



# Combating terrorist financing and other financial crimes through private sector partnerships

Marcy M. Forman

*Department of Homeland Security, Office of Investigations, US Immigration and Customs Enforcement, Washington, District of Columbia, USA*

## Abstract

**Purpose** – Partnerships between the public and private sectors represent one of the strongest means to detect, deter, disrupt and deny terrorist and other criminal organizations illicit profits and material support required to fuel their evil acts. The purpose of this paper is to discuss and illustrate through case study, the importance of public and private sector partnership in combating terrorist financing and other financial crimes.

**Design/methodology/approach** – Two case studies are presented demonstrating how the public and private sectors can collaboratively work to target how criminal organizations earn, move and store their illicit profits. Highlighted is US Immigration and Customs Enforcement's (ICE's) outreach and partnership program, Cornerstone. Through working partnerships with US financial, trade, manufacturing and transportation sectors, Cornerstone's goal is to eliminate systemic vulnerabilities that could be exploited by terrorist and other criminal organizations.

**Findings** – ICE provides the private sector with information on trends, patterns, and "red flag" indicators that are identified during criminal investigations. This information can be used by the private sector to assist in establishment of internal controls and systems designed to protect their institutions from criminal exploitation.

**Practical implications** – Sharing identified vulnerabilities and information with trusted private sector partners, is the first line of defense against financial crimes, and the cornerstone of private/public partnership.

**Originality/value** – The paper stresses that all nations must recognize that any criminal act – whether driven by profit or ideology – threatens a nation's economic security and integrity. In today's global economy, this impact can have devastating consequences transcending many borders.

**Keywords** Terrorism, Financing, State security, Partnership, Private sector organizations, Public sector organizations

**Paper type** Case study

## Introduction

Homeland security is the responsibility of more than law enforcement and government – it is a shared mission of all people. Partnerships between the public and private sector represent one of the strongest means to detect, deter, disrupt and deny terrorist and other criminal organizations illicit profits and material support required to fuel their evil acts.

In March 2003, US Immigration and Customs Enforcement (ICE) was created as the largest investigative arm of the US Department of Homeland Security (DHS), and was stood up as an agency by combining 3,000 former US Customs Service (USCS) special agents, 2,500 former Immigration and Naturalization Service (INS) special agents, 4,000 Immigration and Deportation Service employees, and 1,500 Federal Protective Service personnel, into one unified law enforcement entity. The ICE investigative



---

mission combines and leverages all of the pre-existing law enforcement authorities of the former USCS and INS. In keeping with the mission of the DHS, ICE possesses great law enforcement and jurisdictional authorities, and among other things, is responsible for identifying financial systems vulnerable to criminal exploitation. To accomplish this, ICE employs a broad array of federal laws and resources to identify, interdict, seize, freeze and forfeit wealth associated with terrorists and other criminals. Along with its unique investigative tools and authorities, ICE legacy components have a long history in transnational and international money laundering investigations, and as a recognized leader in these investigations, ICE now possesses an even broader investigative remit in which to apply this expertise.

One of ICE's primary missions is the enforcement of the US Bank Secrecy Act (BSA) and the USA PATRIOT Act, to include: money laundering, bulk cash smuggling, other financial cross-border activities and crimes; and to identify, investigate, disrupt and dismantle terrorist and other criminal organizations involved in cross-border financial and trade crime. Each violation within the spectrum of ICE's investigative purview – financial investigations, contraband smuggling, export and arms control, commercial fraud, intellectual property rights, cyber crimes, and immigration violations (alien trafficking, identity, document and benefit fraud) – has a financial component that impacts the economic integrity and security of the nation.

During fiscal year 2004, ICE conducted 7,104 financial investigations resulting in the seizure of more than \$202 million, and over 1,505 arrests and 1,128 indictments for money laundering and other financial crimes.

During fiscal year 2003, ICE conducted roughly 7,230 financial investigations, resulting in the seizure of roughly \$213 million, and over 1,290 arrests and 832 indictments for money laundering and other financial crimes.

### **Terrorist and other criminal organizations**

The November 2003, General Accounting Office (GAO) report on Terrorist Financing (GAO-04-163) recognized that terrorist organizations are criminal organizations, and as such, need to earn, move and store funds. These organizations constantly adapt their methods to avoid detection and fulfill their goals.

Terrorists use a variety of alternative financing mechanisms to earn, move and store assets their assets based on common factors that make these mechanisms attractive to terrorist and criminal groups alike. For all three purposes – earning, moving, storing – terrorists aim to operate in relative obscurity, using mechanisms involving close-knit networks and industries lacking transparency. More specifically, first, terrorists earn funds through highly profitable crimes such as contraband cigarettes, counterfeit goods, and illicit drugs . . . terrorists also earned funds using systems such as charitable organizations that collect large sums in donations from both witting and unwitting donors. Second, to move assets, terrorists seek out mechanisms that enable them to conceal or launder their assets through nontransparent trade or financial transactions such as the use of charities, informal banking systems, bulk cash, and commodities that may serve as forms of currency, such as precious stones and metals. Third, to store assets, terrorists may use similar commodities, because they are likely to maintain value over a longer period of time and are easy to buy and sell outside the formal banking system.

ICE is uniquely positioned to impact the ability of terrorists and other criminal organizations to earn, move and store their illicit proceeds, and use it's broad

authorities, data sources, and expertise in this arena, in concert with the Federal Bureau of Investigation, and other law enforcement agencies. ICE Office of Investigations, wide range of investigative authorities and responsibilities touch on virtually all of the violations and underlying criminal activity.

Today's well-organized criminal groups engage in highly profitable crimes – generating enormous proceeds that are then laundered through a wide variety of means. Aggressive implementation of anti-money laundering programs within the US financial community has led to an increase in other nontraditional forms of money laundering, for example, innovative insurance schemes, exploitation of automated teller machines, and increasing reliance on bulk cash smuggling.

### **Layered defense**

The 9/11 Commission Report recommended a layered defense to combat terrorism, to include the private sector as well as government agencies. Recognizing that terrorist organizations are just one type of criminal organization and that any criminal activity can impact the security of a nation, and even the world economy – through damaging or undermining financial, trade, and transportation systems – an effective anti terrorism program and national security plan must include identifying and eliminating systemic vulnerabilities that could be exploited by all types of criminal organizations. It is law enforcement's responsibility to identify these vulnerabilities and behaviors indicative of criminal activity – and provide this vital information to the private sector for everyone's well being. It is also important to assist the private sector against fraudulent schemes aimed at their firms. These schemes rob the profits from legitimate businesses and fuel the illegal activity of terrorist and other criminal organizations.

An effective partnership between investigators and the private sector aids companies in implementing systems to prevent their firms from being exploited. A layered defense pushes terrorist and other criminal organizations to seek more desperate schemes that can be more readily identified and countered by law enforcement. Providing the private sector with red flag indicators of suspect behaviors assist them in identifying actions that can be referred to law enforcement for investigation. These simple investigative referrals – can result in the identification and dismantling of an entire criminal organization, or ideally lead to the prevention of a terrorist attack.

One example of an effective defense leading to identification of criminal activity involves the US Currency Transaction Reporting (CTR) requirement under the BSA. The CTR reporting requirements aim to prevent the introduction of illicit bulk cash deposits and transactions. The CTR requirement has forced criminal organizations to attempt to avoid filings, which actually results in behavior patterns and schemes that can be readily detected. The avoidance of CTR filing, known as “structuring” or “smurfing”, is an easily detectable indicator of criminal activity that has been successfully detected and used by law enforcement in thousands of cases.

### **First responders**

The private sector is the first line of defense against financial crimes perpetrated by criminal organizations. They operate and maintain the very systems criminal organizations seek to exploit for their illicit purposes. Regardless, if the crime is one of fraud against a financial institution or the use of a financial institution to move illicit

---

funds – virtually every criminal scheme requires the use of a financial institution in furtherance of criminal activity, i.e. the use of legitimate funds and seemingly legit financial transactions to further illicit activity. Examples include: the smuggling of counterfeit goods generates the same type of financial transactions normally associated with the legitimate importation of goods; the diversion of dual use or military items requires payment and re-appropriation of the proceeds. The financial sector is the first to witness these transactions, holds critical evidence, and acts as the first line of defense in securing and ensuring that institutions are not used to facilitate terrorist acts and other criminal activities.

### **Public-private partnership – ICE’s Cornerstone**

In July 2003, building on 18 months of targeting sources of terrorist financing under Operation Green Quest, ICE launched Operation Cornerstone, a comprehensive initiative that targets the means by which terrorist and other criminal organizations use to earn, move, and store illicit funds. Through working partnerships with US financial, trade, manufacturing and transportation sectors, Cornerstone’s goal is to eliminate systemic vulnerabilities that could be exploited by terrorist and other criminal organizations. The methodology behind Cornerstone is a systemic – rather than a case by case – approach to the investigation of cross-border financial, commercial trade and transportation crime.

Under the Cornerstone concept, ICE uses its unique authorities to investigate cross-border related crimes, by targeting the alternative financing mechanisms employed by criminal organizations. Such alternative mechanisms include commercial and immigration fraud, intellectual property rights crimes, counterfeit merchandise, import-export crime, contraband and human smuggling, and bulk cash smuggling. Cornerstone is addressing these homeland security vulnerabilities by not only investigating the crimes – targeting how criminal organizations earn, move and store their illicit profits – but also by developing a working partnership with the private sector to spot and address vulnerabilities in advance of the crimes themselves.

Through the Cornerstone outreach and partnership program, ICE provides the private sector with information on trends, patterns and “red flag” indicators that are identified during criminal investigations. This information can be used by the private sector to assist in establishment of internal controls and systems designed to protect their institutions from criminal exploitation. As of August 2005, Cornerstone field representatives and headquarters staff have conducted over 2,000 Cornerstone and financial crimes presentations to over 40,000 individuals in the private sector and law enforcement communities around the world.

In furtherance of Cornerstone:

- Over 100 dedicated Cornerstone special agents are assigned to ICE’s 26 field offices as liaisons to the private sector.
- Cornerstone liaisons share trends and “red flag” indicators of criminal activity with the private sector through outreach efforts.
- Cornerstone liaisons continuously develop contacts and partnerships within the private sector.
- ICE publishes quarterly newsletters titled *The Cornerstone Report*.

- ICE's interactive website at: [www.ice.gov/cornerstone](http://www.ice.gov/cornerstone), which has won two awards of excellence for design, content, and usefulness, provides detailed information to the private financial and law enforcement community on such topics as "red flag indicators" and how private industry can protect itself from exploitation from criminal activity.
- ICE has initiated nearly 200 investigations directly attributable to Cornerstone outreach efforts, from information received, resulting in substantial arrests and seizures.

### **Partnership in action: case studies**

#### *Case 1: Operation Cheque Mate*

In December 2004, ICE Special Agent in Charge, New York (ICE SAC/NY) culminated an 18-month investigation, entitled "Operation Cheque Mate", that identified and dismantled a network of individuals in London, England and the US who were, in part, responsible for the production of over \$15,000,000 worth of counterfeit/forged and stolen bank checks seized by ICE SAC/NY, and the defrauding of securities firms of \$250,000. Operation Cheque Mate was successfully conducted in partnership and cooperation with the financial trading community, UK and Spanish law enforcement, Interpol, and US regulatory agencies including the Securities and Exchange Commission, the Commodity Futures Trading Commission and the National Futures Association.

Over 50 private sector companies assisted ICE SAC/NY by either providing undercover email accounts and/or forwarding checks, applications and telephone recordings for handwriting, voice and fingerprint analysis. This information exchange led to the indictment of the two foreign-based principals, 11 arrest warrants; the conviction of two individuals for bank fraud; and the seizure of banks checks, along with stolen identities from both US and UK citizens. As of August 2005, the two principal violators are incarcerated in Spain pending extradition to the US.

*The scheme.* The London, England-based organization managed by the aforementioned two principals, profited hundreds of, thousand of dollars by establishing online trading accounts with numerous brokerage firms with either stolen, fictitious or their own identities. After establishing the online relationship, they would mail bulk packages containing checks ranging from \$61,000 to 600,000 along with applications in pre-addressed envelopes to a US based operative, who would then forward the envelope from a domestic address. This method is believed to attract less scrutiny than foreign correspondence. Soon after, they would request a wire transfer of trading profits to a foreign bank account. As a result, the firm would incur a loss after the check returned as counterfeit, or from a trading loss.

*The partnership.* As part of the combined and coordinated effort, several organizations, associations and brokerage firms placed alerts on their websites, warning potential investors and other firms about the fraudulent scheme. The alerts also included the name and contact number of the ICE case agent for the investigation. These postings resulted in numerous leads for law enforcement, and significantly reduced the potential loss to the securities industry. Based on the alerts and industry cooperation, 14 financial suspicious activity reports (SARs) were filed by affected brokerage firms in support of the ongoing ICE investigation.

---

After uncovering this network, ICE SAC/NY initiated two successful undercover operations to identify individuals and the fraudulent/collusive merchants in the New York area also responsible for receiving stolen checks for goods, laundering the proceeds of illegal activity and brokering such exchanges.

Fortunately, the losses sustained by the victim firms totaled just over \$250,000. Without the early detection and combined and coordinated efforts of law enforcement and the private sector, losses would have far greater.

*The vulnerabilities and red flag indicators.* Operation Cheque Mate disclosed to both law enforcement and industry several vulnerabilities and red flag indicators of criminal activity, as follows:

- non-adherence to best practices and “know your customer” guidelines;
- accepting identification that is unreadable, altered, poor quality copies or facsimiles;
- allowing trading prior to verification of identity through credit checks;
- trading prior to standard 10-day check verification period; and
- not requiring any identification from US citizen.

#### *Case 2: Access Inc. of USA*

The ICE special agent in charge, Newark, New Jersey (ICE SAC/Newark) in conjunction with the Internal Revenue Service (IRS), conducted this investigation based upon the filing of SARs by four different banks, regarding Access Inc. of USA, a licensed money service business (MSB) operating in New Jersey. Although Access Inc. was a licensed MSB, the owners and operators of Access Inc. conspired with four unlicensed money remitters operating out of New York to commit the criminal acts. One of the SARs filed on Access Inc. stated that an unidentified employee of the wire remitter attempted to deposit over \$10,000 in cash. According to the bank, when this employee was advised that the bank needed to verify his identity in order to complete a CTR, the employee refused to comply and changed the deposit to an amount under the reporting threshold.

*The scheme.* ICE and IRS, initiated the investigation of the owner and operator of Access Inc., who represented that he collected small amounts of funds from large numbers of Pakistani immigrants and transferred the funds to various accounts in Pakistan. The investigation actually revealed that the customer base consisted of very few people (approximately one to five per day) who brought large sums of US currency to the business. The business location was also not open to the general public. Access Inc. averaged over \$5 million per month in cash deposits, and the funds were promptly wire transferred out of the US to Europe, Asia and the Middle East.

In addition, New Jersey state law requires money remitters and their agents to register with the state. Although technically in compliance, the wife of the owner of Access Inc. was the license holder and the owner was listed as her registered agent. There were no other agents or sub-agents registered, and the owners never filed the required CTR for the individuals dropping off money.

*The partnership.* In addition to the SAR filings by three different banks, a fourth bank took the extra step of contacting the MSB owner and advising him of BSA requirements and bank policy. This same financial institution, in exercise of their “know your customer” best practices for commercial accounts, visited the Access Inc.

location to verify bank account application information. The SAR filings, and joint investigation by ICE and IRS agents culminated in the execution of six arrest and four search warrants at various locations, the seizure of almost \$200,000 in currency and monetary instruments, two firearms, computer/hard drive images, facsimile and adding machines, and numerous financial records. The subjects were charged with violations of operating an unlicensed/illegal money transmitting business, failure to file CTR, and conspiracy. Four of the six federal defendants were convicted of prohibition of unlicensed money transmitting business and aiding and abetting.

*The vulnerabilities and red flag indicators.*

- MSB was not open to the general public;
- MSB operated with a very limited number of clients, yet took in over \$100 million in cash deposits within 30 months;
- MSB owners failed to file CTR for cash deposits made by their clients;
- MSB prepared fraudulent records to evade their CTR obligations;
- amounts matching deposits were immediately wired off-shore; and
- MSB employee refused to provide identification to a bank official, when requested for CTR identification purposes.

**Conclusion**

All nations must recognize that any criminal act – whether driven by profit or ideology – threatens a nations economic security and integrity. In today’s global economy, this impact can have devastating consequences transcending many borders. Law enforcement must maximize every resource available to identify, disrupt and dismantle the illicit efforts of terrorist and other criminal organizations. Sharing identified vulnerabilities and information with trusted private sector partners, our first line of defense against financial crimes, is the cornerstone of private/public partnership.

**Corresponding author**

Marcy M. Forman can be contacted at: [marcy.forman@ledns.gov](mailto:marcy.forman@ledns.gov)