Ian T. Mitchell
ian.mitchell@53.com
Fifth Third Bank
VP, Director Enterprise Fraud Risk Management

FIRMA: Omni Channel Fraud: Fraudsters Are On The Move – Is Your Bank Ready To Keep Up?

Section 1: Setting the stage

Slide 1
- The landscape of fraud continues to shift as technology evolves in the financial, retail and service ecosystems.
- Attacks are focusing on the least common denominator, which in recent cases has been the collector of data. Banks have deployed traditional countermeasures to combat traditional threats.

Slide 2
- Fraudsters are using information obtained in diverse sources to coordinate attacks on unsuspecting businesses.
- Businesses are now reinforcing their infrastructure and seeking partners to help them fight back.
- Depending on their size and sophistication, businesses are seeking varying levels of advisors and partnerships to protect themselves and their customers.

Slide 4
- Banks have seen fraudsters utilize information across channels and product types.
- Financial institutions without the ability to connect the dots are prolonging their exposure to loss and negative customer impact.

Slide 5
- Counter measures that were designed to stop historical fraudulent pain points have expectedly caused a migration of attack vectors.
- Legacy infrastructure at critical control points contribute to prolonged exposure to new and old front attacks.

Slide 6
- New generations of text savvy and increasingly social people are entering and transacting in a legacy ecosystem that has bolted on new technology.
- The openness and new channels to which these new users interact introduce new risks.
- In addition, criminals are targeting and sometimes partnering with these users in ways that challenge implied norms.
- **Social Networkers** share their social life in digital platforms (like Facebook, Instagram, Snapchat and other networks, but do very little e- or m-commerce, face the risks associated with having their personal information widely available to fraudsters who can use it to overcome security measures or socially engineer victims. This manifests in a 46 percent higher risk of account takeover fraud.

Source: https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

Slight 7

- Fraud and Risk professionals must acknowledge this evolving landscape and meet it with equally evolving infrastructure and anti-fraud programs.
- Unless risk professionals can keep up, the gap may continue to widen.

Section 2: Our Lens Of Fraud

Slide 9 - 12

- Financial institutions, government agencies, solution providers and organizations have strived for many years to evolve the approach to fraud management.
- At first the industry attempted to secure products, and then recognized they were common threads.
- The industry focused on the products, only to realize the complexities that live across the channels within the products.
- Much of our focus is attempted to categorize and compartmentalize fraud, we started with products and now we are attempting to do this at an enterprise level.
- Terms like holistic fraud management have defined much of our technological and program advancements. This traditional application of the term holistic may not encompass the full dimension of the problem.

Section 3: The Fraudsters Lens

- The criminal does not view the world in the same way that we do. They're not constrained by our boundaries and limitations. They are not defined by our programmatic constructs around fraud. They don't play by our rules.
- The goal of a fraudster is simple: To maximize the financial gain with the least amount of effort and resources. This goal of maximization makes them look at our world not by products or channels. They look at it as data. The more data they captured, the more financial benefit.
- They view our channels, products and other internal constructs as nothing more than a game to maximize their benefit. When they exhaust the usefulness of their character, they reset the game.
- Because of their lens of our world, it gives them more flexibility then we have to fight back.

Section 4: The Paradigm Shift

Slide 18

- It was quickly realized, that traditional methods of securing products and authentication channels (i.e. KBA, Drivers license and Passwords) are highly susceptible in the environment of easily accessible data.
- Thus, the industry moved the ball forward with the deployment of multi factor authentication across channels.
- Criminals will always take the path of least resistance. Criminals will gravitate towards the weakest channels or using information from one channel to another.

Javelin's 2017 Identity Fraud Study:

Account takeover bounces back – After reaching a low point in 2014, both account takeover incidence and losses rose notably in 2016. Total ATO losses reached $2.3 billion, a 61 percent increase from

2015, while incidence rose 31 percent. Account takeover continues to be one of the most challenging fraud types for consumers with victims paying an average of $263 out of pocket costs and spending a total of 20.7 million hours to resolve it in 2016 – 6 million more than in 2015.

Source: https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

- In addition, customers are placing more value on authentication methods that make them feel secure. This flight to security has evolved authentication into methods that traditionally customers found to be inconvenient. Thus, strengthening a financial institutions ability to authenticate customers for high-risk transactions.

- The future, appears to be evolving beyond customer interaction points. Capabilities are being developed to seamlessly deploy authentication behind the scenes, where a customer enables functionality like biometrics knowing that in return they achieve a higher level of security and enable a higher level of functionality. Rumored deployments by Apple and Samsung will likely significantly advance authentication capabilities. However, authentication that relies heavily on the device as an authentication point and not a delivery method may only authenticate the account or the transaction to the device and not to the identity.

It is important that banks invest in authentication infrastructures to keep up with the customer expectations for interactions.

Slide 19:

- An increasing number of fraud events are happening across our channels. Fraudsters are not only looking for the weakest links but are demonstrating more ability and patience to gather and leverage information. Schemes like Business Email Compromises (BEC's), credential validation attacks and sophisticated account take overs are demonstrating that institutions need to not only monitor each channel, ensure each channel has equal or consistent infrastructure, but also have the ability to view activity across channels.

Example: account take over fraudsters leveraging new account channels

Section 20:

- The easiest definition for first party fraud is where the individual perpetrating the crime is actually a true party customer. Important: to be fraud there needs to be proven intent to abuse.
- Traditional manifestations of first party fraud schemes are commonly seen in and around depository account abuse schemes, like counterfeit deposits or kiting. Other types of first party fraud include income or employment misrepresentation. All of these are reasonably well defined as an industry and there are Industry best practices to identify and manage these abuses.

- New schemes of first party fraud possess a potentially more lethal angle. In some cases fraudsters enter an organization with the intent to abuse account structures for personal gain. In others, there is reason to believe that they are targeting more vulnerable populations convincing them to knowingly participate in account abuses. The telltale sign of this activity is when investigations show the same exact method of attack.

Slide 21:

- Even more heartbreaking, is that there are innocent participants that get caught up in criminal activities. Work from home, phishing and sweetheart scams can be some of the most harmful. These types of scams require more customer education and hand holding in the remediation process. Each bank is different on how it handles these types of events, regardless of where the financial loss resides, banks are doing more to protect and educate customers. This will likely grow in the future.

Section 5: What can we do?

Slide 23

- Enlist the customers. Customers have a growing desire to partner with financial institutions to fight against this external threat. They're willing to incorporate increasing levels of friction in the process, provided that it is delivered in a way that makes sense to the transaction. They want alerts that identify suspicious activity and empower them to identify suspicious activity. They are seeking education in mediums they operate in. They understand the need for anti-malware. We are dealing, in general, with a better educated and more agreeable customer.

Slide 24:

- It is very important that we leverage the scale and knowledge across the financial marketplace to fight back. Both internally and externally. Call centers, customers and Information Security partners have become critical for success.

- There is a growing need to arm all areas of a bank and its partners. A clear identification and referral program needs to be in place which includes basic training and awareness of different fraud events, and what to do if something suspicious is identified. It is important to make it simple. Reporting unusual activity needs to be something that everyone can figure out easily. Review your processes to identify fraud, both from a customer and an employee perspective. If you can't find it or understand it there's a good chance you're missing something.

    - Establish an identification and referral program
    - Training and awareness
    - What to do's...
    - Make reporting simple

Slide 25:

- The best Fraud fighters are the ones that know no boundaries. Not organizational, not from data and not in their systems. As mentioned above, the criminals don't operate in silos or view the same constructs we do. As they operate in more coordinated and in increasingly boundless approaches, our approach to fraud needs to be nimble also.

- Ensure effective communication across all organizations that identify, detect and respond to fraud.
- Ensure that investments on anti-fraud infrastructure solve the problem across channels and products. Fraudsters won't operate within them.
- Ensure your data environment is comprehensive and nimble enough to adapt to increasing needs.
- Make sure that A data model exists that allows you to follow a transaction, to an account, to a customer and to an employee. Followed by any other data mapping configuration to ensure connectivity across your environment.
- Ensure your detection teams and investigators are talking to each other. Events that appear un-linked, may possess common threads. You need to be able to identify it.

Slide 26:
The main focuses of your controls will likely still remain your card, deposit, check and even consumer loan fraud monitoring platforms. However, there is increasingly more reason to be considering a more holistic integration across these various event types. The following are justifications for such an approach:

- **Fraud reduction**: this reason alone may not deliver enough of the business case to fund a comprehensive transactional fraud approach. But there will likely be some identifiable benefit.
- **Customer experience:** With customers wanting to be a part of the prevention process, they are becoming increasingly aware of inconsistencies in capabilities.
- **Enablement:** With a customer centric view of fraud management, in theory you may be able to offer more functionality in channels that you may not have appetite currently to venture into. I.e. wire transfer request via a mobile device, new account openings via the call center, International purchases on a card in the middle of the night. The more you know about your customer and the more your infrastructure is able to ingest and respond in real time, the more you can do like the customer in

Section 6: The Takeaway

Fraudsters aren't after the banks.

They are targeting your customers.

Nurses, doctors, teachers, retirees…

They are after businesses….

Fraud is becoming more customer centric.

It is critical that we know our customers better than the fraudster do.