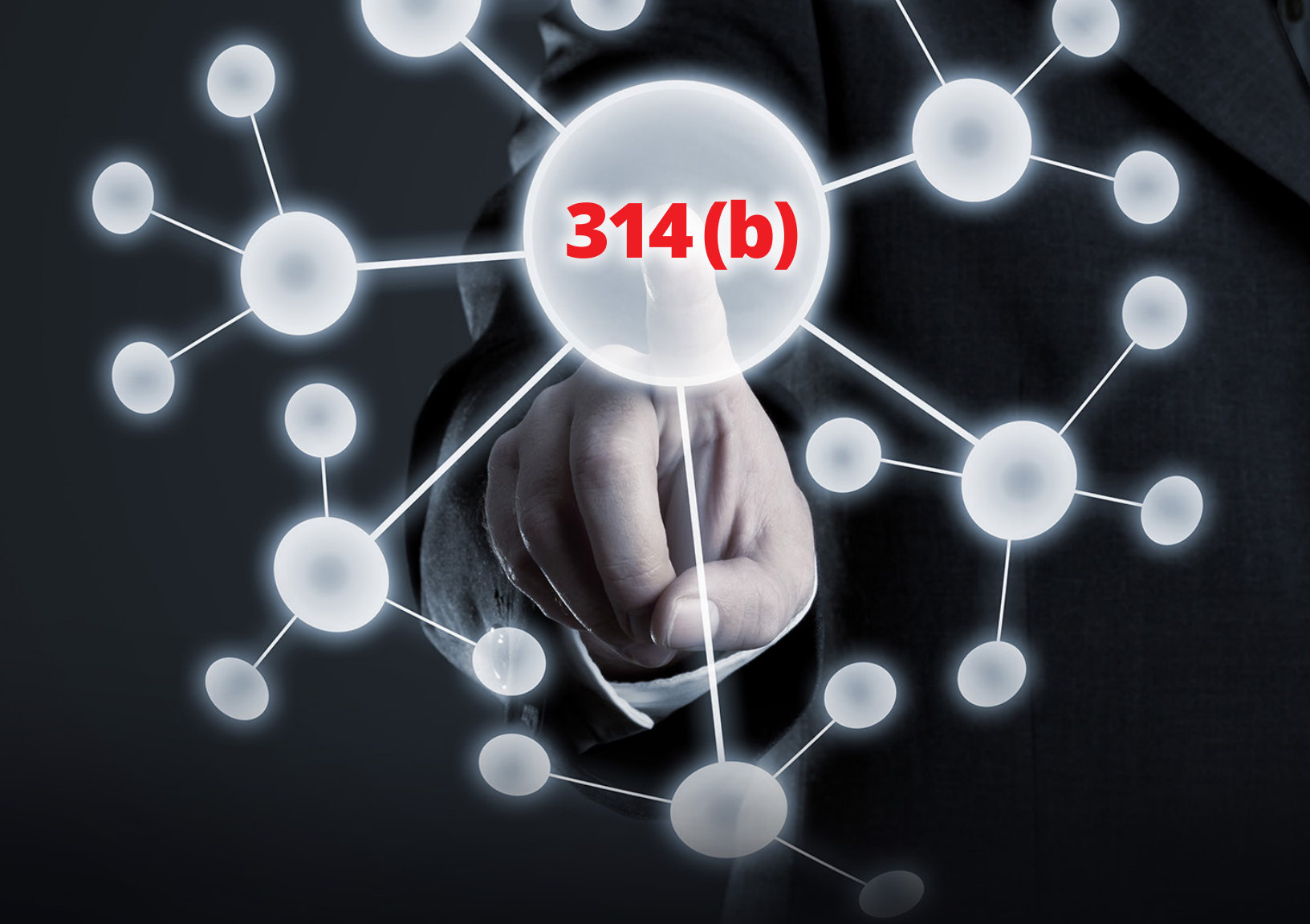

Section 314(b)

The Best Hope For Collaboration Between Financial Institutions To Combat The Movement Of Illicit Proceeds

A Chris Swecker White Paper

Sponsored by: VERAFIN
A STEP AHEAD.

Section 314(b): The Best Hope For Collaboration Between Financial Institutions To Combat The Movement Of Illicit Proceeds

A Chris Swecker White Paper

Global Criminal Enterprises and Terrorist Organizations have been exploiting vulnerabilities caused by persistent silos within and between Financial Institutions (FIs) for several decades and yet one of the most important tools to seize the initiative from them has been underutilized. That tool is Section 314(b) of the USA PATRIOT Act which provides financial institutions with the ability to share information between one another under a safe harbor that offers protections from liability in order to better identify and report potential money laundering or terrorist activities.[1] While Section 314(b) information sharing is a voluntary program, FinCEN has strongly encouraged information sharing through this process when possible criminal activity is suspected.[2]

> *"Linking seemingly unremarkable accounts and transactions at one institution with other accounts at separate FIs which are associated with nefarious activity can provide important context to making decisions as to what action should be taken, such as denial of the account or transaction and/or filing a SAR."*

Unfortunately, despite the enactment of and FinCEN's emphasis on the use of 314(b), relatively little information sharing takes place between financial institutions. The most recent study conducted by FinCEN of the usage of 314(b) between financial institutions shows that only one 314(b) related SAR for every two financial institutions was filed in 2012.[3] In a previous study in 2011, FinCEN had noted that 314(b) participation by smaller FIs was tepid.[4] This very revealing report noted that the lion's share of the sharing took place between the top tier FIs.[5] There is no evidence that this paradigm has changed. While such SAR filings have grown every year since these studies, it is clear that industry-wide collaboration is the exception, not the norm, and systemic cooperation to combat the movement of illicit proceeds in the financial services industry is still in its infancy.

Many Criminal Enterprises prey on credit unions and community banks knowing that resources are scarce and strategies to link or "cross reference" crime ring activity are too often reliant on manual processes. They also know that due to intense competition between institutions, sharing data is not a high priority for bank executives who quite understandably are focused on the bottom line. In this environment, collusive criminal activity targeting multiple institutions thrives and prospers.

1 FinCEN 314(b) Fact Sheet: https://www.fincen.gov/statutes_regs/patriot/pdf/314bfactsheet.pdf

2 " "Specified unlawful activities" under 18 U.S.C. 1956 and 1957 include a broad array of underlying fraudulent and criminal activity" *FinCEN Director Jim Freis to Louisiana Bankers Association, April 26, 2012.*

3 FinCEN Office of Special Programs Development, *SAR Activity Review Trends, Tips & Issues (Issue 23).* See also, FDIC Institution Directory-Advanced Search: https://www5.fdic.gov/IDASP/

4 FinCEN: Financial Institutions Outreach Initiative, *Report on Outreach to Depository Institutions with Assets Under 5 Billion*; page 58-60, February 2011.

5 FinCEN: Financial Institutions Outreach Initiative, *Supra*

FIs are often stymied by a fundamental misunderstanding that acts of fraud or other criminal violations are insufficient to invoke 314(b)'s safe harbor provision. Nevertheless, FinCEN Director Jennifer Calvery could not have been more clear when she stated in a speech to the Securities Industry and Financial Markets Association (SIFMA): "*I can tell you as a former money laundering prosecutor who has handled several fraud related money laundering cases, anytime you have funds that you suspect are related to fraud in or moving through your financial institution, you should also be suspicious that transactions made with those funds may involve money laundering*."

To Director Calvery's point, outside of certain categories of violent crime, there are very few criminal activities that do not produce illicit proceeds. Indeed, profit is the driving force behind most crimes. In the context of a financial institution's obligations under the Bank Secrecy Act, the term "fraud" should be shorthand for any criminal activity that produces illicit proceeds that are involved in an actual or attempted transaction. In other words, the term "fraud" should be viewed as encompassing the entire spectrum of "specified unlawful activities" proscribed by the primary federal money laundering statutes: 18 U.S.C. 1956 and 1957.

Linking seemingly unremarkable accounts and transactions at one institution with other accounts at separate FIs which are associated with nefarious activity can provide important context to making decisions as to what action should be taken, such as denial of the account or transaction and/or filing a SAR. Within financial institutions, however, detection and case management systems drop the next alert or case out of the queue with little insight as to whether the case is linked to others. The use of artificial thresholds and charge-offs ensure that smaller alerts and cases will never be analyzed, let alone linked to broader criminal activity.

Meanwhile, digital age criminals and terrorists who have acquired a profound understanding of financial industry business processes, confound contemporary efforts to detect and mitigate the threats they present to the brand and bottom line by simply refusing to operate in the neat categories that FIs try to place them. They conspire and collude to commit a wide variety of criminal violations across a broad swath of FI service delivery channels and products. They also operate unimpeded across the industry including large, medium and small institutions. A case in point: one recent auto financing fraud ring case that has yet to be prosecuted involves 25 financial institutions across six states and at least five different banking products including credit card, checking account, auto loans, ACH and online banking services. This ring operated for over three years without detection of the broader crime scheme until a pilot project sponsored by Verafin identified the collusive activity.

Avoiding detection by staying below existing thresholds and dispersing the illegal activities across multiple institutions is a key strategy employed by the crime rings.

> *"The activities of money mules, the foot soldiers of a fraud enterprise, can often be the key to linking seemingly disparate accounts and transactions because they perform the actions on the ground such as opening accounts, structuring cash deposits, purchasing gift cards with illicit proceeds, requesting wire and ACH transfers to/from funnel accounts and countless other essential tasks. They also provide addresses, phone numbers, email accounts and other rich data that can be matched."*

Instead of one group conducting a fraud scheme from start to finish, larger criminal organizations will attempt to avoid detection by breaking down into smaller groups that specialize in one aspect of fraud. One group may specialize in stealing identities and selling them; another group specializes in recruiting "money mules" and selling their services; then another group actually trains and uses the mules to commit fraud. The activities of money mules, the foot soldiers of a fraud enterprise, can often be the key to linking seemingly disparate accounts and transactions because they perform the actions on the ground such as opening accounts, structuring cash deposits, purchasing gift cards with illicit proceeds, requesting wire and ACH transfers to/from funnel accounts and countless other essential tasks. They also provide addresses, phone numbers, email accounts and other rich data that can be matched.

This criminogenic environment is enabled and compounded by the tacit and many time express support of countries such as Russia, Romania, Bulgaria, Bosnia and others. Government resources and expertise are scarce, and even if there are rudimentary cyber hacking laws on the books, corrupt and complicit public officials have scarce interest in enforcing them. More importantly, these Criminal Enterprises are far more collaborative than the good guys, cooperating and networking in the hidden crevices of the "deep" web where virtual black markets thrive.

There is no shortage of compelling examples of the yawning holes in the financial industry due to the low level of industry-wide collaboration. Professional crime rings routinely exploit these industry-wide silos. For example, a large bank fraud ring was indicted in U.S. District Court for the Western District of Washington in February 2015. Ten defendants were named in the indictment for fraud on seven different financial institutions. The 60 count federal indictment alleged that between November 2010 and February 2015, the co-schemers used 219 different bank accounts to steal more than $987,000 from the seven banks. The defendants used stolen checks to make fraudulent deposits into various bank accounts, withdrawing large amounts of cash before the bank determined the check used to inflate the balance was no good. This Criminal Enterprise escaped detection for almost five years.

In Operation Trident Breach, an extraordinary FBI cyber investigation resulted in the indictment of 96 money mules and their Russian handlers for inflicting 70 million dollars in losses to banks and businesses across the United States. The mules used account numbers and personal information stolen from tens of millions of consumers and businesses including bank account numbers, passwords, personal identification numbers, and other information necessary to log in online to thousands of bank accounts across hundreds of US financial institutions. Russian mastermind Evgeniy Bogachev stole the personal data by means of the Zeus virus, which he invented and propagated.[6]

“There is no shortage of compelling examples of the yawning holes in the financial industry due to the low level of industry-wide collaboration. Professional crime rings routinely exploit these industry-wide silos.”

[6] Bogachev is the subject of an extraordinary three million dollar FBI reward for his capture and is hiding in Russia where the government is aware of his presence but refuses to extradite him.

At least 46 funnel accounts across a like number of banks were identified during the investigation. The scheme ran for over two years without detection of the massive collusive ring. One mule was an immigrant from Moldova who within a few months of her arrival in New York had opened at least six bank accounts using a trio of names. Another mule, a Russian national, opened eight accounts at three different banks using five different aliases.

New products such as remote deposit capture provide fraud rings fresh avenues to defraud banks by depositing the same check into accounts in multiple institutions. Even the most rigorous deposit review mechanisms are powerless to identify and reject items that have been previously deposited at other financial institutions.

Despite the overwhelming amount of proceeds generated by collusive criminal activity, FIs often erroneously are fixed on the notion that they must have a clear case of pure money laundering or terrorist financing in order to meet the prerequisites of 314(b). In addition, bank attorneys tend to favor a very narrow interpretation of "transaction" as a rationale for restricting the use of the provision. Under this theory, fewer cases investigated equals fewer problems. This mindset runs contrary to the letter, spirit and intent of the legislation and FinCEN's guidance.

The legal foundation of the concept of sharing between institutions is found in the federal money laundering statutes 18 U.S.C. Section 1956 and 1957 where "specified unlawful activities" or SUAs are described and enumerated. These SUAs include no less than 230 state felonies and federal offenses including conspiracies, attempts, aiding and abetting and the Racketeer Influenced and Corrupt Organizations (RICO) statute with all its predicate offenses. FinCEN guidance emphasizes that an FI need only be aware of "*possible money laundering activities, including those associated with the underlying SUAs.*"[7]

Possible transactions involving these proceeds could include the simple act of attempting to open an account that is linked to a funnel account at another FI,[8] attempting to deposit or move funds between banks or provision of false documentation in attempting to conduct a transaction. Furthermore, it is clear also from the text of the FinCEN Fact Sheet and guidance that a "transaction" at one institution can form the basis for action taken at a second institution where a transaction has yet to take place. In FinCEN's own words, 314(b) can be used to "*help a firm's decision to close an account or decline to open a new account. At the same time, a financial institution may proactively use 314(b) to alert other firms of information about their client that they might not have been aware of before the information sharing.*"[9]

> *"In particular, it is undisputed by counterterrorism agencies, but often not well understood by financial institutions, that organizations such as Hezbollah, Al Qaeda and ISIL often use ordinary criminal activity such as various bank crimes, cigarette smuggling, government benefits fraud, drug smuggling, human trafficking, trafficking in counterfeit goods and many other criminal schemes to finance their operations."*

[7] FinCEN Guidance: FIN-2009-G002; Issued: June 16, 2009; Subject: Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act.

[8] Funnel accounts are bank accounts that receive illicit proceeds via various interbank transfers and structured deposits. These funds collect in the funnel account and are periodically transferred to off shore or safe-haven accounts.

[9] FinCEN SAR Activity Review Trends Tips & Issues (Issue 18)

Note the use of the phrase "decline to open" is an event that precedes a transaction and "proactive" clearly supports taking action before a nefarious act takes place.

One significant obstacle to more widespread use of the USA PATRIOT Act provision is the traditional separation between "Fraud" and Anti Money Laundering (AML) programs, an organizational flaw based on the premise that "fraud" and money laundering/ terrorist financing are distinct and separable. Nothing could be further from the truth. In particular, it is undisputed by counterterrorism agencies, but often not well understood by financial institutions, that organizations such as Hezbollah, Al Qaeda and ISIL often use ordinary criminal activity such as various bank crimes, cigarette smuggling, government benefits fraud, drug smuggling, human trafficking, trafficking in counterfeit goods and many other criminal schemes to finance their operations.

"Information sharing within an organization is critically important, but sharing information between financial institutions would be a game changer."

In 2001, one of the earliest prosecutions involving terrorist financing, a simple cigarette smuggling criminal investigation, ultimately revealed a Hezbollah financing and procurement operation that stretched from Charlotte, NC through Detroit, Michigan and Vancouver, Canada all the way to Hezbollah headquarters in Beirut, Lebanon. An active Hezbollah cell based in Charlotte raised over eight million dollars in illicit proceeds through cigarette smuggling; identity theft; counterfeit goods; and extensive frauds involving credit cards, bank loans, bogus marriages and identification documents. The terrorist operatives were also charged with money laundering, RICO, providing material support to a terrorist organization and bribery of a state department official to obtain false Visas.[10] The cell utilized over 500 different bank accounts across dozens of FIs to facilitate the movement of the criminal proceeds, some of which was sent to high-ranking Hezbollah leaders in Lebanon.

Section 314(b) was not in existence at the time of the Smokescreen investigation, but use of today's analytical tools and bank to bank information sharing would likely have revealed the true breadth and scope of this eight year conspiracy in which 18 members were ultimately indicted. To this day, these types of schemes remain a staple of terrorist organizations to raise funds in this country.

There are shining examples of an industry systematically sharing information to combat a common crime problem. One of the best examples of such industry level collaboration exists now in the auto insurance industry where the National Insurance Crime Bureau (NICB), a nonprofit trade association, pools and shares their claims data.[11] NICB analysts use powerful analytical tools to analyze and link this data looking for crime rings preying on multiple institutions. The NICB employs over 100 such analysts and investigators to identify crime rings and refer such cases to affected insurance

[10] FBI Law Enforcement Bulletin, December 2007, Volume 76, No. 12: https://www2.fbi.gov/publications/leb/2007/dec2007/december2007leb.htm - page20

[11] The NICB is the nation's leading not-for-profit organization exclusively dedicated to preventing, detecting and defeating insurance fraud and vehicle theft through data analytics, investigations, training, legislative advocacy and public awareness. The NICB is supported by more than 1,100 property and casualty insurance companies and self-insured organizations. To learn more visit www.nicb.org.

carriers who in turn notify law enforcement. Such cases receive focused attention because they meet the prevailing multi-victim, high dollar loss thresholds that justify federal law enforcement attention. The primary federal agencies involved in financial crimes and terrorism investigations such as the FBI and the US Secret Service do not have the resources to address "one off" or lesser value cases nor will federal prosecutors introduce such low impact matters into an already over tasked judicial system.

Conclusion

It is no secret that criminals and terrorists have all the advantages when it comes to their use of the financial system to further their illicit activities. Pay and chase systems; institutional silos; inadequate resources for detection and investigative programs; the dispersed, global nature of criminal/terrorist enterprises and many other factors conspire against the banks. A large game of whack-a-mole plays out every day, a situation that inures to the benefit of the bad guys. They especially benefit when information silos persist across the financial services industry. The lessons of one of the most tragic events in American history, the terror attacks of 9-11, where disparate but relevant information was not shared across the US government motivated the US Congress to pass laws and regulations that encourage the government as well as FIs to share information between themselves and government agencies by passage of Sections 314(b) and 314(a) of the USA PATRIOT Act.

Former FinCEN Director Jim Freis staked out FinCEN's position soon after the provision was implemented when he stated: "*Fraud generates dirty money. In order to be used by a criminal that money needs to be cleaned and integrated into the legitimate financial system. The more information bankers and brokers can share the more the integrity of our financial system will be protected and law enforcement can gain additional sources of valuable information.*"

Information sharing within an organization is critically important, but sharing information between financial institutions would be a game changer. Unfounded fears of over-sharing abound. While certain conditions have to be met to enable the sharing and take advantage of the "safe harbor", there are no known cases where this process has been abused to the extent that the protections were not available. FIs can and must seize the initiative and disrupt what is currently a permissive environment for criminals and terrorists. They can only disrupt these activities if they can see the broader collusive activity across the industry. Widespread and systemic information sharing under 314(b) would significantly advance this cause.

> *"FIs can and must seize the initiative and disrupt what is currently a permissive environment for criminals and terrorists. They can only disrupt these activities if they can see the broader collusive activity across the industry."*

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 over 1300 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