 100 commercial checks from six different local banks. Known losses in the case exceed \$1.3 million and 11 federal arrests and 2 federal arrest warrants have resulted from the case.
- **14 Arrested in \$10 Million Bank Fraud Case** - On June 18, the Secret Service Newark Field Office, working together with the FBI, U.S. Postal Inspection Service and the Hudson County Prosecutor's Office arrested 14 people involved in a bank fraud scheme. The suspects, using assumed or stolen identities, compromised bank accounts and then conspired to launder proceeds, using the funds as down payments on luxury homes in exclusive neighborhoods. With the assistance of collusive mortgage brokers and appraisers, the suspects then obtained first and second mortgages which exceeded the actual value of the properties, enabling the "buyers" to walk away with hundreds of thousands of dollars in cash at the closing. Also involved in this group is an individual who conspired to re-enact life insurance policies on terminally ill patients, in an effort to collect substantial benefits. Fifteen teams, made up of thirty law enforcement agencies, executed 25 search/arrest warrants, resulting in 13 individuals arrested in New Jersey, and one additional arrest in Philadelphia. The actual fraud loss is estimated at \$10,000,000.
- **Colombian Counterfeit Plant Seized** – On June 13, Secret Service agents joined Colombian police in executing five search warrants in the Cali area, including the seizure of a complete counterfeit manufacturing plant. Plates, negatives bearing images of CFT \$100 Federal Reserve Notes, inks, machinery and printing paraphernalia were seized by Colombian National Police

(DIJIN) officials, as was a total of \$30,000 in finished counterfeit \$100 notes. Eight people have been arrested in connection with this case.

- **Wilmington Man Arrested for Wire Fraud and Money Laundering** – On June 13, Secret Service agents from the Wilmington, NC Resident Office arrested an individual after his indictment on charges of Wire Fraud and Money Laundering. This case originated when the Wilmington Resident Office was contacted by an investigator for an investment company who advised that he had discovered that one of their local account representatives was perpetrating fraud on his clients. The Secret Service investigation revealed that the suspect had established a not-for-profit account with the investment company in the name of a local church and then transferred thousands of shares of securities, held by one of his elderly clients, into his "church" account. The suspect then wrote checks on the "church" account and deposited them into various personal accounts, and used the proceeds to pay off debts and to purchase two homes. The indictment includes a criminal forfeiture count seeking forfeiture of up to \$845,747.62 in proceeds from this fraud. Actual fraud loss in this case is \$700,000 with a potential loss of \$1.5 million.
- **\$6 Million Identity Theft Ring Busted** – After a two-year joint investigation, on June 5, the Secret Service San Francisco Field Office and Berkeley Police arrested two individuals responsible for a nationwide counterfeiting and identity theft ring that resulted in nearly \$6 million in losses from thousands of victims. As part of the investigation, at least 65 local and federal law enforcement officers served 12 search warrants Thursday, including locations in Berkeley, Oakland, San Leandro, Richmond, Antioch, Vallejo and Stockton looking for evidence. Among the items seized were a large number of counterfeit \$100 traveler checks, counterfeit personal checks, personal identification cards, including driver's licenses, and thousands of "personal profiles," which included names of probable victims, dates of birth, and Social Security and credit card numbers.
- **Miami Agents Shut Down Credit Card/False ID Plant** - As part of a six month investigation, on May 29, Secret Service agents from the Miami Field Office arrested four Cuban nationals and seized a large scale Counterfeit credit card/False Identification plant in South Beach. The target of the investigation was charged with manufacturing counterfeit credit cards and false driver's licenses. A total of 314 counterfeit drivers licenses were, as well as a number of Social Security cards and INS Employment Authorization cards. Machines seized included card printers, two drivers license machines, a tipper, computers, an embosser, a manual embosser for logo's, and equipment to replicate credit card holograms.
- **"Moors Nation" Members Arrested for Conspiracy** -- On May 21, nine members of a group know as the "Moors Nation" were indicted in the District of New Jersey for violation of 18 USC 514 (Fictitious Documents) and 18 USC 371 (Conspiracy). This group was responsible for passing over \$10 million dollars worth of fraudulent money orders that were purportedly issued by the Department of Transportation and Treasury. These fictitious money orders were used to purchase airline tickets, mortgages, car loans, personal loans and to pay debts. The arrests are a result of a joint two-and-a-half year investigation between the Secret Service, the Department of Transportation and the FBI.

U.S. Department of Homeland Security Example of Money Laundering Through Insurance Policies



U.S. Department of Homeland Security Example of Money Laundering Through Global Trade



The new \$20 design retains three important security features that were first introduced in the 1990s and are easy for consumers and merchants alike to check: watermark, color-shifting ink and security thread.



Security Thread

Hold the bill up to the light and look for the security thread, or plastic strip, that is embedded in the paper and runs vertically up one side of the note. If you look closely, the words "USA TWENTY" and a small flag are visible along the thread from both sides of the note.

Color-Shifting Ink

Look at the number "20" in the lower right corner on the face of the bill. When you tilt the note up and down, the color-shifting ink changes color from copper to green.

Watermark

Hold the bill up to the light and look for the watermark, or faint image, similar to the large portrait. The watermark is part of the paper itself and can be seen from both sides of the note.

The New Color of Money: Safer, Smarter, More Secure

Newly designed currency — with the addition of subtle background colors — will be issued beginning with the \$20 note in late 2003. New designs for the \$50 and \$100 notes will follow in 2004 and 2005. The introduction of new currency designs is part of an ongoing effort by the United States government to stay ahead of currency counterfeiting and to protect the economy and your hard-earned money.

For more information about new currency designs visit www.moneyfactory.com/newmoney