



FRAUD AND MONEY LAUNDERING: **BIRDS OF A FEATHER**

a Chris Swecker white paper

Sponsored by



“By fighting fraud, you are fighting money laundering.”

Former FinCEN Director, **Jim Freis**

“Ironically most financial institutions treat the criminal activities as if they were separate from money laundering. The separation of these functions has the effect of creating a severe drag on the effectiveness of both AML and fraud related programs and even serves to enable organized fraud schemes to inflict staggering losses over long periods of time.”

The anti-money laundering guru Charles Intriago has appropriately described the Money Laundering Control Act of 1986 (MLCA) as “the Atomic Bomb of the US in its arsenal against financial crime and other offenses.” Few laws that address financial crimes carry not only a 20 year sentence and significant fine/forfeiture provisions, but also can form the basis for the dissolution of a financial institution through a related criminal indictment for failing to maintain an effective fraud/money laundering detection program.¹ The MLCA is the fountainhead of all Anti-Money Laundering (AML) programs and as anti-fraud and anti-money laundering professionals know, the foundation of this powerful weapon is the commission of a “specified unlawful activity” (SUA) that generates proceeds that are ultimately the subject of a financial transaction. It is fundamental therefore that the first step in the commission of the act of money laundering must involve one of 230 criminal acts that are specifically defined in the statute.

The bulk of these SUAs relate to financial crimes that are standard fare such as check/credit card frauds, bank fraud and mail fraud, but also include weighty organized financial crime schemes such as health care, mortgage and investment frauds. By including SUAs based on the Racketeer Influenced and Corrupt Organizations Act (RICO); Interstate Transportation in Aid of Racketeering (ITAR); and Continuing Criminal Enterprise (CCE); along with the inclusion of conspiracy and attempts, and aiding and abetting, the MLCA is arguably the most sweeping and powerful criminal statute on the books. It is hardly a surprise then that prosecutors add money laundering counts to most financial crimes related indictments.

Ironically most financial institutions treat the criminal activities as if they were separate from money laundering. The separation of these functions has the effect of creating a severe drag on the effectiveness of both AML and fraud related programs and even serves to enable organized fraud schemes to inflict staggering losses over long periods of time. Bad guys love the pigeonholed approach and use it to their best advantage. They are versatile, mobile and follow the money without regard to channel, product or classification of their chosen criminal acts.

The above quote by former FinCEN Director Jim Freis is even timelier now than it was almost five years ago when he addressed the Florida Bankers Association. The thrust of his remarks was to encourage banks to use fraud programs to enhance identification of money laundering activities. The detection and investigations components within financial institutions and other non-law enforcement security professionals are in the best position to effect early recognition of fraudulent criminal actions and therefore prevent or reduce associated losses and compliance risks. In short, law enforcement is far downstream from the real action which includes key activities such as account enrollment and transactions of every description. This paradigm underscores the important role of anti-fraud and AML professionals in reducing the impact of criminal activity relating to financial crimes and supporting the broader law enforcement effort to address what has evolved into the most pervasive crime problem of this millennium.

¹ The offense relates to failing to maintain an effective anti-money laundering program, in violation of Title 31, United States Code, Sections 5318(h)(1) and 5322(a).

“This case [Community One] makes a powerful statement in support of consolidating fraud and AML programs. As more banks are called to account for financial crimes related lapses...the traditional argument that AML programs are more compliance focused than fraud programs and thus must be distinct components simply washes out.”

Take the issue of health care fraud, by far one of the largest sources of financial losses in this country. The FBI estimates annual losses attributable to health care fraud schemes to be at least 80 billion dollars annually which may be significantly understated as private medical insurance providers are not required to report their loss levels while Medicare, Medicaid and other government health care programs are more transparent. The loss trend is on a steep upward trajectory as the dollar amount that occurs in a single incidence of fraud is rising. According to the U.S. Department of Justice (DOJ), an individual case of health care fraud now may involve \$30 to \$50 million, instead of a \$1 million figure ten years ago.

The interrelationship between health care fraud and money laundering is illustrated by the 2010 arrests of seventy-three defendants in a major health care fraud takedown, including a number of alleged members and associates of an Armenian-American organized crime enterprise, who were charged in indictments unsealed in five judicial districts with various health care fraud-related crimes. The main perpetrators belonged to the Mirzoyan-Terdjanian organization which was named for its principal leaders, Davit Mirzoyan and Robert Terdjanian. The leadership of the organization was based in Los Angeles and New York, and its operations extended throughout the United States and internationally. Among the defendants charged with racketeering was Armen Kazarian, who was alleged to be a “Vor”; a term translated as “Thief-in-Law” that refers to a member of a select group of high-level criminals from Russia and the countries that had been part of the former Soviet Union, including Armenia. According to the DOJ press release, this was “the first time a Vor has been charged for a racketeering offense” and the first time since 1996 that a known Vor has been arrested on any federal charge.

The breadth and scope of the fraudulent operation was eye-popping, featuring the operation of at least 118 medical clinics located in 25 states that submitted over more than \$163 million in fraudulent billing to Medicare and Medicaid. While the ten count indictment alleges health care fraud, identity theft, mail fraud and credit card fraud conspiracies, it also included two broad money laundering conspiracies and a RICO indictment count prominently featuring money laundering as “predicate” criminal acts supporting the racketeering conspiracy, illustrating that money laundering is a necessary component of these prolific fraud schemes. After a similar takedown, Alex Acosta, former US Attorney for the Southern District of Florida summed up the role of financial institutions in ferreting out these schemes in stating that bank SARs in particular played a “valuable role” in helping his prosecutors identify fraudulent medical billings and payments in southern Florida, allowing his office to prosecute \$638 million in health care fraud and indicting 197 individuals in 120 cases to return \$40 million to Medicare. Acosta made it a point to include money laundering counts with most health care fraud indictments brought by his office.

Perhaps the greatest exposure to financial institutions associated with failing to detect the nexus between fraud and money laundering are the compliance and reputational risks. For example in 2010, the United States Department of Justice filed charges relating to a \$40 million Ponzi scheme in the Western District of North Carolina. Investigation revealed that the Ponzi operator’s bank, Community One of Asheboro, NC failed to detect or report the Ponzi activity and on April 27, 2011, the Justice Department filed a Criminal Information²

² Information is the equivalent of a criminal indictment in which the subject of the indictment waives presentment to a Grand Jury and consents to filing charges in exchange for lesser offense or deferred prosecution.

“To begin to effectively address the scourge of fraud and money laundering, financial institutions must first develop programs that recognize that financial crimes and money laundering are inseparable. Failure to do so will sideline perhaps the single most powerful tool in the government’s arsenal much to the delight of a wide range of criminal elements.”

against Community One. After negotiations the United States Attorney agreed to delay prosecution for two years if Community One paid \$400,000 in restitution and worked harder to prevent similar incidents. According to a Justice Department news release, Community One “waived indictment and accepted and acknowledged responsibility for its conduct.” “Banks asleep at the switch need to wake up,” said U.S. Attorney Tompkins. *“Federal law requires banks to implement a robust and proactive anti-money laundering program to detect fraud and protect the public from harm. This bank’s failure to detect and report a Ponzi scheme cost it 16 percent of its value. Other financial institutions should heed this warning: the Bank Secrecy Act applies to more than just drug and terrorist financing.”*

This case makes a powerful statement in support of consolidating fraud and AML programs. As more banks are called to account for financial crimes related lapses such as the Community One example, the traditional argument that AML programs are more compliance focused than fraud programs and thus must be distinct components simply washes out.

Finally mortgage fraud which was declared to be an epidemic by the FBI as early as 2004 will almost always involve money laundering.³ By the end of 2011, mortgage fraud schemes comprised the largest single category of criminal SAR files by financial institutions. The 92,028 mortgage fraud related SARs filed were almost triple the 33,443 credit card SARs filed the same year. As of 3/31/13, the FBI had 1,954 open mortgage fraud investigations involving losses of at least \$1 million each. In 2012 almost 1,100 mortgage fraud indictments were issued. A typical case prosecuted in San Diego in July 2012 illustrates the role of money laundering in concealing the proceeds of this activity. Mary Armstrong, an unlicensed mortgage broker who operated a nationwide loan origination fraud and kickback scheme from San Diego with a group of co-conspirators, pled guilty to all five counts of an indictment. Four of these charges involved money laundering violations under 18 USC 1956. It’s cases like this that caused FinCEN to implement a set of rules specifically for non-bank residential mortgage lenders and originators (RMLOs) requiring them to report “suspicious activity, including but not limited to fraudulent attempts to obtain a mortgage or launder money by use of the proceeds of other crimes to purchase residential real estate.” Since implementing the rule almost exactly a year ago on April 16, 2012, FinCEN Director Jennifer Calvery said there’s been a 13 percent increase in filers, suggesting that RMLOs are “stepping up to report mortgage fraud.”

In the current criminal environment, sophisticated fraud operators have many advantages and they are always on the offensive. Pay and chase systems, time delayed point detection solutions and AML and fraud programs that run on parallel tracks in banks compound those advantages. To begin to effectively address the scourge of fraud and money laundering, financial institutions must first develop programs that recognize that financial crimes and money laundering are inseparable. Failure to do so will sideline perhaps the single most powerful tool in the government’s arsenal much to the delight of a wide range of criminal elements.

³ The author made this statement to the US House of Representatives Financial Services Committee in 2004 in testimony following a nationwide mortgage fraud takedown.



Chris Swecker

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

ABOUT THE AUTHOR

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 has testified before Congressional Committees 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 also appeared as a guest on such media programs as 60 Minutes, Good Morning America, CSPAN Washington Journal, Oprah Winfrey and North Carolina People. He is a frequent public speaker on financial crimes, money laundering and cyber crimes.

Swecker received the prestigious Presidential Rank Award in 2003 for his service in Iraq and as Special Agent in Charge of the NC Office.

About Verafin

Verafin is a leader in enterprise Fraud Detection and Anti-Money Laundering (FRAML) technology with a customer base of over 1000 financial institutions across North America. Verafin is the exclusive provider of fraud detection and BSA/AML software for the California Bankers Association, Florida Bankers Association, Massachusetts Bankers Association, CUNA Strategic Services and has industry endorsements in 44 states across the U.S. For more information, visit www.verafin.com.

Check out www.verafin.com/resource-center for complimentary educational webinars and white papers on hot industry topics.