THE FUTURE OF FRAUD:
FRAUD EXAMINATION TECHNIQUES BEYOND 2015

Fraud examiners are experts in helping organizations prevent fraud based on known risks and previous fraud cases. However, the future poses many challenges as fraudsters are reinventing how fraud is committed and learning to take advantage of security vulnerabilities. Information fraud has increased in the last few years, and many of those cases were perpetrated by fraudsters from outside the organization. Fraud examiners are currently using more data-driven investigations tools and analytics to identify fraud and fraudsters based on existing fraud cases rather predicting future fraud schemes. This session will explore recent fraud trends and how fraud examiners need to prepare themselves to uncover fraud in the future.

You will learn how to:

- Identify fraud opportunities created by the complexity and technological advances in organizations.
- Recognize the ways in which fraudsters have reinvented old fraud schemes for the information age.
- Develop the skill set to uncover future fraud cases.

IYAD MOURTADA, CFE, CIA, CMA, CCSA
Managing Director
OpenThinking
United Arab Emirates

Iyad is an international speaker, trainer, and consultant with a diverse background in internal auditing, risk management, and fraud examination. He has taught many unique auditing and fraud-related courses to international corporations and government entities. His innovative and creative teaching approach proved to be effective in adding value to the learning process of more than 10,000 professionals in the last eight years. Iyad is the general manager of OpenThinking, a leading business training company in Dubai. Additionally, Iyad is an authorized trainer with the ACFE, where he teaches the *CFE Exam Review Course*, and he is listed as a global public speaker on the IMA Speaker's Bureau.

The Future of Fraud:
Fraud Examination Techniques Beyond 2015
Iyad Mourtada

The Pioneers of Fraud:

Fraud existed since the beginning of humanity. One of the documented financial fraud incidents was in 300 B.C. when Hegestratos, a Greek merchant, bought a large insurance policy on a cargo boat. Then he sent the boat to the ocean empty and tried to sink it to claim for the insurance money. However, when his crew discovered his plan they throw him out of the boat to die in the ocean.

Fraud schemes and fraudsters had evolved significantly in the last 5 years. External fraud from outside the organizations is costing many organizations more than internal fraud. The latest report from the experts at the National Criminal Intelligence Service says organized crime will become more sophisticated and networked in the near future. Based on the latest report from Norton/Symantec Corp, Cybercrimes are global costing organizations more than $114 billion annually.

Fraud Schemes and Trends:

Fraud examiners are experts in understanding how fraud can be conducted inside the organization and how they can help the organization flight against existing fraud. However, they don't have a full understating of how future fraud is affecting the organizations.

Especially that these future threats are coming from outside the organization.

Fraud used to be conducted by one person or small groups of people targeting one individual or an organization. However, recently we had seen more organized crimes that were done by rings and criminal organizations collaborating overseas. Now and in the future, fraud had moved from one-to-one and then many-to-one to many-to-many. Fraudsters are using high tech and advanced platforms to launch massive attack targeting millions or victims and they are doing it on large scale. It is gone the old days where a hacker spends hours trying to hack a personal account or laptop. Now organized hackers are working together to hack large datacenters and compromise millions of valuable financial, healthcare and personal information.

Fraudsters are adjusting their old tricks to new ones by taking advantage of the advance of technology. You can see how organized crimes are done using the same traditional channels that used before like phone, SMS, emails, websites but their tools, methods but the approaches had been evolved with the technology. Fraudsters are currently using automation to be able to target more victims and they are even investing in an advance fraud technology to be able to stay 10 steps ahead of security measures of their victims.

Welcome to the Information Revolution:

As we are living the information revolution, our information are bought and sold daily in the black market and the more interaction and engaged we are in the web the more door we are opening to hackers to gain access to more information about us.

Organizations should move from simply trying to predict if certain fraud may happen or when can happen and focus more on what controls they have in place to over come the fraud risks and deal with their consequences.
Information is the most valuable assets in the organization and they don't need to be missing when they are stolen. How can fraud examiner know when someone stole valuable information from your organization and how can they proof it.

Internet of Things:
Our world is more and more connected with the Internet and servers on the other side of the world now control many internal systems. This created new vulnerabilities, as organizations don't have complete control over its fraud risks. If a breach or virus attacked one your partners, venders or customers, your system maybe affected, as they are all connected. Sometimes it will be to late to take action as with information, the data had been already compromised.

This can be done on a large scale like some criminal control the traffic system of a city or on small scale where a hacker can hack to your home

system, turn on your TV camera and podcast your living room for the whole world to watch.

The fast moving smart technology are invading our like. Amazon's ECHO, a voice command device and JIBO, The World's First Family Robot, as well as many other smart electronics are connected with our lives 24 hours to understand our personal habits and preferences and make decisions on our behave sometimes. Imagine what can happen when someone other than you can control them.

Welcome to the Deep Web:

If you think that the Internet is the place where action is taking place, think again. 90% of the information on the web represents database that are privately protected and not searchable. However, underground hackers and many cyber experts can hack to these highly secured system and obtain information or destroy others.

Fraud examiners sometimes need to work with experts who had access to the Deep Web to be able to gain some information that are useful in understand the source of hacking or how is the broker who is selling the stolen information. However, they should be very careful not give so much information about the organization system and weaknesses.

Forensic Data Analytics (FDA)

It used that fraud examiners Search for a needle in haystack to uncover the fraud, now fraud examiner have to search for a needle in needle

stack. How can fraud examiners understand the system of the organization to build red flags triggers to prevent or catch unwanted fraudulent transactions.

As the organizations are tying to stay one step ahead of the fraudsters, some of them are using now computer systems to perform tasks that typically require human intelligence on massive scale to perform. Such as, language translation, speech recognition, and decision-making. Artificial intelligence applications are flexible and adaptable to new business conditions as they learn from experience and able to process massive amount of data simultaneously.
Fraud investigators can't relay 100% on the results of artificial intelligence applications as they may not connect all the dots or miss connect the dots. They should always analyze the results before depending on them.

A Question of Trust:

Fraud is based on the violation of trust. So, first for fraudster to do fraud, they need to earn your trust and then they can execute their well-designed evil plans. They are generally pushing two weak points to break into your cycle of trust. First through what we call it psychological vulnerabilities. For example, after you check to a hotel someone will call you, as if they are from the front desk, to confirm your credit card numbers. You will for sure trust them and give them your card information to discover just one hour after or several weeks later that

your credit card information had been stolen. The second weak point is technical weaknesses. For example, let's say that you check into the hotel and then you want to connect online, you see the something like "FREE Hotel WiFi". So you connect to it even that you know the Internet in the hotel is not for free. Then once you connect a webpage will appear asking you to provide your hotel room number and full name and promise you with a free fast WiFi. You for sure enter your information and move on. However, the one thing that you don't know that all your activities on this connection is now monitored by the middle man who is offering you this masked free WiFi under the hotel name.

A Question of Privacy:

We are living a new social experience that opened up our live to the World Wide Web widely. Every movement and interaction we have in real live is being tracked with our permission and shared freely with everyone and we love it. More connection means more influence as well as more vulnerability.

It is easy for anyone to get driven by online offers. They just ask for simple information to allow you to access a website or join a network or worst, they request for you to give them access to your information on Social Media Network such as facebook to sign it to their website. This is just the start for them to buy you. At this point for them you are the product not the customer. You are paying for all the free services you are getting online for free. When you share a post on facebook or post a photo on Instagram. They are vary valuable information that can tell a

lot about you for those we are willing to pay money to know more to sell you more or attack you better.

The World of Code:

Everything thing around us is now controlled by code. When they had built the Internet, codes were used as the language that allows machines to communicate. As such, instructions from one machine to anther can be executed based on these codes. Once someone is able to control these instructions, they can control everything. For example, it someone is able to control the code responsible for your mobile battery, they overheat the battery remotely to a degree where your mobile may explode inside your pocket.

The Future of Fraud:

Payment Fraud is not going away anytime soon. Even that Chip-and-PIN is moving to be the standard for consumer transactions and many transition are now performed with through secured smart phone. We can see that fraud will simply move from the financial system to the telecommunication channels and it is expected to be more than before.

Recent survey about BYOD (Bring Your Own Device) indicated that 73% of C-suite executives and IT pros say that BYOD presents the greatest security risk to their organizations. Personal devices can be compromised and they can create a backdoor for attackers to gain access to the organization's network and system.

The value of medical records medical records can be more than 10x premium over personal and financial records. This created pressure on healthcare providers to add more security measures to stop social engineers who are impersonating patients or doctors to get access to private healthcare system.

Hidden in Plain Sight:

"It is always wise to look ahead, but difficult to look farther than you can see." - Winston Churchill

It is most of the time to late to do anything after you discover that data breach happened or your system had been compromised. This is why it is important for fraud examiners to start thinking in a new approach. Preventive and detective controls are great. But there is always a control risk that they are now present and functioning. As such, new controls need to be in place, I call them Investigative/ Monitoring Controls. They are not operational controls but rather informational controls that feed fraud departments with clues and red flags about some unusual activities inside the organization that can lead to potential fraud case. For example, monitoring traffic volume of the organization server can reveal that over the weekend at 4:00 AM there are some unusual many attempts to connect with the server from unknown location. This is not a fraud but rather a warning sign that saying that maybe someone is trying to gain access to the organization's system.

Organizations need to monitor its big data to be able to predict future fraud by its employees, venders, customers and outsiders and act quickly to stop before it is to late.

Carbanak: $1bn Bank Robbery

Over two years, multinational gang of cybercriminals from Russia, Ukraine and other parts of Europe, as well as from China were able to steal up to $1 billion by attacking up to 100 banks, e-payment systems and other financial institutions in around 30 countries.

It was all started by first gaining entry into an employee's computer through phishing, infecting the victim with the Carbanak malware. Then they were able to access the internal network and reach the administrators' computers for video surveillance. This allowed them to see and record everything that happened on the screens of staff who serviced the cash transfer systems. This allowed them to know the full detail of the bank employees' work in many banks globally.

Technographics Profile:

People leave digital footprints behind them while they are interacting with the digital world. Online activities of users can reveal many hidden interest and intent that people don't communicate in the real life but rather share in the digital life. Understanding what people are following on twitter, what post they like and share, what photos they share and which social media they join can give fraud examiners clues about them and by analyzing their online interaction and communication, fraud examiner can identify their digital profile.

Digital Body Language is the aggregate of all the digital activity of an individual. Fraud examiners can read behind the lines in the emails and digital communication to understand what is being said and why it is been said. This especially important as the only thing that can fraud examiner evaluate is the digital evidence left by the fraudsters.

Information Recovery:

Fraud examiners need to gain more negotiation skills to be able to deal with cyber criminals and negotiate a deal with them. It is not always possible for organizations to take action and arrest the criminals who stole the private information of the organization. Sometimes, organizations have to deal with the brokers who are selling these information in the Deep Web and be able to recover the stolen data to stop the bleeding. As such, Fraud examiners are now working with the IT team who are finalizing such deals to be able to ensure the success of negotiation.

This was the case when Symantec, the maker of Norton AntiVirus, negotiated a $50,000 deal with the hacker, who comprised 1.27 gigabytes of the source code of its security software, to stop him from posting the data online.

Working Together to Flight Fraud:

Organizations from the same industry as well as professionals in the anti-fraud industry are now collaborating to be able to identify new fraud schemes and trends and tackle them heads on.

Customers are part of the Game:

Even customers and users are joining hands to stop criminal organizations by reporting fraud calls and cases online and creating anti-fraud communities. For examples, mobile users can install an App on their mobile to filter the upcoming calls and know if a call from unknown number is fraud or not based on what other mobile users reported about the calls after they had answered them.

Modern Fraud Examination:

As accounting, law and investigation techniques are essential knowledge for fraud examiner to have, IT knowledge, Forensic Data Analytics, Cyber Security are becoming part of the daily work that fraud examiners are doing in modern organizations. The role of fraud examiner had moved from simply resolving fraud from disposition to play more proactive role in helping the organization in doing fraud risk assessments and keeping them ahead of potential fraud.

Capturing External Fraudsters:

Fraud examiners are familiar in dealing with internal fraud and interviewing fraudsters from inside the organization. However, as external parties are conducting more and more fraud, it is challenging for fraud examiners to trace criminals who are involved in external fraud, capture them and finally interview them. New skills are needed to be able to think outside the box and understand the appropriate legal ways to deal with fraudsters from many countries. This is true mostly in

the financial services sector as more than 59% of the fraud is now conducted by external perpetrators.

Omnifraud solutions are now being implemented by many organizations that address the enterprise wide fraud risks and look at fraud from a holistic approach across all the channels. These solutions created a strong shield that protects organizations but these solutions are as good as the people who are behind them.