

*The Changing Nature and Growing Threat  
Of Financial Crime*

By:

Kevin R. Brock  
Dennis M. Lormel  
Patrick O'Brien  
Chris Swecker

**August 2009**

## **The Changing Nature and Growing Threat of Financial Crime**

Daily headlines over the past several months describe a level of national and global economic turmoil not seen in most Americans' lifetimes. At this point there are more questions than answers about the source of this sudden and dramatic upheaval, but it now seems clear that arrogance, greed, and criminal fraud – particularly in the mortgage and securitized product arenas - all contributed in a significant way to destabilizing our economy. What's most disturbing is that, despite recognizable indicators, almost no one saw this coming.

The response to this crisis has included actions by the government to inject over a trillion dollars into the private sector in an effort to stimulate restorative spending and credit flows as well as shore up leading financial and industrial companies. At the same time, there is a strong possibility that the government may significantly expand spending on health care as well. And so, on the heels of manipulation and criminality that helped contribute to current difficulties, we can now anticipate an unprecedented follow-on field of opportunity for fraudsters and other financial criminals. Some experts have conservatively estimated that three percent of all monies injected into the private sector as part of the various spending initiatives will be lost to fraud.<sup>1</sup>

Suddenly, the FBI finds itself with a dramatically evolved mission in the area of financial crimes and a new imperative to help protect the nation's critical, and fragile, financial sector by predicting emerging systemic criminal threats and enhancing opportunities to prevent serious financial crimes.

With that as a backdrop, this paper will argue that the contemporary convergence of several key factors compels us to think about the nature and threat of financial crime and specifically fraud in new ways. And that the right strategic approach will have to be informed by these new ways of thinking as well. We begin by highlighting three developing realities that are significantly challenging law enforcement's response to this evolving crime problem.

---

<sup>1</sup> In an interview with the Wall Street Journal on March 8, 2009, Earl Devany, Chairman of the Recovery Act Transparency and Accountability Board, referencing an Association of Certified Fraud Examiners annual study, expressed concerns that the percentage of large government outlays lost to fraud could be as much as seven percent.

**1. Fraud is growing and becoming more complex.** On one level the classic scams continue even with devastating effect (Madoff's Ponzi scheme, 2008.) But there are two realities that have combined to make fraud a crisis on a scale not seen before. As the economy has expanded dramatically over the last twenty years, so has fraud. Progressively higher federal prosecution thresholds for fraud, the growing number of FBI open and unaddressed White Collar investigations, and an expanding number of Suspicious Activity Reports verify this trend.<sup>2</sup> And, as noted above, the government is pushing unprecedented amounts of money into the private sector. If history is an indicator, this will be followed by equally unprecedented levels of fraud. But even more troubling is that fraud is growing in complexity due to the development of new, sophisticated financial instruments and the proliferation of digitally networked communications which has enabled rapid trading, investment, and movement of funds and thereby opened greater opportunities for manipulation. The financial sector is continuously evolving due to innovation and emerging technology. And while innovation drives opportunity, it also can leave behind systemic vulnerabilities readily exploited by sophisticated fraudsters, money launderers, and other financial criminals.

In addition, as the economy expanded rapidly over the last two decades, we saw the emergence of large, complex, multi-billion dollar institutional investment entities that have been described as a "shadow economy." They are non-transparent, poorly understood, and relatively unregulated and include massive multi-billion dollar private equity funds, hedge funds, re-insurance companies and pension funds that, when subjected to huge insider-generated fraud losses or reckless management, threaten – as we have seen - the health of the entire U.S. financial system. The recent credit meltdown also has exposed the interdependence of financial institutions globally. Now we see that the failure or financial distress of one institution has a growing and disturbing domino effect on other financial entities worldwide, so much so that "counterparty risk" has emerged as the most significant threat to otherwise healthy financial institutions. Stress caused by fraud, therefore, can now have a magnified impact and so can no longer be viewed in every instance as an individual crime or stand-alone investigation. This underscores the FBI's imperative to develop a sophisticated Financial Crimes strategy that, like the Bureau's National Security program, has a strong predictive and prevention orientation.

**2. Current resources are insufficient to combat the new financial crimes threat.** And they are insufficient not just in number but also the skill sets that are and will be needed to understand the dense financial and cyber operating

---

<sup>2</sup> In February 2009, FinCEN reported that SARs for mortgage fraud alone increased 44% between 2007 and 2008 and have increased steadily every year since 2004.

environment. The regulatory, investigative, and prosecution resources currently dedicated to combating financial crimes when compared to the scale of the problem seem paltry by any reasonable standard. As a logical result, only the most egregious and readily detectable frauds and other crimes are being prioritized and investigated. The risk is that more and more significant fraud, even that which might ultimately pose a systemic threat, will go unprosecuted and even undetected.

Add in the fact that front end vigilance by financial institutions is being eroded and the risk of failed detection increases even more. The crisis in the financial sector has caused those institutions to reduce compliance and internal investigative staff in an effort to trim costs -- precisely when they are most needed.

There is genuine concern that all of these factors, coupled with a perceived lack of accountability<sup>3</sup> associated with large government spending outlays such as the Troubled Asset Relief Program and the Stimulus Package, will soon result in a wave of financial crimes that could overwhelm law enforcement and the regulators.

**3. Economic instability can also be a significant national security issue.** On February 12, 2009, Director of National Intelligence Dennis Blair testified before the Senate Intelligence Committee that the most significant short term threat to national security was the current financial crisis. Clearly, gross economic destabilization can weaken a country's global posture on many levels beginning with the staggering cost to repair damage done. It is also easy to presume that when sizeable damage can be inflicted in our interconnected world by a surprisingly small set of actors engaged in fraudulent and manipulative schemes those actions are not lost on hostile intelligence or terrorist organizations that may be interested in the destabilization of the U.S. economy. In addition, fraud may grow in attractiveness for terrorists and other enemies as a potentially lucrative funding source. Since 9/11, entities like FinCEN and the FBI's TFOS have documented the intersection between terrorist organizations and financial crimes. This has provided new impetus for the counterterrorism community and the financial sector to pursue and share financial crime intelligence and enforcement strategies as a national security issue.

---

<sup>3</sup> At a hearing on July 21, 2009, the House Committee on Oversight and Government Reform chastised the U.S. Treasury Department for lack of transparency based on a report from TARP Special Inspector General Neil Barofsky.

Viewed in the light of the contemporary convergence of these significant environmental factors, fraud vigilance takes on a greater imperative than it has in the past.

### **Emerging Fraud Challenges**

Fraud is as old as money itself and there are tried and true schemes that reliably ensnare people and institutions year after year. But with the rapid expansion of wealth and technology in this country over the past two decades we are seeing some dynamics emerge that are making the battle against fraud much more challenging than it was even just a few years ago. We've highlighted three of the most prominent:

**→ Complex corporations + complex financial instruments = complex financial crime.**

The corporate world of business has changed significantly in recent years. The marketplace is global and companies have evolved intricate networks of interdependency that make it difficult to isolate and contain economic troubles, as we have seen. Suddenly, it seems like everything is "too big to fail." In order to meet capital and credit needs of corporations eager to stay agile and adaptive and to meet the investment demands of an increasingly affluent society, financial institutions have worked to create new and imaginative financial instruments. From credit default swaps, to securitized mortgages, to derivatives, the list of complex structured financial products has grown to where even experts admit a lack of thorough understanding. We have seen a kind of "mathematification" of finance. It used to be that basic math skills were sufficient for success in finance. Not anymore. Over the past 10 years the emergence and application of sophisticated mathematical models have come to permeate every aspect of the finance industry. Today, banks and investment firms are competing for and hiring some of the best engineers, mathematicians, and scientists they can find and applying their knowledge of quantitative methods and advanced mathematics to making money. This has been the enabler behind the growing set of complex instruments that have gained traction in the financial markets in recent times.

Layer in the rapid money movement of a digital economy and the resulting swirl of complicated transactions can provide a safe haven for fraudulent activity that is both hard to detect and hard to unravel if detected. The advent of internet enabled business models for the finance industry has resulted in global transactions at break-neck speeds -- billions of dollars are moved around the world within seconds providing potentially ideal concealment for fraudulent transactions.

The implications of evermore complex instruments and transactions all moving at warp speed are significant. The FBI and the rest of the enforcement and prosecution community are now facing a drastically different "op tempo" in terms of conducting investigations, preserving evidence, and identifying fraudulent transactions and those who commit them. Communicating with and understanding an industry that is leveraging advanced mathematics and science to constantly evolve their landscape of products presents new challenges. The fight against financial crime in this environment will require skill sets and technology tools that currently are not widely possessed by law enforcement or the regulators. Building those skill sets will necessitate an aggressive learning initiative.

**→ An aging population + increased Government health care subsidies = even more health care fraud.**

It may be hard to imagine health care fraud getting worse, but impending circumstances point to exactly that. The FBI and Department of Health and Human Services have a long battle history with this crime problem and some of the most imaginative and effective proactive measures the Bureau has employed against fraudsters have emerged from the health care investigative arena. For years congress has directed resource enhancements to the Bureau to be used exclusively for health care fraud efforts. Yet, despite such focused attention and many solid investigative victories, health care fraud remains a daunting problem. So lucrative is its potential, drug organizations and gangs have ventured in.

Now the demographic "baby boom" bulge that has defined American culture for fifty years has begun Medicare eligibility. Medicare claims, and therefore fraud opportunities, logically will swell accordingly. In addition, there is the possibility that government funded health care insurance may increase substantially in the near future as coverage is extended to a larger segment of society. These factors forebode a perfect storm and giant leap forward in health care fraud. The Obama administration has already signaled it will be seeking increased funding for fraud detection in health care.

**→ The continued migration of fraud to the Internet.**

There is a saying in law enforcement, "If you're a fraudster and you're not on the Internet, you should be sued for malpractice." This cynical message belies a chilling reality about the nature and opportunities for fraud in a digital, networked world. Fraud on the Internet is difficult to prevent, difficult to attribute, and difficult to bring to justice. Fraudsters feel safe there. There is little overhead needed to propagate a scam that can anonymously reach millions of potential victims with the push of a button and net a sizeable return even if only a tiny fraction fall prey. Much of it flies beneath the radar of investigative and prosecution guidelines since, individually, the fraud may be a negligible amount

and victims won't even bother to report it. There are tricky jurisdictional issues in play, particularly when widespread victimization occurs at the digital hands of an overseas subject completely out of reach of U.S. law enforcement. When factoring in identity theft, which is the fuel that feeds a large part of the Internet fraud wildfire, there may be no more pervasive crime problem in America in terms of number of lives affected.

The challenge to law enforcement posed by crime on the Internet is enormous. This new crime environment is fluid and dynamic and the government, generally, is not. Fraudsters rapidly leverage new technology as well as the vulnerabilities of a population that is still getting used to conducting more and more of its life in a digitally networked world. The result is a growing gap between criminal innovation and government response.

### **The Right Strategy**

A good strategy begins with an honest acknowledgement of the realities being encountered. We have pointed out a number of prominent ones:

1. Financial crime is a significant problem with factors emerging and aligning that will probably make it much worse in the years ahead.
  - Fraud is growing and becoming more complex
  - Healthcare fraud is going to increase even more
  - Financial crime is migrating to the difficult operating environment of the Internet
2. Because of our increasingly interconnected world, the effect of economic perfidy and criminality is having greater negative impact on our economy and its stability than in past years and may even have national security ramifications.
3. At this point, the financial crimes enforcement community may not be optimally positioned from a skill or numbers standpoint to meet the challenges of these realities.

By acknowledging these primary realities, we can see some key capabilities and enablers emerge that will be needed in order to combat this important problem. For example,

- Better intelligence
- Better skills
- Better coordination

Accordingly, we believe the right strategy to confront the growing threat and changing nature of Financial Crime should include three pillars, in particular, that would support a clear-eyed way forward:

**1. Become more predictive and anticipatory.** It would be naïve to think that a pervasive crime like fraud could be prevented to a significant extent. But it's not so naïve to believe that with better development and sharing of intelligence, deeper manipulation and exploitation of already collected data coupled with forward leaning analysis, a greater anticipatory posture may be achieved. This might enable more fluid development and allocation of skilled resources that would perhaps blunt the impact of fraud in a given region or on a given sector of society (e.g. seniors) thereby preventing further victimizations. Timely trend analysis on seamlessly shared information plus collected data subjected to the latest techniques of advanced analytics might reveal emerging mortgage fraud indicators in Omaha or new telemarketing offensives in Florida and give early identifiers on the scope and breadth of globally networked fraud ring conspirators.

A key component of this pillar of the strategy is effective **data management and exploitation**. Whether trying to find a needle of evidence in a haystack of seized data in order to convict someone, or identifying a few pertinent dots to be connected among a sea of trillions of dots in order to prevent something bad from happening or getting worse, the ability to exploit and manage data is becoming more and more critical. In this decade alone, the FBI has increased its data holdings beyond what was previously imaginable. *Having access to a set of constantly adjusting and improving advanced data analysis tools should be a top priority for the FBI.* Financial crimes cases are often some of the most record intensive investigations conducted by the Bureau. Suspicious Activity Reports and other available financial institution data sets could yield a wealth of predictive intelligence if better advanced text analytics were applied than currently are today.

There is no reason why the battle against fraud and other financial crimes cannot become more intelligence driven particularly through better exploitation of already collected data.

**2. Develop and obtain new and critical skills.** Out of necessity, many of those Special Agents who by now would have been the FBI's deeply experienced, journeymen fraud investigators were diverted to terrorism matters after 9/11. Since then we have experienced corporate and mortgage fraud on a scale not seen before, the development of increasingly complex financial and investment instruments, and new modes of fraud schemes in the cyber realm. Getting the training needed to meet these challenges sufficiently and quickly is imperative.

The contemporary knowledge base for these issues currently is not a resident capability for any agency on the scale it needs to be. Expertise from across the public and private sectors will need to be aggregated and leveraged to build the kind of aggressive learning initiative that is called for.

Until this skills gap is narrowed and because the complexity and volume of financial crime in this country far exceeds available FBI investigative resources already stretched to their limit, the FBI may need to augment its internal financial investigative resources with outside resources that specialize in disciplines such as **forensic accounting** or **cyber analytics**. For example, utilizing former FBI and IRS agents as a cadre of experienced financial investigators could assist the FBI through the compilation, review, analysis and investigation of collected data from a wide array of data sources. These forensic/analytic experts could be leveraged to provide tactical (more proactive) and historic (reactive) support to the FBI's financial crimes program.

**3. Aggressively reach out to the Financial Crimes enforcement community and the Financial Services industry.** Historically, the financial crimes problem has been dealt with by a fragmented enforcement community with both discrete and overlapping jurisdictions and usually from a reactive posture as agencies "open cases" on crimes that have already happened or are well underway. And while regulatory reform has been promised to address the current inefficient regulatory environment, turf battles appear to be limiting the scope and effectiveness of proposed changes. Given the realities articulated above, the fragmentation of effort that is currently prevalent and has characterized enforcement response to date must be replaced with a strategy that achieves greater integration among the disparate law enforcement and regulatory entities. Absent this kind of strategic approach, a more forward leaning, proactive posture against this new financial crimes environment will be difficult to achieve.

But greater integration with the enforcement community alone won't be sufficient. Of equal importance is the need for the FBI to become more visible and interactive with the Financial Services industry. While the relationship between the enforcement and financial communities has been and can be adversarial at times, there are opportunities in this challenging operating environment, where problem sets seem to take on intractable characteristics, that make collaborative networking advantageous to both communities. INFRAGARD is an example of an FBI-led public/private collaboration that has helped advance the Bureau's interests in cyber crime. The same approach is needed to take on complex financial crimes.

The FBI has long recognized the value of teaming with other agencies through the task force model and has joined very effectively with private sector partners

to foster cooperation and intelligence in the cyber, counterintelligence, and criminal programs (INFRAGARD, ANSIR, DSAC.) Developing a focused outreach to, and partnership with, the financial industry and key regulatory agencies such as the SEC, FED, FDIC and others would be a logical piece of an overarching financial crimes strategy that could strengthen the FBI's ability to be more predictive and anticipatory in this area.

One other thing appears quite clear: While there are a number of agencies that will have a role in this rapidly evolving financial crimes environment, it is the FBI that will need to lead the way.

### **How the Booz Allen Team Can Help**

Booz Allen and IPSA International are working cooperatively on this issue with the specific goal of assisting the FBI in this critically important arena. This collaboration is led by a set of executives who have had successful careers in the FBI, USSS, DOJ, and Treasury Department with hands on investigative, intelligence, and policy experience and a strong interest in seeing the FBI lead and succeed in this battle. We believe there are four strategic areas where the combined expertise of Booz Allen and IPSA International can be of significant benefit.

**1. Advanced data analytics.** At Booz Allen, we have developed and customized advanced data analysis tools to help government clients improve their ability to make the most out of their data holdings. Our delivery to the FBI of specially designed advanced data analytic capabilities could help put the Bureau on a more predictive, proactive footing in the fraud and financial crime areas.

**2. Training.** The Booz Allen/IPSA team can help manage and deliver this critically important strategic requirement, aggregating in-house, academic, and industry experts to deliver timely and up-to-date instruction on this complex topic, thereby helping build skills and capabilities currently in short supply.

**3. Forensic assistance.** IPSA International has a cadre of over 650 financial investigators and analysts, most of whom are former law enforcement personnel who can augment criminal investigations and prosecutions with forensic/analytic support, as well as facilitate the development and implementation of proactive intelligence initiatives to identify and target the most significant financial criminals.

**4. Managing a public/private partnership.** The Booz Allen/IPSA team, through its extensive government and industry contacts, is well positioned to drive and manage a comprehensive outreach program on behalf of the FBI and thereby

minimize diversion of investigative resources away from critical mission activities.

## **Conclusion**

In the end, it's about leadership. Today, fraud and other forms of financial crime have imperiled our financial and national security as it has in no prior era. While many entities have a role in fighting this problem, without question the FBI is and must be the leader. The problem, however, is immense and growing. It is complex and getting more so. Leadership will require a strategy that acknowledges reality and then considers every tool that will lead to advantage. We believe we can help.

**Kevin R. Brock**, Principal, Booz Allen Hamilton; former Deputy Director, NCTC and Assistant Director, Directorate of Intelligence, FBI; [brock\\_kevin@bah.com](mailto:brock_kevin@bah.com)

**Dennis Lormel**, Managing Director, IPSA International; former Section Chief Terrorism Finance Operations Section, CTD, FBI; [dlormel@ipsaintl.com](mailto:dlormel@ipsaintl.com)

**Patrick O'Brien**, Principal, Booz Allen Hamilton; former Assistant Secretary, Terrorist Finance and Financial Crimes, U.S. Dept. of Treasury; [obrien\\_patrick@bah.com](mailto:obrien_patrick@bah.com)

**Chris Swecker**, Chris Swecker Enterprises; former Director, Corporate Security, Bank of America; former Assistant Director, Criminal Investigative Division, FBI; [sweckchris@aol.com](mailto:sweckchris@aol.com)