



# THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION

VOLUME 8 NUMBER 8

**FEBRUARY 2010**

**BANKING AND FINANCE  
SECTOR**

Banking System Disruptions ..... 2

Trade Based Money Laundering .. 4

Money Laundering Enforcement.. 6

Cyber Resilience..... 9

Information Exchange..... 12

Terrorist Financing..... 14

ACAMS ..... 16

Legal Insights ..... 17

Conference..... 19

**EDITORIAL STAFF**

**EDITORS**

Devon Hardy  
Olivia Pacheco

**STAFF WRITERS**

Joseph Maltby

**JMU COORDINATORS**

Ken Newbold  
John Noftsinger

**PUBLISHER**

Liz Hale-Salice

Contact: [CIPP02@gmu.edu](mailto:CIPP02@gmu.edu)  
703.993.4840

Click [here](#) to subscribe. Visit us online  
for this and other issues at  
<http://cip.gmu.edu>

In this issue of *The CIP Report*, we examine the Banking and Finance Sector. The preservation of this sector is vital to maintaining and protecting the global economy.

First, an Associate Professor of Economics from George Mason University discusses the consequences of disruptions in the banking system. A Principal at deKieffer & Horgan analyzes trade based money laundering. The Co-Director of the Institute for Information Policy at The Pennsylvania State University then reviews the methods involved with money laundering enforcement. The Executive Director of ChicagoFIRST discusses the enhancement of cyber resilience through risk management and information sharing. The concept of information sharing is further explored by the Vice President of Programs and Services at the Financial Services Information Sharing and Analysis Center. The next article provides recommendations to graduate programs for the development of terrorist financing courses. Finally, the Director of the Association of Certified Anti-Money Laundering Specialists describes the mission and the objectives of this international professional association.

This month's *Legal Insights* reviews the new Financial Fraud Enforcement Task Force, established in 2009 by Executive Order 13519: Establishment of the Financial Fraud Enforcement Task Force.

We also include an announcement about the upcoming conference, *Workshop on Grand Challenges in Modeling, Simulation, and Analysis for Homeland Security*, sponsored by the Department of Homeland Security Science and Technology, the Center for Infrastructure Protection, and The Society for Modeling & Simulation International.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter  
Director, CIP  
George Mason University, School of Law



**School of Law**

CENTER  
for  
INFRASTRUCTURE PROTECTION

# The Consequences of Disruptions in the Banking System

by Carlos D. Ramirez, Ph.D.

Department of Economics, George Mason University

Since the September 11, 2001 terrorist attacks, many scholars and policy makers have increased and intensified their research on the consequences of a sudden, unexpected disruption on critical sectors of the American economy. The idea is, of course, to understand the full ramifications of such disruptions in order to devise and implement strategies that would make that sector more resilient, should such undesirable events materialize. The Banking and Finance Sector is not immune to such disruptions. At first, this may not seem very obvious. After all, compared with the destruction of physical infrastructure or the tragedy of human deaths caused by terrorist attacks or natural disasters, the effects of such events on the financial system are surely less devastating.

Imagine a cyber-attack on our bank accounts. How would we react? The answer surely depends on the intensity and frequency of such attacks. A minor and rare disruption on our payment system would perhaps be considered to be annoying, but likely with negligible long-term consequences. However, with a catastrophic cyber-attack, the reaction may be very different. We may identify a cyber-attack as being catastrophic if the frequency and intensity of such attacks is high, including the disappearance

(temporary or permanent) of funds. With a catastrophic attack, we may feel that our financial system is vulnerable, especially if there is a general perception that the government is unable to prevent or control such attacks. As a result, we may end up taking much more drastic measures, including the more radical step of pulling some or even all of our wealth out of the financial system and into more rudimentary forms of savings, such as hiding our money “under the mattress,” figuratively and literally. This scenario is, of course, highly unlikely, but then again, a mere three years ago, so was the likelihood of a financial meltdown in the United States.

Such extreme reaction would be socially undesirable because it would lead to financial disintermediation — the disappearance of funds from the financial system, which could otherwise be used productively for funding worthwhile investment projects that fuel economic growth. The degree of financial disintermediation is undoubtedly going to be influenced by the frequency and intensity of such disruptions: the more severe the attack, the more vulnerable we may feel, and the more disintermediation may take place.

But how can we be sure that such a

scenario would unfold? And even if it unfolds, how serious or damaging is it likely to be? Unfortunately (or rather, fortunately), we have not experienced an intense or frequent enough terrorist-related disruption on our financial system to examine its consequences empirically. Nonetheless, we can learn a great deal by studying something that happens with much more frequency and intensity: banking and financial crises.

A banking crisis can be defined as a sudden and widespread increase in the number of bank failures. Notice that this definition implies that during crises, the number of failures is deemed to be “excessive.” Bank failures per se are not necessarily events to be avoided at all cost, and in a healthy capitalist system, it is completely normal and perhaps even expected that a few banks will fail. But when the frequency of failures increases to a systemic level, it may threaten the well-being of the system as a whole because it increases the likelihood of a banking panic, thereby amplifying the number of failures, and reaching a range that can be considered “excessive.”

A natural question to ask is: Do banking crises occur often? The answer, unfortunately, is yes. The

*(Continued on Page 3)*

## Banking Disruptions (*Cont. from 2*)

vast majority of countries have experienced such a crisis at some point in their recent or distant past. A study conducted by the International Monetary Fund in 1997 documents 112 banking crises in 93 countries between 1975 and 1995 alone. Since 1995, many countries, including Argentina, Russia, Thailand, South Korea, and currently the United States, have experienced systemic banking crises. In fact, at one time or another, virtually all developed countries have experienced such crises. Between 1860 and 1935, for example, the United States endured 10 serious banking crises, including 4 during the Great Depression. Thus, it is fair to say that no country is immune to such disasters. Given the frequency and severity of these crises, many academics, regulators, and policymakers have devoted countless hours to studying these phenomena: their causes, consequences, and policy implications. Sadly, despite the amount of research effort invested, it is evident that we have not yet been able to develop a foolproof mechanism for preventing or avoiding such disasters. This, of course, does not necessarily imply that all research effort has been a waste. But it does imply that we must continue to study banking crises in order to develop more efficient and practical policy tools.

So what are the consequences of banking disasters? The banking and finance literature generally highlights the immediate, short-term effects. In a recently published paper, I present evidence

indicating that banking disasters can also have long-term consequences and that these are very costly to society in terms of output and loss of productivity. In the rest of this article, I sketch the main arguments from both perspectives: that banking disasters have not only short-term but also long-term consequences.

### Short-Term Consequences

Most scholarly studies of the way in which banking distress affects the real side of the economy underscore the “credit crunch” hypothesis — the hypothesis that the credit crunch is the primary avenue by which banking distress is transmitted to the real side of the economy. According to this hypothesis (which is based on the work of Ben Bernanke, the current chairman of the Federal Reserve System), an adverse shock to the Banking and Finance Sector seeps into the real sector via a reduction in bank lending to customers who are heavily dependent on bank loans — typically households as well as small and medium-sized enterprises. As banks tighten consumer credit, a decline in consumer lending tends to aggravate a slump in aggregate demand. A decline in commercial lending affects the financial health of bank-dependent firms, possibly forcing some of them into bankruptcy.

These effects operate in the short run because they end up amplifying a business cycle downturn. As a result, the real sector suffers more than it normally would in a

business cycle downturn. This amplification is undesirable from a social standpoint since it also implies that the rate of unemployment peaks at a higher level than it should — that is, at a rate higher than the one we would expect to observe during downturns without banking crises. But the short-term perspective implies that as soon as banking conditions are normalized, credit will be restored and, at least in theory, the economy should return to its pre-banking-crisis level of activity. It is of course very likely that bank failures delay the speed at which the economy recovers from its slump, but — again, at least in theory — the delaying effects are temporary.

### Long-Term Consequences

Substantial literature on banking and finance, growth, and development has established that financial intermediaries can help stimulate economic growth. The basic mechanism that enables these intermediaries to influence growth is their ability to improve the allocation of resources between those who borrow and those who save.

This argument implies that banking crises could retard growth. That is, banking crises, besides having short-term effects, could have long-term ones as well. But how might this happen? If the banking system lacks institutions that promote or restore Banking and Finance Sector confidence (such as a credible deposit insurance system), or if the

*(Continued on Page 20)*

## Trade-Based Money Laundering

by Donald deKieffer, Principal, deKieffer & Horgan

Trade-Based Money Laundering (TBML) is neither an explosive favored by suicide bombers nor an orphan disease championed by Hollywood celebrities; it is far more insidious. Trade-Based Money Laundering is a method for moving vast sums of money across international boundaries virtually undetected. Although it requires a degree of sophistication, it is not so complex as to baffle organized crime, cosmopolitan con artists, or terrorist financiers. This method of moving money has numerous advantages and few downsides for clever, well-heeled miscreants.

### **It is extremely difficult to detect.**

TBML uses standard commercial trade procedures as camouflage. It is hidden in plain sight. Since several trillion dollars change hands every year via legitimate international commercial transactions, it is fairly easy to conceal a few billion in the crowd.

### **If caught, TBML perpetrators have numerous plausible explanations.**

The international trading system is replete with simple errors, often amounting to millions of dollars. If detected, TBML participants can often characterize their transactions as bookkeeping or administrative errors, suggesting incompetence rather than malevolence. This is highly credible, even outside Washington. If pressed, they can also claim tax or currency control avoidance motives that are routine

in international commerce.

### **Huge amounts of money can be transferred quickly without much chance of theft or interdiction.**

Not surprisingly, one of the largest hazards of many money laundering schemes is not law enforcement, but theft by insiders. It is unwise to report such pilfering to the authorities. Strong-arm tactics to recover the swag are both messy and unlikely to produce much Return of Investment (ROI). TBML, by contrast, is relatively safe in that it uses reputable institutions to transfer funds and even Wall Street bankers are unlikely to hot-wire legitimate accounts.

### **Unlike some other types of money laundering, few people are required to make the system work or even be aware of the plot's existence.**

Some money-laundering schemes rely upon literal armies of intermediaries to operate. This is especially true for such methods as the Black Market Peso Exchange (BMPE), which employs battalions of "Smurfs", or even the low-tech "mules", who carry physical banknotes across borders. TBML needs only a few sophisticated personnel and can be operated in an open office environment where, like Bernie Madoff's sons, everyone can see what the perpetrator is doing without understanding what it portends.

**Laws and enforcement in most jurisdictions are inadequate to prosecute TBML operators even if detected.** Making a money-laundering case against TBML operations is very difficult even for experienced prosecutors in developed countries. Given the complexities of international commerce and the defenses which can be raised, there have been very few convictions. While not bulletproof, TBML operators are much less likely to be making license plates than street thugs. Although money laundering charges are fairly common, this is a definitional crime. In the case of TBML, there are hundreds of plausible reasons why a legitimate transaction may be structured in entirely legal ways to avoid taxes, take advantage of currency fluctuations, or even routine arbitrage. Unless prosecutors can prove *Malum in se*, even the most bizarre TBML scheme can often skate. Given these advantages, why aren't more malefactors using this method to move ill-gotten gains?

Who says they aren't? There are no reliable statistics on the ubiquity of TBML, and given its relative invisibility, it is unlikely there will ever be any. Hundreds of TBML schemes are active as you read this, many of which have been in operation for years.

*(Continued on Page 5)*

TBML (*Cont. from 4*)

There are, however, a few downsides to this method of money laundering that dissuade many schemers.

1) TBML requires a high degree of technical expertise in the logistics and financing of international commercial transactions. This is not a method that can be successful for Friday-night crooks. To work, a TBML operation must closely resemble a legitimate transaction so as not to attract the attention of banks, Customs or tax authorities, national security agencies, or even their unwitting accomplices in the private sector. These entities have numerous trip-wires which can be triggered if a transaction departs significantly from the norm. Like a Mississippi River pilot, good TBML operators know these reefs and shoals well, but amateurs are often brought low by their ignorance.

2) By its nature, TBML is most useful when large amounts of funds need to be moved. Although it is possible to structure a transaction of only a few thousand dollars, it is just as easy, and often more plausible, to transfer hundreds of thousands or even millions of dollars at a time. Many money laundering operations, such as hawalas, rely upon small transactions unsuitable for TBML in most instances. A successful TBML operation also needs credibility, often developed over many years, to move substantial sums. Patience is often a forgotten virtue for money launderers; TBML is a long-term business.

Due to the fact that these disadvantages deter most putative

TBML users, specialists control most of this industry. Like BMPE brokers, TBML operators often have no personal stake in either the goods being shipped or the funds transferred. They are paid on a commission or flat-rate basis. Their job is to structure the entire transaction, from routing the cargo to arranging financing and payment flows. For experienced professionals, this can be done from anywhere in the world, using a simple laptop. Even shipping documents can be created electronically that will pass in all but the most rigorous examination. The most experienced TBML brokers will be able to set up shell companies in distant lands, arrange for Letters of Credit, book ocean transit, and prepare shipping documents with a few keystrokes.

Although there are dozens of variations to TBML schemes, most rely upon disguising a money laundering operation behind a façade of a legitimate commercial transaction. This can be as simple as under-or over-invoicing a shipment (depending upon which direction the flow of money is to be diverted), to more elaborate scenarios involving interdiction of shipments by intermediate consignees, redirecting the goods to higher-margin markets.

TBML plots generally abjure shady financing deals such as those involving Panamanian banks, preferring established financial institutions in New York, London, Frankfurt, Paris, or Tokyo to handle transfers. To do this, TBML brokers need to carefully disguise

the transactions as being benign so as not to attract the attention of either the banks or their regulators. It is the ironic truth that bureaucrats monitoring large, respected banks tend to look for missteps by the banks themselves rather than their customers, while law enforcement agencies are more interested in the clientele of financial institutions in dodgy countries, often assuming that the bank is crooked in any event. Using a large bank, then, can often protect a TBML operator because the inspectors simply have different assumptions and targets.

Some TBML schemes are so polished that they use not only premier banks, but Fortune 500 companies as cover. This is especially the case where product diversion is the vector. Here, the TBML facilitator may establish phony offshore companies to place orders for legitimate goods, allegedly for distribution abroad. Depending upon currency valuations and similar considerations, the goods are actually shipped to higher-priced markets in a classic arbitrage. Even when the transaction does not garner much profit per se, it can generate a legitimate paper trail, which is almost impossible for the victim (i.e. the duped supplier), the banks, or regulators to even discover, much less understand.

Other variations include the use of legitimate charities, especially those which provide disaster relief. Here, the TBML operators act as brokers for charities to dispose of surplus donations, returning a portion of

*(Continued on Page 21)*

# Protecting Critical Infrastructure through Effective Money Laundering Enforcement

by John W. Bagby

Professor of Information Sciences and Technology  
The Pennsylvania State University

In the protection of critical infrastructure, law enforcement and counter-terrorism must increasingly focus on tracing payments to discover money laundering schemes — a wide variety of deceptive transaction practices intended to create the illusion of legitimate dealings that disguise the origin and movement of proceeds from unlawful activities or to finance terrorism. Money laundering techniques are most successful when there are plausible explanations for cash flows and cash reserves. In the law enforcement vernacular, the phrase “follow the money” suggests that tracking the trail of money movements helps to discover terrorists, criminal masterminds, and many intermediary accomplices. Modern anti-money laundering (AML) forensics deploys a form of social network analysis wherein the nodes are institutions or money-laundering participants and the links are flows of information, currency, electronic money, or other forms of value.

## Traditional Money Laundering

Money laundering is both a literal and metaphoric reference to “cleansing” the appearance of money “sullied” by criminal

activities. In the 1920s and 1930s gangster era, a large, recurring and potentially incriminating cash flow of coins accompanied “the numbers racket,” illegal, small stakes gambling. Mobsters owned coin-operated laundries that provided plausible excuses for handling coins and currency. Routing these wagering proceeds through the laundries helped to cover up the criminal payments making them practically untraceable. Indeed, unregulated gambling today remains a substantial money laundering “front.” Money laundering may have existed for over 4000 years, having originated to hide both legitimate and illegitimate earnings from oppressive government taxation or unfair confiscation. Money laundering has also likely been a component of securities fraud, mail and wire fraud, and the financing of terrorism that threatens all critical infrastructures. Money laundering is a classic component crime in racketeering because both the underlying crimes for which money is laundered and the money laundering itself are repetitive and similar. Racketeering is a compound crime illegal under state and federal law.<sup>1</sup>

## Money Laundering Architectures

While money laundering methods are varied, many are well-known and they evolve after exposure by successful enforcement. Detection often remains difficult so enforcement can be costly. Launderers prefer methods with few official records so their payments are not easily traceable. “Cash is king,” so transfer of currency to launder money is preferable to payment by checks, wire transfers, or credit cards because cash transfer can be accomplished without official recordkeeping, thereby providing cover for transactions. Of course, there are natural limits on cash movements; small bills can impose staggering practical impediments to tracing even with the use of marked currency or the verification of serial numbers. Furthermore, innovations in currency designs, such as UPC codes, imbedded rfid’s, and stagenographic techniques, will further challenge money launderers’ reliance on currencies.

Under one general model, money laundering has three basic stages: (1) placement, (2) layering, and (3) integration.<sup>2</sup> Placement (promotion)

*(Continued on Page 7)*

<sup>1</sup> 18 U.S.C. §§1961–1968 (2008).

<sup>2</sup> Report To Congress, In Accordance with §356(C) Of The USA Patriot Act, Secretary of the Treasury, Board of Governors of the Federal Reserve System, Securities and Exchange Commission, Dec. 31, 2002 at 7, accessible at [http://www.fincen.gov/news\\_room/rp/files/356report.pdf](http://www.fincen.gov/news_room/rp/files/356report.pdf).

## Enforcement (Cont. from 6)

refers to the stage when laundered funds are initially made less suspicious, more convenient and first fall under the financial system's control after initial acquisition. This is the first step to hide funds following their use in an illegal activity. Layering, a concealment process of movement, separates the proceeds from their illegal source using multiple, complex financial transactions (e.g., wire transfers, monetary instruments, asset purchases/sales). Layering further obscures the links between placement and integration, sometimes by altering the size of the lump sum to obfuscate the audit trail. Integration describes when the funds are spent or invested through reentry into the legitimate economy. These three steps describe only a basic model. Cat and mouse changes to money laundering architectures induced by enforcement enhancements are well-known, ultimately diversifying and increasing the complexity of money laundering schemes. Like terrorism threats, architecture evolution is inevitable as creative money launderers seek to avoid detection or eventually exhaust investigator resolve and enforcement resources.

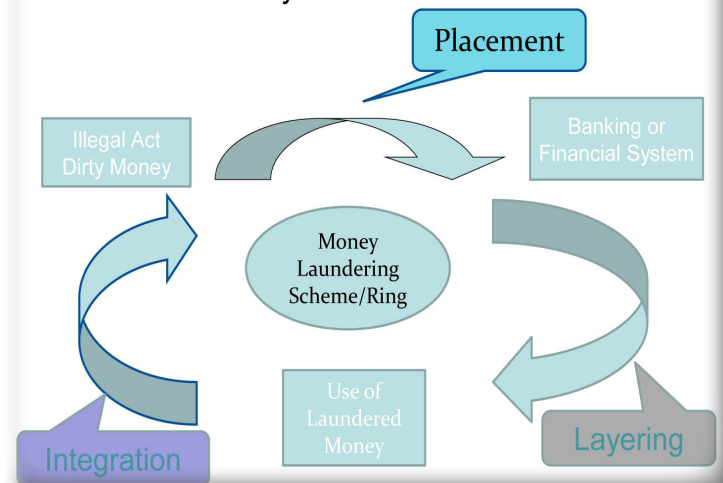
"Fronts" are useful to money launderers; these are apparently respectable businesses that cover up illegal activities. Increasingly, sham transactions and inter-corporate transfers among complex or nested shell corporations are used. In addition, phony charities or trusts,

and investment accounts are chosen layer payment flows. Bank or trading accounts located offshore or in tax havens provide additional cover when local authorities in some foreign nations fail to cooperate.

### The Objects Cleansed

Increasingly, other financial services can be deployed to transfer wealth such as fictitious trading in securities or commodities, use of money transmitters, remittances to developing countries handled through wire transferors, and currency exchange firms. The Federal Reserve Board is continually expanding the list of financial service firms that could assist in money laundering reporting, detection, and enforcement, including mortgage lenders, pay day lenders, finance companies, mortgage brokers, non-bank lenders, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors, and other financial

Figure 1: Flow of Laundered Money



advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that are not required to register with the SEC.<sup>3</sup>

Money laundering does not rely solely on the physical movement of currency or the traditional paper-based or electronic transfer of funds through commercial banking networks. Scrip, virtual money, goods, or even services may constitute the flow of "value" to or from the criminal perpetrator or terrorist back to the illegal organization sponsoring or assisting in the illegal activity. Indeed, diamonds, gold, or other precious and valuable assets might be used. Consider how counter-trade is a particularly insidious money laundering method because of the appearance of humanitarian motives.<sup>4</sup>

(Continued on Page 8)

<sup>3</sup> See 65 Fed. Reg. 33646, 33647 (May 24, 2000).

<sup>4</sup> Bagby, John W. & F. William McCarty, *The Legal and Regulatory Environment of E-Business: Law for the Converging Economy*, (West, 2003) at 346-47.

## Enforcement (Cont. from 7)

### Activities Reliant on Money Laundering

Law enforcement and counter-terrorism forces now focus increased attention on money laundering presuming that payment flows are indispensable to underground economic activities and unlawful activities such as drug trade, bootlegging, gambling, organized crime, weapons trade, and smuggling. AML laws help identify criminals, reveal accomplices, accessories, and co-conspirators who might testify against others in the money laundering supply chain, recover money, assets or freeze accounts, and help deter additional criminal activity by reducing the incentive to spend criminal proceeds.

### The Money Laundering Offense

In the United States, the money laundering offense was clarified and AML enforcement powers extended significantly by the Money Laundering Control Act of 1986. This law criminalizes some forms of money laundering when the proceeds of certain listed crimes are used in a financial transaction. The elements of federal money laundering violation include a (i) financial, (ii) transaction, (iii) involving proceeds from any specified unlawful activity,<sup>5</sup> (iv)

scienter, and (v) this affects interstate commerce. There are separate money laundering conspiracy provisions.<sup>6</sup> The money laundering penalties can be harsh: 20 years in prison for each transaction by convicted individuals. For each money laundering transaction, businesses can be fined up to the greater of twice the transaction's value or \$500,000. Property is subject to forfeiture if acquired, involved, or traced to the transaction. Banks can lose their charters. Bank employees face the same individual penalties and can be debarred from banking industry employment.

Contemporary Supreme Court cases interpreting money laundering have impacted AML enforcement in two ways: easing and impeding the burden of proof. Two companion 2005 cases support AML enforcement by relaxing proof of any overt act in the conspiracy offense.<sup>7</sup> However, two 2008 cases focus on the proceeds and scienter elements. First, actual profits, not just gross receipts, of an illegal activity, constitute proceeds. Thus, a successful money laundering conviction requires AML enforcement to uncover bookkeeping evidence of the criminal activity; in this case, the difference between the gross receipts or bets collected in an illegal lottery ("bolita") and the expenses

of the illegal gambling enterprise.<sup>8</sup> Acquiring accurate accounting records for illegal gambling can be elusive. Second, scienter as to the concealment of proceeds has also become a more stringent proof requirement. Prosecutors did not prove that the considerable cash concealed in a defendant's car was intentionally portrayed as legitimate wealth. The layering step of money laundering traditionally deceives as to how it was derived from an underlying illegal transaction. Proof that proceeds were simply hidden during transportation is not enough. Instead, prosecutors must show that the nature, location, source, ownership, or control of the proceeds was hidden.<sup>9</sup>

### Money Laundering Enforcement

The classic AML forensics method is used to examine the finances of suspects for irregular receipts or spending beyond that suspect's regular transaction type, transaction volume, or their earnings. This enables tracking back through payers and recipients of suspicious, repetitive, or large transactions for further investigation. AML forensics following a completed crime are used to discover perpetrators and accomplices ex post. Paradoxically, AML intended

*(Continued on Page 22)*

<sup>5</sup> These are predicate offenses that include a wide range of state and federal offenses. Nearly every predicate offense under RICO is included.

<sup>6</sup> 18 U.S.C. §1956 (h) (2008).

<sup>7</sup> *Whitfield v. United States*, 542 U.S. 918 (2005), *Hall v. United States*, 542 U.S. 918 (2005).

<sup>8</sup> *United States v. Santos & Diaz*; 553 U.S. --- (2008).

<sup>9</sup> *Cuellar v. United States*, 553 U.S. ---; 128 S. Ct. 1994 (2008).

<sup>10</sup> Gouvin, Eric J., *Bringing Out The Big Guns: The USA PATRIOT Act, Money Laundering, And The War On Terrorism*, 55 *Baylor L. Rev.* 101 (2003).

## Promoting Cyber Resilience through Coalitions like ChicagoFIRST

by Brian Tishuk\*, Executive Director, ChicagoFIRST\*\*

Cyber resilience is a hot topic today and deservedly so. However, much of the attention, from both public agencies and private companies, focuses on how individual organizations can protect themselves from cyber attacks, rather than on developing a response framework that incorporates broader information sharing, both internally and externally.

Consequently, protective efforts tend to be both confined within information technology (IT) departments and to be limited to technological solutions. A broader risk management approach must be taken to promote cyber resilience. The Banking and Finance Sector is a leader in this area, and one of its current tabletop exercise programs enhances cyber resilience in several ways, all of which can be emulated by financial and non-financial firms alike.

### ChicagoFIRST Cyber Resilience Tabletop Exercise

The use of the Internet to commit fraud against financial firms and their customers has been well documented. Less well established and understood is the ability of criminals to hinder financial transactions through Internet attacks. This has business continuity, as well as IT, implications.

Moreover, cyber resilience should include a local response component, even though the issue is seen as national in scope. Finally, firms should establish protocols for sharing cyber attack information internally with other departments and externally with other firms and with trusted law enforcement representatives.

ChicagoFIRST, a coalition of primarily financial institutions in Chicago, in coordination with the U.S. Department of Homeland Security (DHS), held a cyber tabletop exercise in 2008 designed to address all three of these issues. The event raised cyber threat awareness among business continuity and disaster recovery executives and managers, and included participants representing the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), DHS, and the private sector.

Participants examined existing and necessary information sharing and incident response processes in the event of a coordinated cyber attack. Speakers and panelists reviewed recent cyber threats and the potential impact to an organization's IT systems and business operations, stimulating discussion during the exercise on how to effectively manage these events from a business, as well as a technical, perspective.

### Lessons Learned

The scenario presented to exercise participants detailed a cyber attack that resulted in a self-propagating virus spreading across company networks, leading a steadily increasing number of operational files to become encrypted and, thereby, inaccessible, to the firm. These issues were further complicated by an extortion demand and the execution of a successful denial-of-service attack.

### *Information Sharing Processes and Procedures*

Firms would benefit from a more formalized process. For instance, during a coordinated cyber incident, the informal trusted member of one organization may be unavailable, stopping information flow due to the lack of a formalized process with clearly defined roles.

Thresholds to determine when to share information, the type of information to share, and with whom to share the information need to be established. For example, during the exercise, many participants discussed and questioned the threshold that necessitated law enforcement involvement — and the opinions differed.

Active use of an information sharing

*(Continued on Page 10)*

## Cyber Resilience (*Cont. from 9*)

collaboration tool, such as the ChicagoFIRST message boards or Financial Services Information Sharing and Analysis Center portal, can provide an additional means of sharing efficiently and effectively the most up-to-date information relative to a potential cyber threat or during a crisis.

There is often a significant lag time or information gap between technical staff and leadership within an organization. A similar gap tends to exist between technical and business continuity staffs.

Some firms are reluctant to share with external sources the fact that a cyber security problem has arisen, whether with the various financial information sharing organizations or with law enforcement. In fact, some firms reported that they would check these organizations to see if other firms have reported similar problems, but they would not report the situation themselves.

On the other hand, these firms are willing to reach out to trusted individuals about their situation. Therefore, any internal processes should encourage information sharing earlier in the process, particularly with information sharing organizations and law enforcement.

### *Cyber Education and Awareness*

Cyber education and training are essential components to an effective cyber detection, response, and recovery plan. Education and training allow organizations to better understand the need to

safeguard systems, infrastructures, and employees against the evolving cyber threat.

In addition to presentations and training events, continued participation in cyber exercises provides educational components that can be incorporated through hands-on learning and decision making that is free of real world consequences. Exercises provide participants the vital exposure to the cyber threat environment and allow them to stay aware of the ever increasing threat to their organizations.

### *Cyber Incident Communications Plan*

When a cyber incident occurs, pre-established communication plans make it possible to exchange information within organizations, between organizational entities, and across public and private sectors, to include the media. Those organizations which lacked a communications plan spent a great deal of time during the exercise trying to discern at what stage in the crisis they would issue certain communications to their customers, internal employees, external sector partners, government, and the media.

An established communications plan affords organizations a more active role in shaping media and public perception by ensuring that well coordinated communications are issued during a crisis.

### **ChicagoFIRST and Similar Coalitions**

By way of background, ChicagoFIRST is a nonprofit association of more than two dozen firms in the Chicagoland area, most of which are financial institutions. Formed in 2003, ChicagoFIRST fosters collaboration among its private sector members and between those members and the public sector on issues affecting resilience.

ChicagoFIRST is funded and run by its private sector members. As a public/private partnership, it interacts regularly with the public sector, including the City of Chicago, the State of Illinois, and the U.S. Department of the Treasury and DHS. Areas of focus include business continuity, pandemic planning, and physical security, as well as cyber resilience.

Within the financial sector, many other similar "FIRST" organizations have formed, leading ChicagoFIRST, in 2005, to establish the Regional Partnership Council (RPC*first*) to foster the sharing of lessons learned and best practices among these entities. Currently, more than 20 such organizations operate in nearly 20 states. Each of them is a member of RPC*first*.

### **A Replicable Cyber Tabletop**

Following the successful 2008 cyber tabletop, ChicagoFIRST, as the head of RPC*first*, determined that other coalitions would benefit from holding similar events tailored

*(Continued on Page 11)*

## Cyber Resilience (*Cont. from 10*)

to their needs and circumstances. ChicagoFIRST and DHS have thus been collaborating to produce a cyber “tabletop-in-a-box” product that could be replicated by RPC*first* members across the country.

The product was piloted in 2009 with two RPC*first* members. The Bay Area Response Coalition (BARC*first*) tested it in October, while the National Capitol Region coalition (NCR*first*) implemented a revised version in December. The tabletop product is scalable and flexible, to the point of being amenable to largely private or largely public participants.

In 2010, the tabletop product will be completed and provided to all RPC*first* members. Subsequent experience will lead to refinements, so that a final product will be available by the end of the year. It may then also be used not only by coalitions, but by the individual members of any given coalition. In fact, the product could benefit any partnership or any company or public agency.

### Other ChicagoFIRST Activities

In 2009, ChicagoFIRST and DHS conducted the first urban-based Regional Resiliency Assessment Program (RRAP), focusing on the Chicago financial district. The effort amassed data on the security measures of buildings, power, water, and telecommunications, all of which are vital to the operations of financial institutions. A tabletop exercise based on the RRAP results will be held in 2010.

Since 2005, ChicagoFIRST has been working with DHS on pandemic preparedness, and, more specifically, the Internet congestion that would occur if an event led a significant number of employees to telecommute. In 2006, ChicagoFIRST members provided data to DHS by zip code as to where critical operations would be conducted if employees were telecommuting. This formed the basis of a 2007 report showing that Internet congestion could threaten critical operations, thus requiring a federal government strategy for mitigating that risk. ChicagoFIRST then worked successfully with congressional leaders to have them solicit a study by the Government Accountability Office (GAO) in 2008, the results of which were released in October 2009. The GAO recommends DHS action, and ChicagoFIRST will follow up with the appropriate agencies.

Given that some of its members have security clearances, ChicagoFIRST is obtaining a seat in the City of Chicago fusion center, which complements its seat in the City’s emergency operations center. The ability to combine access to relevant intelligence and law enforcement personnel with access to first responders will be a model for the Banking and Finance Sector, as well as other firms and sectors.

### Conclusion

Localized public/private partnerships can effectively enhance cyber resilience even though cyber issues are viewed as not tethered to a particular geography, like a flood

or fire. As with all other hazards and emergency events, the solution lies not only in knowing who to call, but also to developing trusted relationships with public and private individuals and entities. Such relationships should be formalized in protocols, and the underlying trust will ensure that calls get answered.

Every firm should develop a relationship with the FBI and/or the USSS. The specific relationship that is formed depends on which is nearby and with which a firm feels comfortable. The FBI operates InfraGard, while the USSS runs the Electronic Crime Task Forces. Both afford the opportunities necessary to form the essential trusted relationships that may become invaluable during a cyber attack, protecting a firm’s reputation, and helping to resolve its cyber problem. In the same vein, physical and cyber security personnel should coordinate more closely as part of a general risk management approach. (In 2009, ChicagoFIRST combined both types of security into a tabletop exercise for these often disparate disciplines.)

Firms participating in operational coalitions like ChicagoFIRST have an advantage over other companies. The relationships already exist or can be formed more easily, because the organization serves as a single point of contact. Sharing information across the private sector and between the private and public sectors remains a key to addressing risk management, and coalitions

*(Continued on Page 23)*

## The FS-ISAC: A Model for Critical Infrastructure Protection through Information Exchange

by Denise Anderson, Vice President, Programs and Services, Financial Services Information Sharing and Analysis Center

On Christmas Day, a Raleigh woman did not realize anything was wrong until she received a phone call from her financial institution informing her that money had been taken from her account. As it turns out, she was not the only victim of 'skimming', the theft of credit or debit card information during a legitimate transaction. Over 300 debit card holders were affected. Officials pointed to a skimming device on a gas pump as the likely culprit. The device, which is put over the card slot, reads and captures the information on the magnetic strip of the debit or credit card and is often used in conjunction with a hidden camera, which captures the cardholder's pin number when he or she enters it. The devices are very hard to detect.

Financial fraud has dominated the news in recent years. In November 2008, 'low-level' cashers used cloned gift and payroll cards at 130 ATMs in 49 cities worldwide to withdraw \$9 million in a 30-minute period. In New York City, in June 2009, law enforcement reported that a criminal gang had stolen \$500,000 from cardholders at several Sovereign Bank branches in Staten Island. The criminals had installed cameras to capture PIN information and had card cloning devices to carry out the scheme. Indeed, a survey by Actimize, a security company, revealed that

financial institutions reported a 70 percent increase in 2008 over 2007 in ATM/debit card fraud.

In August 2009, the Financial Services Information Sharing and Analysis Center (FS-ISAC), along with NACHA (The Electronic Payments Association) and the FBI, posted a joint bulletin outlining criminal activity regarding business accounts that were taken over by cyber criminals. Hundreds of companies have been attacked using



this scheme. One company in Georgia lost \$75,000 and another in Baton Rouge lost almost \$100,000. The FBI has estimated the losses from online fraud involving malware and money mules at almost \$40 million to date.

The FS-ISAC celebrated its tenth anniversary in 2009. It was formed as a result of Presidential Directive-

63 (PD-63), which directed the public and private sectors to form information sharing partnerships to protect critical infrastructures. It was further refined by Homeland Security Presidential Directive-7 (HSPD-7). The organization is a nonprofit private sector initiative and it is designed, developed, and owned by the financial services industry: Banks, Card companies, Payment and Clearing Processors, Brokerage Firms, Insurance companies, and Credit Unions. Its lead government agency is the U.S. Department of Treasury.

Since 1999, the goal of the FS-ISAC has been to share timely, relevant, and actionable information and analysis of physical and cyber security information that can impact the financial services sector. Membership has grown steadily from a small cadre of less than 100 in 2004 to over 4,000 members in 2009.

The FS-ISAC works closely with its partners in the critical infrastructure community, including the Department of Homeland Security, the United States Secret Service, the FBI, other ISACs, and the Partnership for Critical Infrastructure Protection (PCIS), among others, to achieve this goal. The FS-ISAC shares

*(Continued on Page 13)*

## Information Exchange *(Cont. from 12)*

actionable information with the Banking and Finance Sector and the critical infrastructure protection community on issues such as pandemics, natural disasters, terrorist attacks, cyber threats, cyber vulnerabilities, and cyber attacks.

The FS-ISAC maintains a 24 x 7 watch center and offers members a secure portal for sharing information and alerts on physical and cyber threats, and vulnerabilities and incidents. The FS-ISAC also offers members a critical incident notification alert system (CINS), bi-weekly threat calls amongst members with reports from Microsoft during Microsoft patch week and from iDefense, member surveys, industry best practices, industry exercises, listservs for member collaboration, and anonymous information sharing. It also holds crisis management calls and activates incident analysis teams during crises.

The FS-ISAC has several committees devoted to business resiliency, education, threat intelligence, online fraud, and governance as well as special interest groups for the insurance community and the payments community.

In addition, the FS-ISAC holds two three-day conferences for members and industry; one focused on the Banking and Finance Sector and the other for the entire critical infrastructure protection community, as well as webinars and regional seminars. The threat to financial services institutions and their customers from cyber attacks, particularly from phishing attacks

and malware, is very real. The Anti-Phishing Working Group reports that Financial Services continues to be the most targeted industry sector, growing to 92.6% of all attacks. Over 80% of these attacks contain malware.

According to the Kroll Annual Global Fraud Report, the financial services industry was the most targeted sector with losses per company amounting to over \$15 million on average in the past three years. PandaLabs reported that malware to steal personal information for financial gain rose 600% in 2008 with three percent of web users reportedly victims of malware. According to PandaLabs, it receives over 37,000 samples of new viruses, worms, Trojans, and other types of internet threats daily, with Trojans representing 71 percent of the samples.

The FS-ISAC has been at the forefront of a number of these attacks. In August, as mentioned above, the FS-ISAC, NACHA and the FBI issued a joint bulletin on the account hijacking of a corporate customers threat and recommended best practices to combat it. In May 2009, the FS-ISAC, along with the Financial Services Sector Coordinating Council (FSSCC) and the Financial and Banking Information Infrastructure Committee (FBIIC), unveiled a Supply Chain Toolkit with mitigation techniques to protect all phases of the supply chain including procurement, production, and distribution. This toolkit looked at internal software development best practices,

Commercial Off-the-Shelf (COTS) software best practices, and Hardware testing.

In July 2008, the FS-ISAC, in conjunction with the Communications ISAC and the IT ISAC, published a joint-bulletin on the DNS Cache Poisoning Vulnerability with recommendations for mitigation. In March 2009, the FS-ISAC published a Conficker/Downadup cyber threat advisory with notices of signatures, tools, and mitigations and hosted a call with iDefense, the FBI, and the United States Computer Emergency Readiness Team (US-CERT) for the CIP community on the threat.

The FS-ISAC has proven time and time again that information sharing is vital to protecting critical infrastructure. In March 2008, for example, the FS-ISAC, through its partnership with iDefense and from member submissions, discovered that there was going to be a potential escalation at the end of the month of spear phishing Better Business Bureau (BBB) and Internal Revenue Service (IRS) attacks against business customers using financial institution web-based cash management services. These slick attacks appeared as a personal email to financial institution executives notifying them of a BBB complaint against their company. They were asked to click on the complaint, which then downloaded malware to capture personal or financial information. In the case of the IRS, a message

*(Continued on Page 23)*

## Education and Financial Sector Security: Need for a Graduate Course on Terrorist Financing

### Introduction

This article lays down a dire need for a graduate course on terrorist financing as part of the course curricula for national security/homeland security programs across the United States. It also delineates what the content of such a course should be, and describes how graduate students may benefit from taking such a course.

### Existing Graduate Course Curriculums in National Security and a Critical Gap in Security Studies Education

Across the United States, many graduate programs in security studies do not, as of yet, offer a course on terrorist financing as an integral part of the curriculum. While most courses in such programs focus on issues like the radicalization process that leads to terrorist activity; critical infrastructure protection; border protection; law enforcement; intelligence; and other aspects of national/homeland security, they are remiss in not offering instruction to graduate students about how terrorist threats confronting the homeland, the nation, and the world are financed. This is a critical gap in security studies programs that must be addressed. This gap can be suitably filled by introducing a course on terrorist financing as part of the course curriculum in graduate programs in security studies.

The concept of financial security in homeland security practice and study has hitherto revolved around the physical and cyber security of the Banking and Finance Sector. An all-encompassing view of security in this sector must include instruction on terrorist financing and countering the Financing of Terrorism measures. Counter-Terrorist Financing is an integral element of any counterterrorist strategy. It is important that the process of orienting the national security managers of tomorrow towards terrorist financing and its implications on national security be started at the graduate level itself. A course on terrorist financing would do precisely that.

### What are the Contents of a Graduate Course on Terrorist Financing?

Such a course examines the phenomenon of terrorist financing. It takes the student through a blend of the theoretical and practical perspectives on terrorist financing. It offers an overview of terrorist financing methods, including ways in which terrorists raise, store, conceal, and transfer funds. The course explores how terrorist organizations and terrorist networks are trying to adapt their funding strategies to counter-terrorist financing measures at the national, regional, international, and multi-lateral levels. In addition, it focuses on the legal, regulatory, administrative, organizational,

and political responses to terrorist financing, and explores the means by which these could be more effective in light of the evolving threats from terrorist financing. The course also looks into the role of governments, international organizations, and the private sector in countering the financing of terrorism. Non banking informal value transfers like hawala are also discussed. A key aspect of this course relates to how specific terrorist groups and terrorist networks finance terrorist activity. While most open source media accounts as well as the report of the 9/11 Commission mention that the 9/11 attacks were financed by a relatively small sum of approximately half a million dollars, it is important to note that terrorist finances are used not just for perpetrating terrorist attacks, but also include funds spent on radicalization, indoctrination, training, and the establishment and maintenance of terrorist networks. When governments highlight the fact that the assets of a certain terrorist/terrorist network have been seized/frozen and express this as an achievement of deployed counter-terrorism financing measures, they miss the important point that assets freeze is part of the overall strategy to counter the financing of terrorism. This includes, and rightfully so, a well developed financial intelligence system that can trace the flow of money from the source of terrorist

*(Continued on Page 15)*

## Terrorist Financing (Cont. from 14)

funds like legitimate businesses, organized crime, etc., and can follow and track, in meticulous detail, how funds used by terrorists or terrorist networks are transferred, hidden, stored, laundered, and transmitted to the scene of the actual terrorist activity. The course addresses the importance of financial intelligence in the overall countering the financing of terrorism mix. Students, who are our future national security/homeland security managers, need to know that it is only by mapping information about threats emanating from terrorist financing against information about terrorist financing vulnerabilities, that the risks from terrorist financing activity can be determined, and optimal resources allocated to mitigate such risks. Since the banks and financial institutions have information about terrorist financing vulnerabilities, largely by virtue of past experiences of exploitation of their systems by terrorist financiers, and government law enforcement agencies have real time information/intelligence about threats from terrorist financing, it is only natural that public private partnerships are as much the norm in the effective implementation of countering the financing of terrorism measures as they are in ensuring the physical security and the cyber security of the Banking and Finance Sector. The global nature of the international financial system makes it vulnerable to attack by terrorist financiers on a worldwide basis; the concomitant countering the financing of terrorism measures therefore demand bilateral and multilateral

cooperation. Therefore, quite naturally, this course delves into such issues of global compliance and conformance with international standards. Many tend to confuse the phenomenon of money-laundering with terrorist financing activity. While the two have obvious similarities, and terrorists may employ money laundering as part of their efforts to conceal the flows of funds going into terrorist activity, the two practices are distinct. Lessons from anti-money laundering strategies can be used to formulate the strategies to counter terrorist financing, since money laundering as a process is better understood. The course attempts to draw a neat distinction these two activities.

### What Value will the Student See in Such a Course?

Given the title of the course and what they hope to learn, students generally tend to find such courses exciting and interesting. There is also a fallacy amongst students and graduate schools alike that most of the information taught in such a course must be classified and thus inaccessible. Nothing could be further from the truth. Given the reality that we live in the Internet age, where most of the information relevant to the course is accessible online, all the information contained in the readings, and what constitutes the raw material and subject matter for course assignments and presentations, is open-source.

Upon completion of the course, the students will develop a better

understanding of the means that terrorists use to raise, store, transfer, and utilize funds to finance terrorist operations. They will also become acquainted with the policy, legal, administrative, and organizational responses that the international community, national authorities, and financial institutions have developed to tackle the challenge of terrorist financing. Through class readings, case study presentations, and writing assignments, students will hone up their critical thinking, and analytical skills. It is expected that the course will help students, many of whom may be currently working or may wish to work in the counterterrorism arena, to enhance their abilities at developing policies and devising practices to deal with terrorism in general and terrorist financing in particular.

In particular, upon completing their graduate education, students who wish to join the Federal Bureau of Investigation, Immigration and Customs Enforcement, Department of Justice, Financial Crimes Enforcement Network, the Office of Terrorism Finance and Intelligence within the United States Department of Treasury, state and local law enforcement, including city police departments, are likely to find this course useful. Also, students who want to join the Anti-Money Laundering/Countering the Financing of Terrorism Units within the compliance divisions of banks, as well as other financial institutions, would find this course interesting and enlightening.

*(Continued on Page 21)*

## The Association of Certified Anti-Money Laundering Specialists (ACAMS)

The professionals who work in the government, the private sector, and academia to combat money laundering have access to forums and associations to support their goals. One of the leading international professional associations is the Association of Certified Anti-Money Laundering Specialists (ACAMS). Its headquarters are located in Miami, Florida, with a division office also located in Hong Kong. ACAMS Director Gregory Calpakis took the time to explain more about the organization, its mission, and its activities.

In 1989, Alert Global Media began as a trade publication, entitled “Money Laundering Alert.” This publication was created to provide a source for regular updates on money laundering-related news and events. In 2002, based upon a perceived need for a forum that provided education, professional networking, and credentialing for anti-money laundering professionals, Alert Global Media branched out to form ACAMS. The subscribers to the “Money Laundering Alert” formed the core of this new association.

ACAMS is a completely voluntary association from member support. Approximately 50 percent of its members work for financial institutions, 15 percent for various governmental organizations, and the remainder work in associated fields, such as law, accounting, or academia. Calpakis referred to the

former two of the group as “gatekeepers.”

ACAMS focuses its efforts on three goals: helping its members protect the organizations around the world that employ them, advancing member knowledge, and advancing international guidance. The most significant effort is expended on educational efforts, with ACAMS providing an ongoing forum to keep abreast of new developments in the field as well as sponsoring a specific international certification and associated training. ACAMS sponsors the accreditation as a Certified Anti-Money Laundering Specialist (CAMS). ACAMS provides information to guide the development of better policy and works closely with lobbying organizations like the American Banking Association, but does not conduct direct lobbying itself.

The CAMS certification process consists of a 120-question, three and half hour exam. To sit for the exam, a prospective examinee must first possess a certain number of “points,” which are granted based upon years of experience, educational level, and other relevant factors. The idea is to ensure that no one can come in off the street and take the exam without at least some relevant background. ACAMS provides a wide range of study materials and preparatory classes specifically geared towards the exam. The test itself is based in large part on international standards

and laws and regulations with an extraterritorial reach, so that someone who passes it has a skill set applicable anywhere in the world. The test focuses on four basic areas of knowledge: the risk and methods of money laundering, anti-money laundering programs, compliance standards, and investigative techniques. Calpakis believes that this last category is key, because this is how anti-money laundering specialists actually stop, or help stop, money laundering.

The exam is revised every couple of years by a committee of CAMS volunteers selected to represent a wide range of professional perspectives and geographic locations. The exam is intended to reflect some of the concerns that the large financial institutions, where most ACAMS members work, experience on a daily basis. The drafting of the exam questions by the committee is a lengthy process; in addition, the questions are also reviewed by an external team of psychometricians who are responsible for examining the specific wording of each question (Psychometrics is a field, related to educational psychology, concerned with the theory and technique of educational assessment). This specific part of the review process takes over six months. There is a consistent need to produce refined exams with questions and answers that do not confuse or bias test-takers and the need to test on

*(Continued on Page 24)*

## LEGAL INSIGHTS

## New Financial Fraud Enforcement Task Force: An Admirable Goal that will not be Reached without Private Sector Participation

by John J. Byrne, CAMS

Executive Vice President, Association of Certified Anti-Money Laundering Specialists  
and Dennis M. Lormel, President, DML Associates, LLC

There has certainly been broad consensus that at least a large portion of the 2008-2009 economic melt-down can be attributed to financial fraud. The magnitude of the problem was amplified in February 2009, when Dennis Blair, Director of National Intelligence, informed Congress that the financial crisis had become the biggest threat to our national security. While financial crime has existed since the founding of the republic, the methods are more varied, the technology more complicated, and the impact more devastating than ever before. Given this fact, it is essential that a strategy to address this problem be timely, creative, and comprehensive. Unfortunately, while the Obama Administration deserves credit for taking on this pervasive issue, the announced approach to this massive problem is both incomplete and some say doomed to failure. Why?

Based on our experience with the government and the banking industry, success for a goal such as financial fraud enforcement cannot be adequately achieved unless there is recognition by the Federal and

state governments of the need to seek support and expertise from the private sector. Committed industry officials are ready, willing, and able to work in concert with government partners to challenge the status quo. The question is, does the government understand this fact? This review will cover the establishment of the task force, interviews with previous and current government officials on whether success is possible, and recommendations for potential success.

### Background

On Nov. 17 2009, Attorney General Eric Holder, Treasury Secretary Timothy Geithner, Housing and Urban Development (HUD) Secretary Shaun Donovan, and Securities and Exchange Commission (SEC) Chairwoman Mary Schapiro, jointly announced that President Barack Obama had established, by Executive Order 13519, an interagency Financial Fraud Enforcement Task Force “to strengthen efforts to combat financial crime.”<sup>1</sup>

According to the Executive Order, the Department of Justice will lead the task force and the Department of Treasury, HUD, and the SEC will serve on the steering committee. The task force has been given the mission of working in conjunction with other law enforcement agencies, Federal or otherwise, to investigate and prosecute both serious financial crimes and those stemming from the current economic crisis. The task force is also charged with recovering the proceeds of such crime and ensuring the punishment of the perpetrators. This means the task force possesses a wide jurisdiction, as a “serious” financial crime is not defined, but instead consists of a narrow set of authorities. The actual responsibilities of the task force are listed as advising the Attorney General on the investigation and prosecution of cases, recommending ways to increase inter-jurisdictional cooperation, and to coordinate operations between different law enforcement agencies. State and local agencies will be “invited,” but

*(Continued on Page 18)*

<sup>1</sup> President Obama Establishes Interagency Financial Fraud Enforcement Task Force, November 17, 2009, <http://www.justice.gov/opa/pr/2009/November/09-opa-1243.html>.

## Legal Insights (Cont. from 17)

this coordination is not compulsory.

The task force is initially tapping participants from over 25 agencies and plans to “work with state and local partners to investigate and prosecute significant financial crimes; ensure just and effective punishment for those who perpetrate financial crimes; address discrimination in the lending and financial markets; and recover proceeds for victims.” This is termed “outreach” in the Order.

All of these are worthy goals but this is not the first creation of a “task force” to address fraud, therefore, how can the public believe that this will be any different? Another question is where is the outreach to outside experts in the financial sector that have worked their entire careers to pursue fraudsters and assist financial crime victims?

Based on the language of this Executive Order, it seems right to fear that the focus will not include those outside the industry that engage in the prevention of financial crime. Attorney General Holder, at the press conference, made this point:

*We will be relentless in our investigation of corporate and financial wrongdoing, and will not hesitate to bring charges, where appropriate, for criminal misconduct on the part of businesses and business executives. (For more, go to the Treasury website.)*

Similar comments were made by Treasury Secretary Timothy Geithner and other government

officials.

*How can a task force dedicated to fraud be comprehensive, without seeking advice from the men and women in the industry who tackle these crimes every day.*

The answer — it cannot.

### Recommendations for Success

Apart from tapping the expertise of the private sector, the Financial Crime Enforcement Task Force must learn from previous attempts to address major national and international problems such as financial fraud. We spoke to several former government participants in other task forces who pointed to the 2002 “Corporate Fraud Task Force,” also established by Executive Order, which seemed to be at least a qualified success. This task force was formed in response to the massive business frauds we had encountered, including Enron, WorldCom, Adelphia, etc. In the 2002 crisis, the government was better equipped to respond to the crime problem. The investigative initiative was more specifically focused to corporate accounting frauds and misrepresentations. Investigators possessed the requisite skill sets and experience to adequately address the frauds. In addition, the government was able to dedicate adequate resources to conduct investigations. According to one former high-level government official:

*This task force had teeth. A comprehensive strategy was mapped out, indictments occurred sooner*

*rather than later, agents were transferred if they failed, and it was an all out effort.*

The same former official says he is not optimistic that the new task force will succeed. He did say, *if agents are transferred, high level executives are indicted, or one dedicated task force for a specific case staffed with accountants, agents with a finance background, etc., I might be less cynical.*

The proof, according to several interviewed “will definitely not be in indicting more garden variety mortgage fraud cases. They are a dime a dozen.” What these former officials say needs to occur are prosecutions of the more complex cases involving collateralized debt obligations, mortgage backed securities, misrepresentations about valuations, and underwriting fraud. Due to the sophistication of these frauds, it is essential that the government include business experts in the investigative process and planning.

Even with the relative success of earlier task forces, the Justice Department has admitted that those earlier task forces, established in the wake of the Enron and WorldCom corporate accounting scandals, had too narrow of a focus.

Hannah August, a Justice Department spokeswoman said of the new initiative:

*This task force will focus on problems that are more systemic and*

*(Continued on Page 25)*

Workshop on  
Grand Challenges in Modeling, Simulation, and Analysis for Homeland Security  
(MSAHS-2010)

March 17-18, 2010

at  
FDIC L. William Seidman Training Center,  
Arlington, VA

Modeling and simulation is being adapted to a wide variety of applications that impact our daily lives. When dealing with protecting critical infrastructures such as: Energy, Drinking Water/Wastewater, Transportation, Food & Agriculture, or Chemical, it is critical to take into account the multi-events, multi-threats and cascading effects. Addressing such complex threat structure presents a tremendous challenge—modeling and simulation has proven to be a powerful technique for effectively addressing this challenge.

Workshop registration is free. For registration details, to view the agenda, hotel accommodations, and the current version of the workshop announcement, please visit: <https://www.enstg.com/Signup/index.cfm?CFID=192587&CFTOKEN=50132802>

Sponsored by: Department of Homeland Security Science and Technology Directorate (DHS S&T) and George Mason University Center for Infrastructure Protection (CIP)

### Banking Disruptions (Cont. from 3)

country has those institutions and people lose confidence in them (as a result, for example, of periodic crises), depositors who lose their funds (even partially or temporarily) will most likely be disinclined to keep their money in the banking system (if they eventually retrieve it at all). At the early stages of a financial crisis, one may suspect that some re-depositing of funds from weak banks to stronger ones ought to take place. In all likelihood, however, not all funds will be transferred to the stronger bank if depositors believe that even the stronger bank might suffer from the shock and end up closing. In such circumstances, the logical response will be to diversify funds and leave some of them outside the banking system altogether. Banking crises, therefore, can induce a portfolio modification in savings, with funds moved away from banks and into rudimentary forms of “safekeeping,” such as hidden under the mattress or buried in the back yard. When this type of modification occurs, financial intermediation and therefore long-term growth are compromised.

To investigate the extent to which banking crises affect long-term growth, I studied the incidence of bank failures across states in the United States in the aftermath of the Panic of 1893. This panic can be considered an ideal laboratory for studying the long-term consequences of banking crises for two reasons. First, after it occurred, no government intervention took place. This is important because intervention may “contaminate” the results in the sense that it obscures

the consequences of the panic. Second, the panic affected some states, but not others. This is also important because we can use these differences across states to compare long run growth performance between the states that experienced severe crises and states that did not. The results of my investigation indicate that between 1900 and 1930, states that endured the brunt of the crisis grew more slowly than all the other states.

An important implication of my research is that developing and maintaining credible institutions is crucial for avoiding widespread loss of confidence in the banking system, the kind of loss of confidence that so many states in the United States endured at the turn of the twentieth century. It is also important to stress the modifier “credible” because heavy-handed attempts to introduce quick remedies almost always end up aggravating rather than improving the original problem. A historical example of such substandard remedies is the introduction of deposit insurance at the state level between 1907 and 1918. During that period, eight states experimented with insurance schemes, presumably to reduce the number of crises, but all of these schemes were ill designed and ended up encouraging banks to take on more risk. By 1929, all of them had collapsed. ❖

### References

Bernanke, Ben S. (1983). “Nonmonetary Effects of the Financial Crisis in Propagation of

the Great Depression.” *American Economic Review* 73, no. 3: 257–76.

Calomiris, Charles W. (2000). *U.S. Bank Deregulation in Historical Perspective*. Cambridge and New York: Cambridge University Press.

Friedman, Milton, and Anna J. Schwartz. (1963). *A Monetary History of the United States, 1867–1960*. Princeton: Princeton University Press.

Ramirez, Carlos D. (2009). “Bank Fragility, ‘Money under the Mattress,’ and Long-Run Growth: U.S. Evidence from the ‘Perfect’ Panic of 1893.” *Journal of Banking and Finance* 33, no. 12 (December): 2185–2198.

TBML (*Cont. from 5*)

the proceeds (or substitute goods) to the charity. This scheme is often used to arbitrage donated pharmaceuticals, where profits can be immense. One fillip to this scheme is the “salting” of returned goods with generics which can further magnify profits.

Putting aside the “salting” technique, which necessarily involves at least fraud, most TBML operators try to stay as far within the law as possible. If one is transporting narcotics on an Interstate highway, it is prudent to stay within the speed limit and to check for burnt-out brake lights. Similarly, TBML brokers are careful to comply with all regulations that they possibly can so as to avoid suspicion. This usually requires years of experience with legitimate commerce, yet another reason the fraternity of top-flight TBML brokers is so small. When they must violate the law due to the nature of the transaction itself, they usually do so in a way which is least likely to be detected. For example, experienced TBML brokers know it is far more common for imports to be examined at the dock than exports. A false export declaration is much less likely to be questioned than a spurious import declaration. There are hundreds of tricks such as this which are routinely employed to cover the illicit activity.

Governments around the world have hired thousands of investigators to combat money laundering. The measures of their success are purely anecdotal. No one has the slightest idea of how much money is successfully laundered by

any method, but it is beyond debate that TBML is one of the apex fruits in this milieu. Since it is so difficult to detect and prosecute, investigators usually spend their efforts on easier cases, especially those cases more convivial to photostops of shrink-wrapped currency bricks.

To combat TBML, investigators must overcome their reluctance to cooperate with the private sector in examining commercial transactions. For their part, multinational companies must understand that they are often acting as laundromats for criminal and even terrorist organizations. It is much easier for a company to monitor its own shipments than for law enforcement to do so. Companies must be able to recognize suspicious transactions, and overcome their reluctance to forego apparent profits if the result will be to undermine their international markets. ❖

Terrorist Financing (*Cont. from 15*)

Another highlight of a course such as this is that it would include guest lectures by officials from the government, multilateral institutions, and the private sector, that are tasked with formulating and implementing countering the financing of terrorism measures, and who have first-hand experience in dealing with the problems that confront execution of such measures. Furthermore, by interacting with such experienced professionals, students taking the course can learn more about the career choices that await them.

**Conclusion**

Thus, it is paramount that graduate programs in national/homeland security studies include a mandatory course on terrorist financing. It would not only equip students with a well-rounded and more holistic training background in counterterrorism studies, but could attract a slew of government agencies, and private sector players in the domain and practice of countering the financing of terrorism to the students taking the course. ❖

**Enforcement** (*Cont. from 8*)

to prevent terrorism ex ante examine terrorist financing of speculative future terrorist events.<sup>10</sup> Refinement of AML forensics is likely informed by both techniques.

Banks and most other financial institutions are required to develop AML programs that include: (i) the development of AML policies and procedures, (ii) the designation of an AML compliance officer, (iii) AML training programs, and (iv) independent testing of the AML program's efficacy.<sup>11</sup> Not surprisingly, these are related to the internal control system requirements imposed on publicly-traded companies by the Sarbanes-Oxley Act.<sup>12</sup>

Money laundering enforcement in the United States is largely entrusted to the Justice Department, the Internal Revenue Service, and a Treasury Department bureau, the Financial Crimes Enforcement Network (FinCEN) established in 1990 to prevent corruption of the U.S. financial system. FinCEN is tasked to fight the financial war on terror, combat financial crime, and enforce economic sanctions against rogue nations. Other federal banking and financial market regulators are also involved. Nevertheless, AML relies heavily on private sector assistance, particularly from the financial services industry.

to prevent terrorism ex ante examine terrorist financing of speculative future terrorist events.<sup>10</sup> Refinement of AML forensics is likely informed by both techniques.

Banks and most other financial institutions are required to develop AML programs that include: (i) the development of AML policies and procedures, (ii) the designation of an AML compliance officer, (iii) AML training programs, and (iv) independent testing of the AML program's efficacy.<sup>11</sup> Not surprisingly, these are related to the internal control system requirements imposed on publicly-traded companies by the Sarbanes-Oxley Act.<sup>12</sup>

Money laundering enforcement in the United States is largely entrusted to the Justice Department, the Internal Revenue Service, and a Treasury Department bureau, the Financial Crimes Enforcement Network (FinCEN) established in 1990 to prevent corruption of the U.S. financial system. FinCEN is tasked to fight the financial war on terror, combat financial crime, and enforce economic sanctions against rogue nations. Other federal banking and financial market regulators are also involved. Nevertheless, AML relies heavily on private sector assistance, particularly from the financial services industry.

for the transaction after examining the available facts, including the background and possible purpose of the transaction."<sup>15</sup>

**Epilogue**

Successful AML to combat terrorism requires cooperation from banks as well as "underground," remittance systems and money handlers (Hawalas, Hundi, Chit) employed to skirt official exchange rates, taxation, and avoid the paper trail of transactions. Money laundering involves architecture innovations requiring constant vigilance. ❖

<sup>11</sup> See generally, Lormel, Dennis M., *Terrorist Financing: Balancing the Benefits and Burdens of Reporting Requirements*, Feb. 16, 2009; *Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*, Organisation For Economic Co-Operation And Development (2009); *Money Laundering and Terrorist Financing in the Securities Sector*, Financial Action Task Force, October 2009.

<sup>12</sup> 15 U.S.C. §7262 (2008).

<sup>13</sup> 31 U.S.C. §§5311-5330, 12 U.S.C. §§1818(s), §1829(b), & §§1951-1959.

<sup>14</sup> See e.g., 31 CFR §103.18.

<sup>15</sup> 12 C.F.R §21.11.

## Cyber Resilience (Cont. from 11)

offer extensive advantages. ❖

*\*Brian S. Tishuk joined ChicagoFIRST in February 2004 as its first Executive Director. Prior to that, Tishuk enjoyed a career at the United States Treasury Department (Treasury) during which he addressed a vast array of public policy issues affecting financial institutions. Tishuk has an undergraduate degree from Lawrence University in Appleton, Wisconsin; a master's degree in public policy from the University of Michigan; and a law degree from Georgetown University.*

### Contact Information:

ChicagoFIRST  
353 North Clark Street  
5th Floor  
Chicago, IL 60654  
[www.chicagofirst.org](http://www.chicagofirst.org)  
[brian.tishuk@chicagofirst.org](mailto:brian.tishuk@chicagofirst.org)



Brian Tishuk, Executive Director,  
ChicagoFIRST

*\*\*ChicagoFIRST was formed in July 2003 by Chicago-area financial organizations and seeks to enhance the resilience of the Chicago financial community and critical infrastructure overall. It does this by establishing relationships between its members and all levels of government, and by providing a means by which the critical private firms can coordinate with respect to homeland security and emergency management issues. Additional information can be found at [www.chicagofirst.org](http://www.chicagofirst.org).*

## Information Exchange (Cont. from 13)

appeared half-way through indicating that the document was not fully loaded, leading the executive to double click to reload msword.exe. The threat was discussed at both the FS-ISAC bi-weekly threat call and at a special member call where threat and mitigation/customer education recommendations were discussed. Over 20,000 spear phishing attacks occurred of which 2,000 were successful. FS-ISAC member losses were minimal as a result of the information shared.

As the future threat landscape continues to evolve, the role of the FS-ISAC in protecting the financial services sector and other critical infrastructure sectors is becoming increasingly important. The FS-ISAC regularly engages with stakeholders in the critical infrastructure community to enhance information sharing and promote risk mitigation. In 2010, the FS-ISAC will establish a partnership for information sharing with US-CERT and the Defense Industrial Base (DIB) that will most likely serve as a model for cross-sector information sharing. It is also exploring, along with other sectors, the creation of a joint coordination center for cyber security and the publication of a global plan for infrastructure protection.

The increasing reliance on cyber and the increasingly apparent interdependencies amongst critical infrastructure sectors shows that those in the CIP community need to be ever vigilant to protect our countries and our world from man-made or natural harm. The FS-ISAC aims to continue to serve its members and ultimately, the nation and the world, with information and analysis that will allow stakeholders to mitigate risk and remain resilient. ❖

For more information on the FS-ISAC, please visit [www.fsisac.com](http://www.fsisac.com).

*ACAMS (Cont. from 16)*

the latest set of international material, which can change at any time. A set of exam preparation materials and course curricula are prepared in tandem with the test itself by a separate committee of members. Everyone who performs this work does so without compensation and has their normal work responsibilities to manage as well.

When asked about current and future trends in money laundering, Calpakis said that he believes money laundering continues to be a serious challenge. In fact, despite well-financed enforcement efforts in many regions of the world, countries continue to be vulnerable to money laundering. The United States, for example, possesses one of the biggest problems with money laundering. Despite its well-developed economy, strict laws, and enforcement mechanisms. Different parts of the world experience different aspects of the problem, be it drug-related money laundering, laundering related to white collar crime, or that related to governmental corruption. Money laundering is the inevitable consequence of a financial system. Calpakis is seeing a shift in the way anti-money laundering efforts work. Large financial institutions are breaking down silos between units designed to prevent or attack different financial crimes and placing the entire team in one division. This increases the potential for collaboration and cooperation between specialists, which in turn allows for the gathering and analysis of useful data. New technological

developments do make it easier to launder money, but they also make it easier to combat money laundering. It is becoming easier to access and monitor data and systems, which is key in a line of business where the customer and their line of business is always growing and changing.

What is Calpakis's advice to the aspiring anti-money laundering specialist? Get trained and network. After all, these two key activities are why ACAMS exists in the first place. In addition, many intelligent people are thinking about this. Why reinvent the wheel? Ask what is going on and what the best practices are around the world. Work with other people, because this is a problem that no one person can approach, let alone solve, on their own. Networking is not just about career advancement, it is also about collaboration. The field changes very quickly and you cannot fight today's war with yesterday's weapons. An anti-money laundering specialist's most important weapons are their knowledge and their relationships.



## Legal Insights (Cont. from 18)

*interlocking, like fraud and other crimes related to [the Troubled Asset Relief Program].*

Current government officials involved with the new task force was designed around the intelligence function. Each involved agency has been charged with collecting and sharing intelligence across agency lines. As an example, the Federal Bureau of Investigation's Financial Crimes Section stood up a Financial Intelligence Center to exchange intelligence with the other member agencies. Field operations will be driven by development of actionable financial intelligence. This is where the Financial Fraud Enforcement Task Force is flawed.

Although the agencies involved in the task force possess considerable financial intelligence, it is nowhere near as robust as it could be if financial institutions were included in the financial intelligence collection and sharing initiative. Financial institutions possess a wealth of financial intelligence information, far exceeding the government. The government and the Banking and Finance Sector should be brainstorming on how financial intelligence from the financial sector could be shared with the government in consideration of

bank secrecy and privacy restrictions.

A potential impediment to the success of the Financial Fraud Enforcement Task Force is the government's capacity to adequately address the magnitude and complexity of the crime problem. The first question is the adequacy of investigative resources. Do the various agencies and state and local investigative agencies have the number of investigators dedicated to adequately address the crime problem? Quite frankly, this is doubtful. In addition, do the investigative resources dedicated to the crime problem possess the necessary experience and understanding of sophisticated financial mechanisms used to facilitate the various fraud schemes? Again, this is questionable.

To overcome these potential impediments, the government should partner with the Banking and Finance Sector. The investigative and compliance resources of financial institutions should be used as force multipliers to overcome potential impediments. They should be used to provide investigative support and to unravel the complexity of the different frauds committed.

At the policy level, senior financial services executives should be sitting at the table with senior government officials addressing policy issues such as sharing financial institution financial intelligence in conformance with bank secrecy and privacy considerations. At the operational level, the investigative and compliance resources of financial institutions should be working side by side with operational government investigators to address and diminish the crime problem.

As we noted at the outset, the Obama Administration deserves credit for confronting this most serious crime issue with an Executive Order-level initiative. However, it is time to do it right and to truly partner with the private sector. ❖

The Center for Infrastructure Protection works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:  
<http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1>