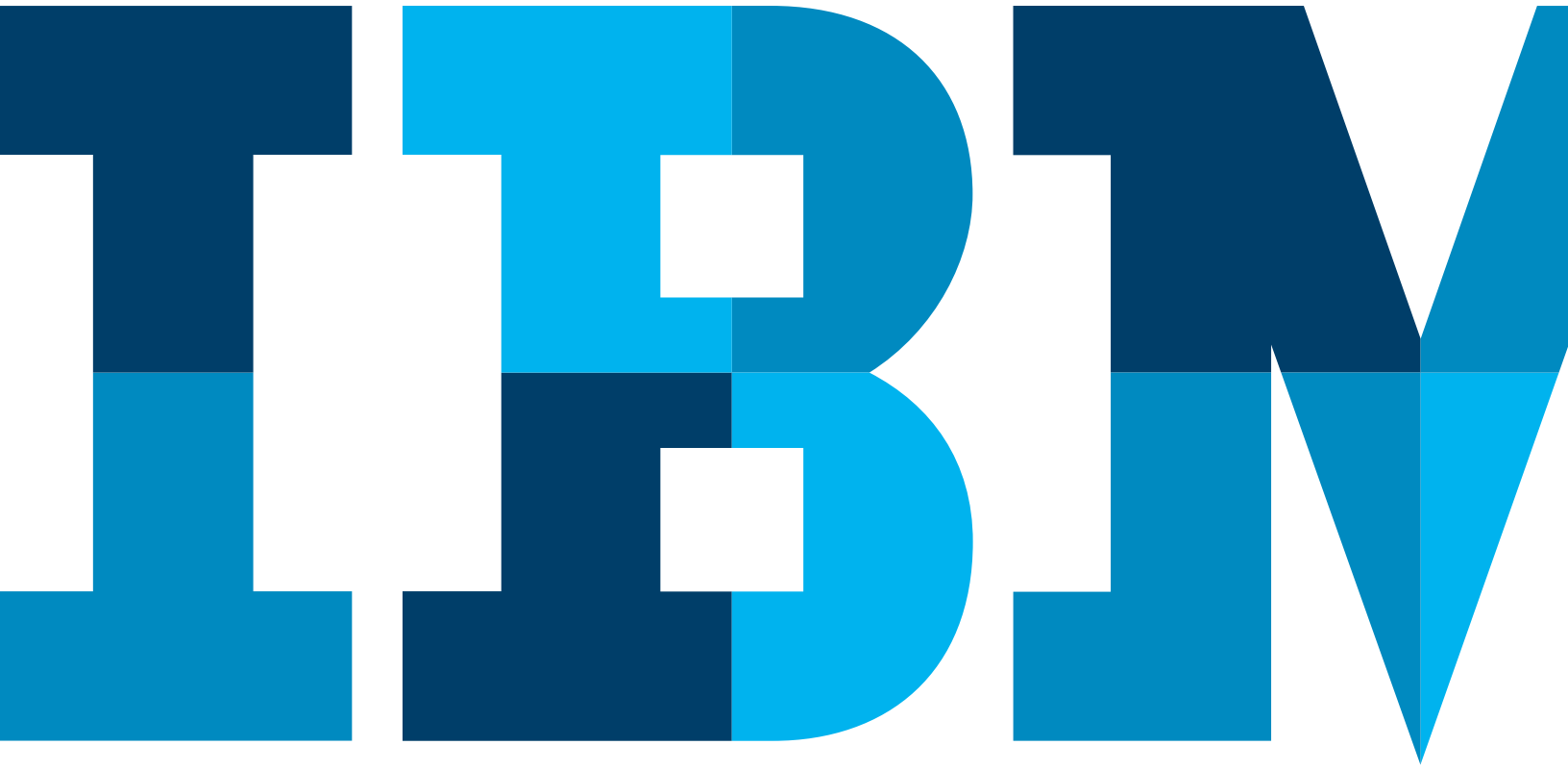
Insurance Fraud and Organized Crime

An IBM thought leadership paper by Brooke C. Satti



IBM

Contents

Introduction

Insurance fraud is big business, white-collar crime with an estimated loss of USD30 billion per year. The FBI reports that "in most cases, it's dishonest policyholders, insurance industry insiders (i.e.[sic] agents, brokers, company execs[sic]) and loosely organized networks of crooked medical professionals and attorneys who use their knowledge to bypass anti-fraud measures put in place by insurance companies" (FBI, Federal Bureau of Investigations, 2012). In addition, "Organized crime rings across the globe have been diversifying into sophisticated forms of crime" (Thomson Reuters, 2013) with a focus on insurance fraud.

Industry trends

Organized crime families such as the Cosa Nostra, Italian crime families in the US and Sicily, along with Russian, Mexican and Albanian mafia families have been found in a number of recent crime ring investigations. These organized crime rings are targeting insurance companies for several reasons:

- *Competition between insurance companies*. "…fierce competition between insurance companies drives many companies to pay claims as quickly as possible, which makes it extremely difficult to recover money that has been paid out for bogus claims." (Thomson Reuters, 2013)
- *White-collar crime*. Insurance fraud is "more lucrative, less dangerous and [poses] lower odds of being caught." (Jay, 2012).
- *Internet*. The internet is the easiest method for "communication, information sourcing, marketplace, and recruiting." (EUROPOL, 2011)
  - The purchase of an insurance plan and submission of a claim can all be found and filed online;
  - Criminals use the Internet as a gateway to Personally Identifiable Information (PII)[1].
- *Prolonged Pursuit*. Organized crime rings are able to file multiple claims, often making millions of dollars in profits before they are caught. Many crime rings are able to stay under the investigative radar for years.
- *Investigation Issues*. Insurance companies run into a number of issues when trying to investigate these cases effectively. "Lack of IT Resources; Demonstrating ROI (Return on Investment); Acquisition and integration of data; Legal and compliance issues; and Lack of proof that new technology will be effective." (Thomson Reuters, 2013)

An organized crime ring identified in Miami, Florida, purchased numerous insurance policies online. The criminals used stolen, unauthorized credit card information and electronic bank checks to facilitate their crimes. Investigators identified the ring through their use of common email addresses used to purchase multiple policies. The investigators linked the policies to staged automobile accidents and false claims that the crime ring made with the help of shady clinics.

Clearly, the Internet makes insurance fraud an easy crime for any fraudster to commit. For criminals to perpetrate online insurance application fraud, fraudsters must complete several steps.

Identity theft. Fraudsters purchase stolen identification to submit fraudulent applications and stage false claims. Fraudsters purchase most of their stolen customer information from deep Web marketplaces such as Agora Marketplace, Hydra Marketplace along with the now infamous Silk Road. These sites are only accessible with the use of The Onion Router (Tor)[2]. (Tor allows users to anonymously access information in the deep Web.)

Payment fraud. Fraudsters use stolen credit cards, debit cards and checks to purchase new identities and policies mostly from the same deep web marketplaces.

Email addresses: Fraudsters tend to use the same email address to perpetrate multiple crimes. Email addresses are easy and cost nothing to create. In addition, no-cost email addresses are easy to dump when no longer needed. With same email address that was used purchase a stolen identity, a fraudster can complete an online insurance application that is the insurance company provisionally approves. Usually, fraudsters pay the application fees with a stolen credit card or fraudulent check. The insurance company provides provisional proof of coverage upon submission of the application. Proof of coverage is sent to same email address. To collect on a claim later, such as a bogus auto accident, proof of insurance is required. Ultimately, the insurance company rejects the charges, but by that time, the fraudster has already obtained proof of coverage.

Once these steps are completed, the fraudsters can begin the next phase of their scheme to begin making fast, easy money.

Organized crime ring insurance fraud

A Bulgarian organized crime group, with ties to the Russian mafia, Serbian mafia, and the Italian Cosa Nostra, creates security and insurance front companies to mask their criminal activities. A mafia clan in southern Italy stages hundreds of fake cars crashes every year to gain millions of in insurance payouts. An Armenian organized crime group with connections to the Russian mafia perpetrates healthcare fraud using their ownership and operation of Family Chiropractic Center, Inc. These activities are all examples of how organized crime groups target the insurance industry.

Here are the most targeted insurance types with recent examples of how organized crime groups submitted fraudulent claims for monetary benefit.

Automobile theft. There are many types of automobile theft fraud scams, but the most common scams are found in crime rings involving overseas transactions without proper paperwork and undocumented sales with body shops. In both instances, the cars are reported stolen after they leave the US, or are disassembled and sold for parts.

"In June 2010, law enforcement officials announced indictments of 17 participants in an alleged scheme that pilfered 450 cars annually in New York, New Jersey, and Connecticut. According to law enforcement officials, the group, described as a "steal to order" outfit by New York State Attorney General Andrew Cuomo, filled specific requests from US customers and others in Senegal and netted up to USD25,000 per car. The group supposedly relied on specialists who could reprogram car keys to match a vehicle's specific code, exporters, and two car dealership employees, among others. The ring allegedly stored vehicles in four Bronx, NY, garages and loaded those automobiles destined for Senegal into shipping containers, concealing the cars behind furniture." (Jerome P. Bjelopera, 2012)

In December of 2013, 18 individuals were charged for their roles in a luxury automobile theft ring known as "Operation Tidal Wave." This ring was responsible for the theft of 48 high-end vehicles valued at approximately USD2.4 million. Automobiles were taken directly from dealerships and were later linked to vehicles in Israel and the United Arab Emirates. Each ring member had a specialized role in the operation. The group had designated thieves who stole the vehicles and fed the stolen cars to the brokers. People referred to as taggers supplied packages for stolen cars that included VIN stickers and license plates Designated brokers obtained cars from thieves and sold them on the black market. Title washers provided forged titles for the stolen vehicles; and black market dealers sold the tagged and washed vehicles to local and out-of-state buyers" (Weekly, 2013). It is unclear if these ring members were direct members of a Mexican organized crime group. However, during the investigation, law enforcement seized more than 20 kilograms, or 44 pounds, of cocaine upon its delivery to New York by way of California from the Mexican border crossing. Its street value was estimated at more than USD1 million.

Car Accidents and Damages. Staging automobile accidents to collect on premiums; inflating damage sustained to a vehicle to collect higher premiums and claimed that more vehicles were involved in an accident to receive larger payoffs. This ruse requires multiple bad actors such as drivers, insurance investigators and bystanders.

Philadelphia mobster, Ronald Galati, ran an elaborate insurance fraud scheme through Galeti's auto body shop. This highly lucrative auto crash ring would claim damages or accidents to previously damaged cars. In addition to Galati, the ring included auto body-shop employees, tow-truck operators, a Philadelphia police officer and two insurance adjusters. The body-shop employees went to great lengths to make these claims appear real by collecting and storing deer blood, hair and carcasses as props in photos submitted with the bogus insurance claims. Prosecutors allege that the deer carcasses were not the only props used. "There were geese and dogs and chunks of metal and concrete, as well as hurtled cartons of fruit." (Slobodzian, 2014) Galati's scheme predominately submitted single-vehicle accident claims because insurance companies classify these accidents as no-fault claims and pay the claims without raising premiums. In addition to this scheme, Galati would also make copies of vehicle's keys brought into Galati's shop for legitimate repairs. An accomplice of Galati would later locate these cars on the street, steal the cars and crash them. These actions created more work and potential insurance paydays for Galati's auto body shop.

The United Kingdom's, Mohammed "Mojo" Rashid ran an organized crime scheme known as Crash for Cash. Rashid began to orchestrate and report false, staged, or inflated accidents to insurance companies to receive greater payouts. As a government-certified accident claims manager, Rashid recruited people to join the fraud ring. Rashid was sentenced to five years in prison and forced to repay the government an estimated GBP150,000.

Health insurance fraud. Corrupt and fake medical practices send insurance companies inflated bills for standard procedures, or for procedures that didn't occur. These practices are known for creating and filing false billing for medical equipment, medical prosthetics and prescriptions. Another tactic is to inflate bills using a billing code for expensive and unnecessary procedures. Often, this scam occurs with staged auto accidents with the intent to collect personal injury collection benefits. Criminals target both private industry or government run organizations.

The Coalition Against Insurance Fraud states that the US spends more than USD2 trillion on healthcare annually.

Fraud amounts to between USD125 billion and USD175 billion annually, including everything from bogus Medicare claims to kickbacks for worthless treatments and other services. (Reuters).

Government healthcare and Medicare fraud

Affordable Healthcare Act fraud

This scheme sprouted from faulty technology in the healthcare.gov enrollment tool.

The recent creation of the Affordable Care Act, (ACA) has opened up millions of Americans to identity theft and fraud, also known as ACA fraud. Individuals who enrolled in healthcare via the healthcare.gov might have gotten more than they bargained for. It is old news that the system had issues, "….healthcare.gov is unstable — at times denying people access, terminating communications mid-session, or crashing entirely. Buggy systems often provide criminals the opportunity to exploit glitches to gain unauthorized access, read data, and even modify code executed during subsequent user sessions" (Steinberg, 2013). The media reported that organized crime groups and opportunistic fraudsters began bombarding potential victims with emails and phone calls in an attempt to trick or socially engineer them into giving them their social security number, bank number or other types of PII.

After a 69-year old Ohio man signed up for healthcare via healthcare.gov, he became a prime target for fraudsters. The man began receiving spam emails by the dozen and even received a phone call where a "convincing-sounding man claiming to be from the national Medicare office [informed him] that he was ready to send him a new Medicare card but first needed to verify the 69-year-old's identity — by asking for his bank account number." (Hunt, 2013)

Medicare fraud

Medicare fraud is the act of collecting Medicare healthcare reimbursements under false pretenses.

- Total amount of Medicare fraud is unknown
- Estimated fraud losses are upwards of USD48 billion
- Annual Medicare spending is upwards of USD500 billion

Konstantin Grigoryan was indicted of stealing doctor's identities in a Medicare Russian-Armenian organized crime ring. The scheme profited more than USD20 million through a group of medical clinics they ran in the Los Angeles area. Grigoryan and accomplices would recruit fake patients for unnecessary medical treatment and then bill the agencies for the services. The ring would create fake test results to ensure that the patient files would pass if audited by Medicare.

Similar Russian-Armenian rings aggressively pursued elderly patients, pressuring and intimidating them into providing their Medicare numbers. The group also broke into banking systems and paid corporate insiders to provide key information from court and various other government agencies.

Eleven members of New York's Bonanno family were indicted in a Medicare fraud scheme in South Florida. They stole Medicare ID numbers and submitted false claims.

Christopher Iruke and his wife Connie Ikpoh, both from Nigeria, were charged with owning fraudulent medical equipment supply companies and defrauding the government via Medicare of USD14.2 million. The husband and wife team used documents and prescriptions for high-end medical equipment such as high-powered wheel chairs and orthotics and would bill Medicare for the cost.

Private healthcare fraud

Coalition Against Insurance Fraud released these statistics on their website:

- Every USD2 million invested in fighting healthcare fraud returns USD17.3 million in recoveries, court-ordered judgments plus bogus claims that weren't paid and other anti-fraud savings. (*National Health Care Anti-Fraud Association, 2008*)
- The average health insurer's anti-fraud investigative unit has an annual budget of slightly more than USD1.9 million and 19 full-time employees. (*ibid*)
- The average health insurer has 363 open cases in 2007, and each insurer investigation unit handled an average of 791 cases total for 2007. (*ibid*)
- More than seven of 10 insurer investigative units use fraud-detection software. (*ibid*)

Operation Sledgehammer: In May 2013, law enforcement officials arrested 26 people in Dade and Palm Beach counties in Florida for involvement in an insurance fraud ring where the defendant allegedly staged auto accidents to collect personal injury protection benefits. Those [persons] arrested are charged with having billed more that USD20 million to insurance companies over a three-year period." (Thomson Reuters, 2013)

A Russian crime ring in New York City involving 10 doctors, nine health clinics and 105 different corporations planned to defraud insurance companies for more than a quarter billion dollars. The ring focused on New York because they are a no fault state under insurance law. For New York registered vehicles, insurers pay to pay up to USD50,000 per person in the vehicle who experienced injuries from accidents, regardless of who was at fault for the accident. The charges brought on to this ring include "conspiracy to commit health care [sic] fraud, mail fraud and money laundering." (RASHBAUM, 2012)

Home, fire or vandalism fraud

False reports of break-ins and vandalism or actual fires started for the collection of premiums.

One example of this type of fraud is Operation Leaky Pipes. In February 2014, around two-dozen people were arrested and charged after officials identified a major home insurance fraud ring in South Florida's, Miami, Dade County. The crimes committed included a fraud type known as "Flames and Floods" where the offender uses both arson and deliberate flooding to defraud various insurance companies.

Client needs and challenges

Insurance fraud has existed since the creation of the first insurance policy. Organized crime rings emerge and view this type of fraud as an easy, white-collar, more lucrative and less dangerous way of obtaining millions of dollars in cash. While insurance companies are continuously investigating fraudulent claims, they face the challenge of providing their management with favorable return on investment (ROI).

Insurances schemes victimize the law-abiding individuals and corporations they intertwine in their illicit money making process. Large criminal rings and individual criminals alike take similar steps in accomplishing fraud. Staying abreast of this type of information helps investigators discover these crime rings sooner.

Both entities watch global market trends. Organized crime rings run their organizations like a business and follow global trends like any other business or for-profit organization does. Are there requests increased for scrap metal overseas? Does this trend coincide with an increase in insurance claims on stolen or crashed cars?

Many organized crime rings have ties overseas in both legitimate and black market. When there is a specific desire for luxury cars in a certain region, organized crime groups shift their operation to meet that demand. In some cases, the organized crime groups use their own cars (purchased legitimately or illegitimately) and ship the vehicles to locations where they can sell the vehicle for well over the asking price. These crime groups would report their cars as stolen to the insurance company. The insurance company then pays fair market value for the vehicle. Claims departments and investigators watch these global trends to help isolate spikes in fraud from true claims.

Both entities use technology to their advantage. Business uses technology to reduce fixed costs and make transactions more convenient for the customer. Fraudsters can use that same technology negatively to help facilitate nefarious activity.

Purchasing policies, reporting a false claim, or overbilling a medical expense, and so on, are all processes available online. Claims and investigative units can also use technology to their advantage by creating strategies that monitor similar claims data such as email addresses (used both for opening policies and for reporting claims), IP addresses, auto body shops and medical practices. This link analysis helps unravel the fraudulent claims and facilitate the identification of the unknown unknowns much faster.

Organized crime operations are large. "Increasingly, large, complex crash rings are run by organized crime, often ethnic groups including Russians, Armenians, Estonians, Latvians and various Spanish-speakers, either domestic or tied to organized crime in their home countries." (Insurance Fraud NEWS, 2014) These large rings tend to use the same people over and over to perpetrate their fraud. Watching what body shop is reporting the damage, what medical clinic is requesting patient care (and the degree of care), the name of the officer who filed the claim, and other data. These data points are all important, relevant factors. Often times a little investigation, uncovers a more significant problem.

The vulnerable are always at risk. Fraudsters target the vulnerable. "Whether it's disaster-stricken homeowners desperate to put their world right again or immigrants unclear on the ways of insurance, fraudsters prey on the vulnerable. Staged accident rings for extortion often happen in places like Los Angeles target drivers in Hispanic or Korean neighborhoods. Fraudsters deliberately hit cars on foot or on bikes then demand money on the spot in return for not reporting the accident. The Russian-staged accident rings in New York have "runners" or "cappers" who recruit legal or illegal immigrants to claim injury and collect medical treatment from unethical clinics. Unfortunately, sometimes these people end up injured or dead in staged accidents gone awry." (Insurance Fraud NEWS, 2014) Companies need to train their employees on how to watch for the vulnerable clients.

Conclusion

Organized criminals and lone fraudsters are continuously adapting to the ever-changing world we live in, using everything at their disposal to commit their illicit activity. Financial Institutions and investigation teams need to be more flexible and adapt as easily as the fraudsters. Additionally investigators need to be prepared to go undercover and maneuver in the deep web marketplaces to position themselves in a proactive state. Through communication and investigative sharing, both enterprise and industry-wide, financial institutions and investigative teams can work together to help detect crime rings and prevent future fraud.

For more information

To learn more about IBM solutions for insurance fraud prevention, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/analytics/solutions/threat-fraud/fraud-prevention/

Bibliography

EUROPOL. (2011). Threat Assessment - Internet Facilitated Organized Crime. EUROPOL Public Information. EUROPOL.

FBI, Federal Bureau of Investigations. (2012). Investigating Insurance Fraud - A $30-Billion a Year Racket. Retrieved 4 25, 2014, from FBI: http://www.fbi.gov/news/stories/2012/january/insurance_013112

Jay, D. (2012, July 10). Property Casualty 360. Retrieved April 25, 2014, from Organized, Violent Criminal Empires Target Insurers: http://www.propertycasualty360.com/2012/07/10/organized-violent-criminal-empires-target-insurers

Jerome P. Bjelopera, K. M. (2012). Organized Crime: An Evolving Challenge for US Law Enforcement. Congressional Research Services. Congressional Research Services.

Thomson Reuters. (2013). Detecting And Investigating The Growing Presence Of Organized Crime In Insurance Fraud. Thompson Reuters.

Insurance Fraud NEWS. (2014, May 28). Top five strategies outlined for insurance fraudsters . Retrieved from Insurance Fraud NEWS: http://www.insurancefraud.org/IFNS-detail.htm?key=18789#.U8bG0aPD_Gg

RASHBAUM, W. K. (2012, February 2012). New York Times. Retrieved from The New York Times: http://www.nytimes.com/2012/03/01/nyregion/dozens-said-to-be-arrested-in-health-care-fraud-scheme.html?pagewanted=all&_r=0

Slobodzian, J. A. (2014, May 30). Retrieved from Philly.com: http://articles.philly.com/2014-05-30/news/50185714_1_insurance-companies-philadelphia-grand-jury-south-philadelphia

Weekly, T. N. (2013, December 19). Retrieved from Times News Weekly: http://www.timesnewsweekly.com/news/2013-12-19/Crime_(and)_Cases/Cops_Bust_Made_To_Order_Luxury_Vehicle_Theft_Ring.html

Hunt, A. (2013, November 11). Scams sprout with rollout of Obamacare. Retrieved from USA Today: http://www.usatoday.com/story/news/nation/2013/11/11/affordable-care-act-scams/3501595/

Steinberg, J. (2013, October 30). Is Healthcare.gov An Identity Thief's Dream Come

True? Retrieved from Forbes: http://www.forbes.com/sites/josephsteinberg/2013/10/30/is-healthcare-gov-an-identity-thiefs-dream-come-true/

Insurance Fraud NEWS. (2014, May 28). Top five strategies outlined for insurance fraudsters . Retrieved from Insurance Fraud NEWS: http://www.insurancefraud.org/IFNS-detail.htm?key=18789#.U8bG0aPD_Gg

Coalition Against Insurance Fraud: http://www.insurancefraud.org/index.htm#.U-E0aqPD-gc

IBM Corporation
Software Group (or appropriate division, or no division)
Route 100
Somers, NY 10589

Produced in the United States of America
September 2014

1 PII is information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context.

2 Free software for enabling online anonymity and resisting censorship. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than five thousand relays to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis.

Please Recycle

KIW12345USEN-00