Tackling the New Wave of Organized Crime

Why staggering fraud losses are still occurring, and what insurance companies should be doing to stem the tide

Featuring

Chris Swecker, retired Assistant Director for the FBI Criminal Investigative Division and former Head of Security for Bank of America
Contents

A Profitable Crime and Growing Threat....................... 1

Why Even the Most Audacious Fraud Rings Have Been Tough to Spot.............................................. 2

- Fraud detection and investigation units operate in silos........................................................................ 2
- Big ears, tiny brains................................................................................................................................. 3
- There’s not a lot of risk for the bad guys................................................................. 3
- Thresholds are high................................................................................................................................. 3
- We’re playing a random game................................................................................................................ 3

What Works................................................................................. 3

- Break down the silos................................................................................................................................. 3
- Find the mules........................................................................................................................................... 3
- Find the links............................................................................................................................................. 3

Closing Thoughts........................................................................ 4

About the Presenter ............................................................... 4
A Profitable Crime and Growing Threat

In late August 2005, Hurricane Katrina hit America’s Gulf Coast, causing an estimated $100 billion in economic damages. Approximately 1.6 million insurance claims were filed, totaling $34.4 billion in insured losses. Of the $80 billion in government funding appropriated for reconstruction, it is estimated that insurance fraud may have accounted for as much as $6 billion.

The total cost of insurance fraud (non-health insurance) is estimated to be more than $40 billion per year, according to the US Federal Bureau of Investigation (FBI). That means insurance fraud costs the average US family between $400 and $700 per year in the form of increased premiums.

And that’s just a sliver of the picture. There’s also health care fraud, identity theft, workers compensation fraud, financial institution fraud and Internet fraud – virtually all have some associated element of money laundering.

It’s hard to put a dollar figure on the magnitude of the risk, because summary statistics don’t exist. “Measuring insurance fraud is an elusive target,” says the Coalition Against Insurance Fraud. “No single national agency gathers omnibus fraud statistics. Insurance fraud data thus are relatively piecemeal, making our understanding of insurance fraud an ongoing work in progress.” And since fraud is designed to be undetected, we can only guess at what we don’t know.

What we do know is that fraud is exploding, both in tactics and losses, said Chris Swecker, a fraud and financial crimes specialist, a 25-year veteran of the FBI and former Head of Security for Bank of America. Speaking at a SAS-sponsored event for insurance fraud managers, Swecker said global organized crime has been radically transformed by two forces: the fall of the Berlin wall and the rise of the Internet. One gave Eastern Europeans and Russians access to new opportunities outside their home countries; the other made it incredibly easy and low risk to do so.

“Virtual criminal networks and Eastern European criminal enterprises now are the most dominant and profitable mafia on the planet,” said Swecker. “Fraud professionals must be aware of this new paradigm and always be on the lookout for links and associations when they address a fraud event. Many financial crimes are really part of a larger group activity and the activity will continue unless the larger activity is shut down.”

The crime strategies of the traditional mafia seem almost archaic now, rooted in the bricks-and-mortar world – activities such as extortion, drugs, bribery, gambling, loan sharking, cargo theft, hijacking and bid rigging. “Even on their best day, traditional organized crime never even came close to the Internet fraud rings and health care fraud rings that operate in the US today,” said Swecker. “In terms of sheer profitability, those guys were replaced by about the mid-’90s.”

“When the Soviet Union fell apart, it unleashed this new breed of gangster, combining a toughness learned in the Gulag labor camps with a street-smart entrepreneurialism” said Mark Galeotti PhD, a Professor of Global Affairs at New York University. A look at the top 50 players in the Russian mob reveals that about half are current or former government officials within the country. Most have access to US markets, and they’ve been in the US quite a bit.

The union between the Russian organized crime and government is perhaps best symbolized by Semion Mogilevich, a Ukrainian-born organized crime boss who is associated with huge companies and a Russian state energy group – and believed to be the leader of the Russian mafia. Mogilevich also has the distinction of being named to the FBI’s Ten Most Wanted list in 2009. The FBI has described him as the most dangerous mobster in the world. He lives in Moscow under the protection of the Russian government, but he has travelled to the US and has colleagues in Brighton Beach, NY, a hotbed of Russian organized crime nicknamed “Little Odessa.”

This new breed of organized criminals started with traditional crimes but quickly figured out where the real money was. Now they focus almost exclusively on financial crime schemes. It’s not surprising, since they came from that background. They understand business processes. They understand economic surveillance – monitoring a system, finding its vulnerabilities, and exploiting them.

“It didn’t take them long to figure out where the vulnerabilities are in the health care system,” said Swecker. “That was one of the first areas they exploited as well as the insurance industry. What’s interesting about these guys is the staggering amounts of losses they inflict. These are long-running schemes that go on for four, five and six years.” For example, the ring leader known as Yaponchik managed to extort $2.7 million from an
investment advisory firm run by two Russian businessmen before being arrested in 1995.

An Armenian-American organized crime ring defrauded the US Medicare system of $100 million through 118 fictitious clinics with addresses in 25 states. In another high-profile case, Mikhail Zemlyansky’s gang made at least $400 million in dirty auto crash-injury claims, according to federal prosecutors. “That audacious money haul is nearly the team value of the Baltimore Orioles,” said Swecker. “It was the largest auto fraud scheme in US history until the gang was broken open this winter.

“There has been a steady drumbeat of these cases, and each case is touted as the largest ever in terms of the amount of losses and the number of defendants indicted. $163 million, $200 million, $295 million, $420 million. The arrests are great moments for law enforcement – nice times to spike the ball in the end zone – but then you have to step back and say, ‘How did these things go on for five, six and seven years without being detected?’

“Making matters worse, Russian organized crime groups were transformed from basic groups with simple tactics of intimidation to highly trained and knowledgeable groups with more precise targeting and a better arsenal of hardware and connections. This transformation occurred as approximately 40 percent of workers from the KGB left government employment. The majority of these former KGB employees either entered the personal protection business – most of whom found work for criminals and the new class of oligarchs – or simply joined criminal groups.”

This trend has given rise to a whole new cottage industry. For example, the remote Romanian town of Râmnicu Vâlcea is thriving on e-commerce scams and malware attacks on businesses, enough to earn the nickname, “Hackerville.”

These transnational crime syndicates are becoming more involved in insurance fraud, according to Steve Barkhuizen, a Senior Manager at KPMG. “It’s a problem that is getting more and more serious as the information age matures. We see the crime rings targeting the companies that do not have an effective fraud fighting strategy that includes the use of technology to detect and resist this activity. Growing symbiotic connections among crime cartels such as drug cartels, terrorists, large scale insurance fraud rings, cyber thieves, crime syndicates, and other players seek sophisticated ways to use each other’s networks and skill sets for mutual profits.” (Source: “Transnational crime gangs make fraud a global epidemic,” Journal of Insurance Fraud in America, Spring 2014, Vol 5, Number 4)

Why Even the Most Audacious Fraud Rings Have Been Tough to Spot

Fraud detection and investigation units operate in silos

Data silos. Technology silos. Component silos. All these silos make it difficult to connect the dots and see collusion or aberrant patterns. There has been some consolidation in the insurance industry, but there’s still much room for improvement, Swecker said.

“When it comes to technology, most every [fraud management] component in the organization goes out and gets the technology they need. They’re not going to sit around and wait for something that’s more integrated and more consolidated enterprise-wide. So you get a patchwork quilt of technologies. A large institution might have hundreds of databases, dozens of components and a dozen or more watch lists that were not consolidated. Even within one organization, you’ll find pockets of anti-fraud activity without knowledge of one another.”

When you have data silos and industry silos - systems and people not talking to each other - a suspicious activity or known fraud might be detected in one place, but you never connect up the larger organization.
Big ears, tiny brains
Even when organizations have a lot of data, they rarely make the best use of it. “Fraud detection and investigation teams have been taking in a lot of data but very seldom connect it up in the way that we need to,” said Swecker. The events of 9/11 are a case in point. Various entities – the CIA, FBI, Department of Defense, local law enforcement – each had pieces of the picture. But those pieces weren’t connected in a way that would reveal the bigger picture shaping up.

There’s not a lot of risk for the bad guys
Fraud represents a heady opportunity with minimal risk, and the criminals are not afraid of US jails. They use extensive system and process surveillance, and continuously test thresholds to learn how to stay under the radar. They are networked and collaborative, making use of insiders and virtual black markets. They are nimble, adaptive and innovative, staying a step ahead of detection and enforcement.

“We most of the time when we’re rolling out new products and services, the security runs well behind the product or the service, and you’re giving the advantage to the bad guys,” said Swecker.

Thresholds are high
“When I was head of the FBI’s criminal division, starting in around 2005, we wouldn’t investigate a case unless it was up around $500,000,” said Swecker. “Individual fraud cases generally don’t get prosecuted in federal court, not necessarily even in state court. You pretty much have to bundle up that fraud and put a bow on it” for a prosecutor to take an interest.

We’re playing a random game
“We continue to play a game of Whack a Mole with the approach of taking the next fraud case out of the queue, addressing that fraud case, and then not spending at least some time and resources on linking together and looking for clusters of criminal activity,” said Swecker. “We’re still using the manual tools, and we’re not prioritizing the cases based on the amount of loss involved and the reputational risk of these types of cases. … The insurance industry is light years ahead of health care, the financial sector and government benefits in this, but there’s still a lot of manual detection taking place.”

What Works
Break down the silos
Consolidate multiple data sources to enable a bigger-picture view. Use entity resolution and matching to find previously unknown links. Clean, high quality data is key to detecting, triaging and investigating suspicious activity that may involve organized crime.

Once fraud is detected and assigned, you can benefit from a shared case management system. Serving all fraud components in the organization, this shared case management system sits on top of the same data, looks at the same historical alerts, and looks at the same internal data you have available. A caveat: “Often what people call case management is simply a case retrieval or case inventory system,” said Swecker. “You can’t mine the data. You can’t manage the workflow. Case management means a lot more than being able to pull up a case and look at the notes.”

Find the mules
“Even in white-collar crime, you have to have mules and smurfs, the ant army of little foot soldiers that go out and actually do something,” said Swecker. There’s your opportunity to hook into the larger criminal enterprise. “Somebody has to stage the accident, be in the accident, take the credit card number and cash it in, buy gift cards, clone the card, and so on. They have to show up and give you data – an address, phone number, cellphone number, email – and that’s where I think we have an advantage. In fact, in the financial services industry, we’re beginning to concentrate almost exclusively on the mules. Once you’ve identified a group of money mules, you now have something tangible that you can take to law enforcement. Then let them work their way up the chain.”

Find the links
Swecker told a story of a Medicaid contractor who billed for performing 85 proctology procedures on a single patient in 20 months. Ouch. “Give me a break; that didn’t get detected by someone?” said Swecker. “Across all of these different Medicare and Medicaid contractor systems out there to detect fraud, no one picked up this. It was actually caught on a tip.

“What we’re doing is detection without context. We need to make those links to identify the malignant social network, and prioritize the linked activities over the singular, one-off, opportunistic fraud that takes place every day, which isn’t as good a use of our resources. Law enforcement can take it
further down the line, but we all know, we’re not going to get a case prosecuted – we’re not going to get that deterrent value - unless we have a network of criminals to take to the FBI, Secret Service, postal inspectors or local law enforcement.”

Here’s a prime application for link analysis, a semi-automated process of modeling relationships between entities. Entities may be defined as locations, service providers, phone numbers and vehicle identification numbers—to name just a few. Tools can be tuned to display link frequencies that exceed a programmed threshold. Large volumes of seemingly unrelated data can be checked, and then patterns and problems identified.

For example, link visualization might show a high-activity account with links from many accounts, or a low-activity account with strong links to a master account. It might reveal multiple claims in a short period of time from related parties, such as members of a single family. Or the classic ring pattern associated with staged accident scams.

Fraud investigators can search across a full customer base of claims, policies or accounts in seconds, and turn up visual indications of connections and overlaps among them. A skilled analyst can then assemble more pieces of the puzzle.

“In a pilot for a large bank, we pooled all the data we had available, consolidated from dozens of databases, then brought SAS in and had them do some link analysis to look for fraud rings,” Swecker said. “Within a couple of days, we had identified 40 fraud rings that the bank was just completely blind to until we did that data analytics. If we’d had this kind of firepower when I was working the streets at the Bureau, my hair wouldn’t be as gray as it is now.”

Closing Thoughts

Bring the data together. Make the links. “Data is a valuable commodity. Data that transcends silos can be mined like gold,” said Swecker. “Data is where we can make those links. When we found the 40-plus fraud rings in that short time period, it was almost so simple. The connections were identified through common addresses, common bank accounts, and common email addresses and cellphone numbers.

“We had overlooked the simplicity of some of this, just working with the data that we have. And there is a lot of rich data we can add to it, merging public and private data. If you can compile a database of historical cases, such as suspicious activity reports (SARs), indexed properly, that becomes your anchor data. When you start linking that out, you’re linking to something that’s already known to be fraudulent.

The National Insurance Crime Bureau (NICB) certainly believes in link analysis, devoting close to 200 analysts to detecting rings. If your fraud unit assigns even one analyst to the task, it will make a difference, said Swecker. “Any resources you devote toward making the links on these criminal networks is time well spent. The insurance industry is ahead with the best example of a consortium approach – an industrywide approach to fraud detection, going after the groups that are inflicting the most damage.

“These fraud operators are like apex predators. Nobody is really proactively hunting them down. They’re operating in the comfort zone, with very little risk. Maybe we can turn the tables. Maybe we can inject a lot more risk into that environment by going after them as an organizational structure rather than taking the next one-off, opportunistic case off the queue. Maybe we can find them and hunt them down, instead of waiting to be the next victim.”

About the Presenter

Chris Swecker started his career as a prosecutor in North Carolina, which included handling fraud cases. In 1982 he began a 25-year career with the FBI, ultimately heading up criminal investigations as Assistant Director for the Criminal Investigative Division and Acting Executive Assistant Director (EAD) for Law Enforcement Services. He then took his FBI experience to a position as Head of Security at Bank of America, which included physical security, anti-money laundering, executive protection and background screenings as well as fraud investigations.

Swecker is a consultant and attorney specializing in public speaking, commentary, advice and solutions in areas of financial crimes, organized crime, cybercrimes, security and anti-money laundering. He also provides whistleblower legal representation under Dodd-Frank, Sarbanes, FDIC and OSHA laws and regulations.