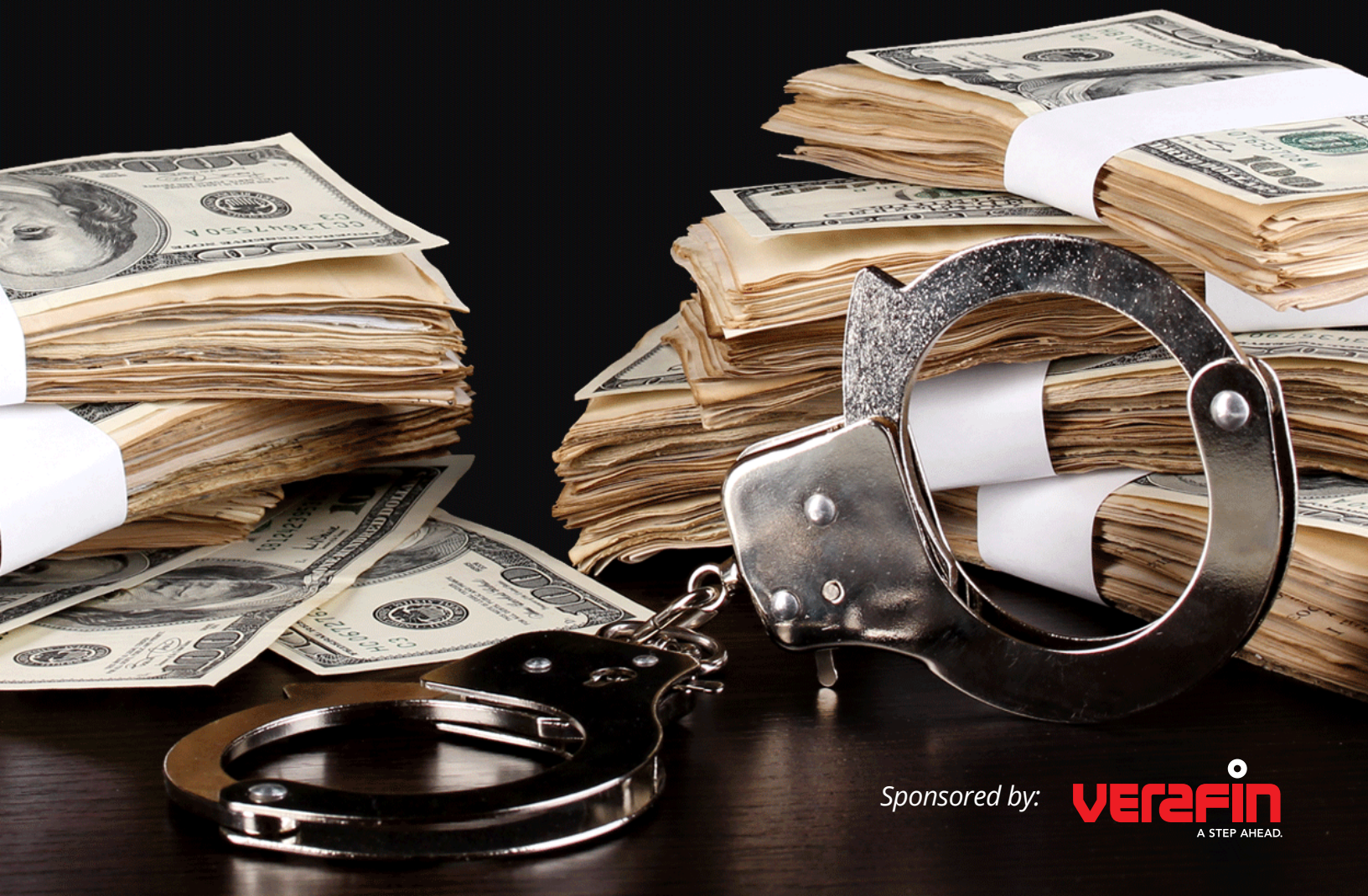
Global Criminal Enterprises Pursue the Most Profitable Crime Model in Modern History

Distributing Losses Across the Financial Services Industry

A Chris Swecker White Paper



Sponsored by: Verafin — A STEP AHEAD.

Global Criminal Enterprises Pursue the Most Profitable Crime Model in Modern History Distributing Losses Across the Financial Services Industry

A Chris Swecker White Paper

Prior to the Internet and the financial crime wave led by the Russian/Eastern European criminal enterprises a lone white collar criminal like Frank Abagnale of *Catch Me If You Can* notoriety could garner the full attention of dozens of FBI Agents across the United States and spark an international manhunt. In today's fraud environment dominated by global criminal networks Abagnale would be just another paperhanger who would scarcely draw the attention of a single federal agent or prosecutor. A dearth of investigative/prosecution resources, the rise of multinational fraud rings and common sense has forced the federal agencies to prioritize their work in favor of targeting collusive criminal organizations who inflict multimillion dollar losses over extended periods of time in contrast to colorful one-off actors like Abagnale, who, while worthy of some attention, lack the capacity to cause such damages.

> *"The next stage in seizing the initiative from the criminal enterprises is taking the bold step of collaboration across the entire FI industry. Only then can the FIs move from reactive to proactive and lead the triumph of our most critical industry over the grimy global empire of fraud."*

Despite the massive losses inflicted by the crime rings it is an unfortunate reality that financial institutions still seem focused on working one fraud at a time without building in processes to identify the malignant social networks that vex the industry. Internal silos built up over time compartmentalize data by products, channels and services. Technology is a patchwork quilt of legacy systems and solutions geared towards meeting the needs of individual business components. Cross-referencing and linking seemingly disparate fraud events is still a heavily manual process. Outside the auto insurance companies, industry wide cooperation is the exception not the rule, especially between financial institutions. This is despite the availability of powerful analytical tools, easy access to big data relevant to fraud detection and the knowledge that digital age offenders ply their trade across multiple industries and government agencies.

Speaking of industries, these global criminal enterprises have created an evil industry of their own focused on looting banks, government benefit programs, insurance companies, retailers, the payment card industry and their customers that has no rival in modern history. Aided by a permissive environment, business savvy fraud professionals have mounted a digital crime wave that makes traditional "bricks and mortar" organized crime seem pedestrian in comparison. Our government and private industries are by no means idle, but current detection systems that provide

alerts without informative context, "pay and chase" strategies and the ability to build fraud into the balance sheet while passing the costs on to a fraud weary customer are inefficient and ineffective.

These losses are due to an unprecedented rise of criminal enterprises focused almost exclusively on financial crimes. The scope and breadth of the losses inflicted by these digital age crime syndicates is staggering. US companies and government agencies are not clamoring to publicize their losses, or "improper payments" in the parlance of government auditors and program integrity professionals, but a cursory survey based on the most credible figures provided by professional associations and government watchdogs places losses at over 650 Billion dollars[1].

Identifying and understanding the risks facing an organization and an industry is a multi-step process. It is not only necessary to understand the type of risk presented, it is critically important to fully understand the dark forces that present the risk. In other words one must not only understand the "what" but also the "who." Moreover, as the legendary warlord Sun Tzu advocated, risk executives must advance beyond these fundamental tenets of conflict to then accurately assess your own strengths and weaknesses in order to determine how to most effectively match up against the enemy. This strategy requires us to be very familiar with our own capabilities and limitations. The results of such an assessment with respect to financially driven crimes highlights a significant mismatch with the overwhelming advantage to the financial crime rings.

These well-networked criminal enterprises inflict massive losses and damage to a company's reputation and brand in an era where customers have been sensitized to the seeming inevitability of victimization. Unfortunately the victims, government agencies and private industries, tend to deploy strategies and electronic alerts that treat each incident as isolated and unrelated. Thus criminal networks thrive and endure for extended periods while the good guys engage in a never-ending game of whack-a-mole, taking the next case or alert without regard to its significance in terms of its relationship to the broader, collusive ring activity. Only by understanding the full nature and scope of the threats presented by financial crime conspiracies can our industries and agencies mitigate and prevent these losses.

Modern criminals, if nothing, are students of our business processes and procedures. Russian/Eastern European/Balkan transnational criminal networks have a long and intimate association with current and former intelligence services and their agents who not only tolerated a thriving black market, they enabled them and were active participants. Infiltration, surveillance and even ownership

"Criminal networks thrive and endure for extended periods while the good guys engage in a never-ending game of whack-a-mole, taking the next case or alert without regard to its significance in terms of its relationship to the broader, collusive ring activity."

1 This data was derived from the FBI, the National Insurance Crime Bureau (NICB), the US Government Accountability Office, The National Anti Health Care Fraud Association, the Mortgage Banker's Association and Javelin.

of legitimate businesses were and still are their specialties. In the 1980s and 1990s, instead of being arrested, criminal hackers were often identified and pressed into service by corrupt government agencies. Another specialty is extensive knowledge of IT systems and their vulnerabilities. As a result these are the most formidable, and the most profitable criminals in the world today.

After the collapse of the Soviet Union and its satellite states, Eurasian criminal syndicates swept across Europe and into the United States innovating such crimes as staged accidents, healthcare fraud, internet facilitated electronic crimes, data theft and many of the more profitable bank fraud schemes. They are responsible for virtual black markets that facilitate complex schemes that syndicate fraud across the globe and produce massive losses. They have not cornered the market on financial crimes schemes however. Homegrown United States based fraud rings have perfected conspiracies revolving around mortgage, check, auto loan and investment fraud schemes. Together these criminal enterprises have created a financial crimes tsunami that begs for institutions to adopt new and more effective counter fraud strategies.

While insurance companies, the retail sales industry, government benefit programs, financial services and their customers/beneficiaries are all victims of these malignant networks, the financial services industry bears a disproportionate burden. This is because they have the legal responsibility to not only detect fraud against their products and services but they must also detect, prevent and report the movement of illicit proceeds and terrorist funding. Most of these illicit proceeds, including the terrorist funding are the fruits of crimes. In fact any criminal activity that produces proceeds will inevitably involve the federal offense of money laundering.

Bank executives have to also consider that the average consumer now looks to their chosen financial institution to protect them from the ubiquitous crimes of credit card fraud, identity theft, account takeovers and the like. To these customers fraud is a personal affront and unfortunately most banks fumble the mitigation process, further alienating the customer. There are many credible indications that protecting the customer from fraud is now a business differentiator. For example a 2012 Aite Group survey of over 5000 consumers in 17 countries revealed that attrition rates after experiencing card fraud average 21% among cardholders surveyed. Almost 50% of the respondents were especially concerned about identity theft. They blame both the financial institution and the retail establishment where the underlying data compromise occurred and vote their displeasure with their feet.

An honest assessment of the current vulnerabilities of the financial services industry in particular paints a picture of an industry rife with cracks and seams that are systematically exploited. It is not that the banks are not working furiously to discharge their fraud and anti-money laundering responsibilities, it is more a function of their flawed strategies and the limitations of law enforcement that inhibits them from stemming the losses.

> *"This resource driven strategy ensures that a huge volume of losses will be misclassified as credit loss and charged off. The tragedy is that this information is not systematically analyzed to possibly link with other fraud activities."*

In addition to scarce resources, the limitations on the part of law enforcement center on the global and dispersed nature of the transnational criminal networks and the use of the Internet to steal personal data and market it to virtual networks via dark web based black markets. Electronic crimes can be committed from permissive countries around the globe without ever setting foot in the US confounding traditional law enforcement jurisdictional reach. Furthermore the agencies that are best positioned to address these networks, the FBI, the US Secret Service and the US Department of Justice are downstream from the real action where accounts are established and transactions move through the bank's systems. They are highly dependent on criminal referrals and SARs to provide the predication to open an investigation.

> *"Homegrown United States based fraud rings have perfected conspiracies revolving around mortgage, check, auto loan and investment fraud schemes."*

Because of limited resources the FBI and federal prosecutors has been forced to set dollar loss thresholds of at least $250,000 or more before investigations and prosecutions can be initiated. In one study the FBI revealed that over 5500 potential embezzlements SARs were reported by financial institutions but only 550 were actually investigated and only 429 were ever prosecuted. In essence even an internal fraud operator had a 92% chance of getting away clean.

In the final analysis, it is the financial institutions themselves who are best positioned to impact this crime problem. Financial institutions however have significant limitations that go beyond those discussed above. They set their own thresholds that often mirror the SAR filing triggers of at least $5000 and some go as high as $40,000. This resource driven strategy ensures that a huge volume of losses will be misclassified as credit loss and charged off. The tragedy is that this information is not systematically analyzed to possibly link with other fraud activities.

Law enforcement agencies and senior executives have characterized Transnational Criminal Organizations (TCOs) as systemic threats to the financial industry. Former Treasury Undersecretary Office of Terrorism and Financial Intelligence, David Cohen, put is best when he said "Almost no illicit activity is off-limits for today's transnational criminals. From drug trafficking to human trafficking to weapons trafficking, and from identity theft to cyber theft to intellectual property theft, TCOs today engage in an unprecedented array of illicit activities all across the globe, often aided by corrupt officials and criminally-connected powerful businessmen. In doing so, they have become adroit at exploiting the scale and speed of information flows, online money transfers, and virtual "black marketplaces" while reducing their risk of detection by taking advantage of regulatory gaps and open borders"

The best way to illustrate the threats facing the financial industry by criminal networks is to look to actual cases. In a recent November 2015 indictment U.S. prosecutors unveiled criminal charges against three men accused of running a sprawling computer hacking, money laundering, identity theft and bank fraud scheme that included a huge attack against JPMorgan Chase & Co. and generated

hundreds of millions of dollars of illegal profit. The indictment paints a picture of a multinational criminal enterprise built in part on data acquired through major breaches at a dozen financial companies. Prosecutors said the enterprise dated from 2007, and caused the exposure of personal information belonging to more than 100 million people. "By any measure, the data breaches at these firms were breathtaking in scope and in size," and signal a "brave new world of hacking for profit," U.S. Attorney Preet Bharara said at a press conference in Manhattan. The alleged enterprise included pumping up stock prices, online casinos, payment processing for criminals, an illegal bitcoin exchange, and the laundering of money through at least 75 shell companies and accounts around the world.

The second example is a common scenario in the auto industry—an auto loan fraud ring that netted over 1.9 million from a total of 18 financial institutions. This fraud operation used a system of recruiters to find straw car buyers and supplied them with fictitious earnings and other essential borrower information. The straw borrower then financed a car purchase but instead of taking ownership of the car they received a lucrative kickback while the ring leaders took possession of the car and either resold it or rented it to drug dealers or other dodgy characters. After two to three loan payments were made the loan would "bust out" or default leaving the banks with the losses and a red face[2]. In this scheme several corrupt car dealers were participants in the fraud so not only did they receive the proceeds of the loan but also the car. In many cases the auto was financed by one dealer but actually sold to the straw buyer by another sketchy car dealer without the knowledge of the hapless lender. An additional example of an auto loan fraud ring is one which was recently detected by Verafin that involved 42 loans across 29 financial institutions in 10 states while inflicting losses of a million dollars.

Another area where FIs are challenged by fraud rings involves mortgage fraud. An investigation by the North Carolina FBI office code named "Operation Waxhouse" uncovered a massive fraud ring in the town of Waxhaw, NC that consisted of over 100 individuals many of whom were industry insiders including four appraisers, 38 promoters, six financiers, 13 loan officers and mortgage brokers, six residential builders, six real estate agents and six attorneys. These coconspirators were charged with mortgage fraud; money laundering; racketeering; wire and mail fraud; securities fraud and tax violations. The scheme consisted of straw buyers who purchased and financed real estate that was fraudulently appraised at highly inflated values. Kickbacks were provided to all the participants along with dummied up fees and costs to the attorneys, builders and real estate agents. Banks were left holding the bag with precious little restitution made after the prosecutions were completed. It was schemes like those found in Operation Waxhouse that contributed to the financial meltdown in 2008-2009.

An additional example of an auto loan fraud ring is one which was recently detected by Verafin that involved 42 loans across 29 financial institutions in 10 states while inflicting losses of a million dollars.

2 By contract if a loan defaults within 2-3 payments it falls on the dealer who brokered the loan to absorb the losses.

And last but not least, health care fraud perpetrated mainly by Russian/Eastern European mobsters accounts for up to 263 billion dollars a year in losses based on false claims to Medicare, Medicaid and private medical insurance[3]. In one national takedown in June 2015, more than 240 individuals—including doctors, nurses, and other licensed professionals—in 17 cities were arrested for their alleged participation in Medicare fraud schemes involving approximately $712 million in false billings. Note that in addition to fraud and conspiracy charges, the subjects were charged with money laundering. These types of losses can only be inflicted by large conspiracies operating for years in contrast to opportunistic individuals who simply lack the capacity. All of these fraud proceeds ran through various accounts within US financial institutions, which begs the question of how such massive schemes can be missed for such lengthy time periods.

"Criminal enterprises have created a financial crimes tsunami that begs for institutions to adopt new and more effective counter fraud strategies."

CONCLUSION

The famous political philosopher Edmund Burke once said, "the only thing necessary for the triumph of evil is for good men to do nothing." Financial crime enterprises have become the most dominant crime problem of this millennium and present a systemic business risk. As measured by the dramatically rising loss levels across the financial, retail and insurance industries as well as government benefit programs, it is not overly harsh to say that clinging to outdated strategies has the same effect as doing nothing.

Owing to their obligations under the Bank Secrecy Act and its progeny, the financial services industry bears the greatest burden to detect, report and mitigate the unlawful acts of the coconspirators. Our legal system views collusive criminal activity as more dangerous to society than single criminal actors by providing for severe penalties for conspiracies and racketeering enterprises. In spite of this, the strategies and tools deployed by FIs still focus on the single event rather than collusive action. The first step to breaking the loss paradigm is to prioritize the detection and mitigation of criminal enterprises over individual opportunistic fraud events. FIs must break down data silos and employ the most powerful analytical technologies available to link fraud events to identify the ring activity that is hemorrhaging individual banks and the financial services industry as a whole.

The next stage in seizing the initiative from the criminal enterprises is taking the bold step of collaboration across the entire FI industry. Only then can the FIs move from reactive to proactive and lead the triumph of our most critical industry over the grimy global empire of fraud. As Edmund Burke also said: "When bad men combine, the good must associate; else they will fall one by one, an un-pitied sacrifice in a contemptible struggle."

3 In 2012 Donald Berwick, a former head of the Centers for Medicare and Medicaid Services (CMS), and Andrew Hackbarth of the RAND Corporation, estimated that fraud (and the extra rules and inspections required to fight it) added as much as $98 billion, or roughly 10%, to annual Medicare and Medicaid spending—and up to $272 billion across the entire health system.

About the Author

Chris Swecker

Financial Crimes Consultant and Attorney; retired Assistant Director, FBI; and former Global Security Director, Bank of America

Chris Swecker has 30 years of experience in law enforcement, national security, legal, and corporate security/risk management. Swecker served 24 years with the Federal Bureau of Investigation (FBI) before retiring as Assistant Director of the FBI's Criminal Investigative Division. He was responsible for eight FBI divisions including Cyber, Criminal, International Operations, Training, Crisis Management, Operational Technology, Criminal Justice Information and the Law Enforcement Liaison office encompassing more than half of the FBI's total resources. Swecker also served as the FBI's On Scene Commander in Iraq in 2003 where he led a team of FBI Agents conducting counter-intelligence and terrorism investigations.

As head of the FBI's Criminal Division, Swecker led all FBI criminal investigations including public corruption, money laundering, organized crime/drug trafficking and financial crime matters. He was instrumental in the development of the FBI's post 9-11 strategies, leveraging criminal investigative resources to support counter terrorism/intelligence efforts. He led national task forces on corporate fraud, violent gangs, financial crimes, crimes against children, public corruption and organized crime and established the MS-13 National Gang Task Force and the National Gang Intelligence Center. Swecker has extensive experience in organized crime, money laundering and major drug trafficking investigations.

As Corporate Security Director for Bank of America, Swecker led investigations; physical security; international security; employment screening and executive protection. He executed a comprehensive transformation of all aspects of the security organization, emphasizing the use of advanced analytical software, security technology and fusion of open source, government and internal information to drive strategies to prevent fraud, privacy and security events.

Swecker received the prestigious Presidential Rank Award for his service in Iraq and as Special Agent in Charge of the NC Office. He has testified before Congress on topics such as identity theft, crimes against children, mortgage fraud, human trafficking, financial crimes, information privacy and data compromise, crimes on the Internet, drug trafficking and gangs. He has appeared as a guest on numerous media programs including CNN, 60 Minutes, Good Morning America, CSPAN Washington Journal and Oprah Winfrey. He is a frequent public speaker on financial crimes, money laundering and cyber crimes.

About Verafin

Verafin is the leader in cloud-based, cross-institutional Fraud Detection and Anti-Money Laundering (FRAMLx) collaboration software with a customer base of 1400 financial institutions across North America. Its solution uses advanced cross-institutional, behavior-based analytics to help financial institutions stay a step ahead of numerous types of fraud as well as the BSA, USA PATRIOT Act, and FACTA compliance landscape, while allowing them to collaborate cross-institutionally.

Verafin is the exclusive provider of fraud detection and BSA/AML software for the California Bankers Association, Florida Bankers Association, Illinois Bankers Association, Massachusetts Bankers Association, CUNA Strategic Services, a preferred service provider of the Independent Community Bankers of America, and has industry endorsements in 44 states across the U.S.

Learn more

For more information on this topic, or how Verafin can help your institution stay a step ahead of financial crime, visit www.verafin.com/framlx, email info@verafin.com or call 866.781.8433.

To access Verafin's archive of webinars, white papers, success stories and other materials focusing on BSA/AML compliance and fraud detection topics relevant to financial institutions across the country, check out our online Resource Center at www.verafin.com