RSAC®
eFraud Global Forum

RSA Conference 2019 eFraud Global Forum (eFG) Topics
Monday, March 4 Agenda
(Listed in Alphabetical Order)

NOTE: Subject to change

MONDAY, MARCH 4TH
7:15am – Continental Breakfast
5:45pm – Closing Remarks & Cocktail Reception
Series of Peer-to-Peer Sessions during Lunch

A Sunday In Hell – Best Practices from Law Enforcement
Cooperation between Law Enforcement and Private Industry is a pretty tough thing to do in general. It gets very complicated when the Private side not only does not cooperate, but actually actively tries to make LE's life harder, if not impossible. This presentation will take you through a real scenario where a Provider thinks he can outsmart Law Enforcement, hide evidence from them and get away with it. Be ready for a lively demonstration on Best Practices on how to convince an unwilling Provider to obey the rules and eventually cooperate in the end and some entertaining side stories to the path we went down.

ATO From a Retailer's Perspective
Account Takeover (ATO) attacks are a persistent threat to any organization or business that offers online account creation/access or an E-commerce platform for its customers or employees. In the retail industry, ATO attacks from sophisticated cybercriminals are rampant, continually attempting to gain unauthorized access to customer accounts. Once compromised, cybercriminals attempt to steal payment card or gift card data, or to abuse these accounts in other nefarious ways. Learn how Target Corporation used cyber intelligence to tackle a persistent ATO problem, and what steps were taken to minimize impacts and get ahead of these attackers.

Combatting New Account Fraud – Interactive Hands-On War Game
During this interactive, hands-on "war game" exercise, our team of experts will present a series of scenarios in which an identity decision is needed – by evaluation the data at hand as well as data that can be acquired to support your investigation process you and your team (5-8 eFG attendees) will use NAF fighting best practices to make the final decision. Based on real data and events, our devious scenarios will challenge your skills, and force you to make trade-offs between investing further time and resources in the investigation, or make the call - and risk having a false decline. Test your skills, learn from others, and takeaway new best practices.

Dynamic Application Response and User Flows for Fraud and Compliance Use Cases
In this session we will discuss how financial institutions and application owners can create omni-channel visibility and use cases around identity flows, and build new user flows, in an application, across applications, and across channels for various fraud, risk, and compliance use cases with no new software development.

Hook, Line and Sinker: Advances of a Modern Phisher

Today's modern phisher is a force to be reckoned with. She is more ruthless, cunning, and harder to detect than ever before. Leveraging today's readily available technologies, she can easily bypasses 2FA security mechanism and get the victim to call her! This session will highlight the latest evolutions in phishing techniques including 2FA-bypassing tactics and advances in vishing attacks, namely the "reverse vish." The presentation will cover the newest techniques in phishing and vishing. While phishing is often considered the oldest cybercrime ploy, these new attacks offer a twist on the traditional creating a need for new countermeasures to detect and shut them down.

Hot Off the Press Attacks, Emerging Threats and Crystal Ball Predictions

The online fraud landscape is constantly evolving, as criminals fine tune attacks and get more sophisticated in how, what, and who they target. A panel of experts will discuss the most recent set of attacks and what organizations need to do to defend themselves and their customers. They will also share crystal ball predictions of what to expect next…and how best to prepare.

How Digital identity will Reduce Fraud

Digital Identity offers the promise of greater security, trust and efficiency….and correspondingly the reduction of fraud. However, it doesn't come without considerable hurdles. This session will provide a deep dive into the status of the initiative, how it may deliver on its promises, and what to realistically expect.

How We Combat Synthetic Identity

Synthetic Identity Fraud is growing fast, resulting in more fraud losses than ever. In this 3-part series of presentations and discussions we will:

- Review case examples to show the scope and scale of this fraud threat and how social media is being leveraged to facilitate it
- Demonstrate how a Red Team created a synthetic identity using "credit repair" techniques and false SSN
- Present techniques for detecting and mitigating synthetic Identities and facilitate an interactive discussion focused on what industry needs to do to address the challenges posed by this growing threat, including pressing Congress to expedite Section 15 of the recently passed Economic Growth, Regulatory Relief, and Consumer Protection Act which aim to provide an electronic identification validation system to quickly validate identities.

Leaky Mailboxes -- Fraud Implications of Mass Email Compromise Via Credential Stuffing

Criminals have stepped up the credential stuffing game, testing billions of credentials against associated email providers and getting in at a rate of tens of millions of accounts per month. This approach is driving ATO activity against organizations with weak password reset procedures or who allow 2FA via email. Additionally, email access provides criminals with the intel necessary to execute highly targeted phishing and malware email campaigns. This presentation will provide a summary of Baldwin's analysis of 9 billion IMAP stuffing attempts observed over just a two month period. Highlights of the presentation include: Which providers are being targeted for stuffing, attack success rates, specific content criminals are searching for in victims' inboxes, what they're finding/stealing, and how this approach is driving ATO.

Lessons Learned from a Major Former Hacker

In this session a former United States Most Wanted central figure in the cybercrime world who was instrumental in developing many areas of online fraud including Identity Theft, Account Take Over Fraud, Card Not Present Fraud, IRS Tax Return Identity Theft, and more, will reveal insight into exactly what criminals are currently doing, and will share recommendations on what organizations need to do to detect and defend.

Next Generation Strategies for Battling Fraud

In the post Equifax breach world, KBAs just don't work. Leading organizations from across the world are moving to hybrid fraud prevention and detection strategies that include behavioral analytics in real time, machine learning, and now entity analytics, all of which have as a foundation data lakes of rich data. This session will explore this evolution and will dive into how two organizations have embarked on this journey.

Social Engineering – Changes in Accountability and Liability and Approaches to Mitigate this High Impact Attack

Over the last 5 years, social engineering scams have increased in complexity, occurrence and financial impact, and most of the time customers have solely bared the liability. In this presentation we will review changes that are: causing a rapid increase in social engineering scams across banking, telecom, retail industries, changes that are reassigning accountability and liability, changes that are causing greater reputational and revenue risks, and new innovative approaches to mitigate social engineering scams across call center and digital channels.

Solving Day 0 Identity Verification with Enhanced Data and Machine Learning

Why are we still struggling with new customer identity verification? What can be done to improve the low pass rates of current KYC programs? How do we finally reduce new account fraud? In this session we will share Socure's Data Science team's latest research findings quantifying the influence of various Personally Identifiable Information (PII) elements, such as email, phone, address, and IP on identity prediction across several industries.

The Battle of Identity – Best Practices for New Account Fraud Defense
Organizations across industries struggle to establish a new defense doctrine against New Account Fraud (NAF). How do we identify NAF? How do we stop it? What are the fraudsters' intentions, methods and tools? What are the costs of allowing bad users in, and keeping good users out? In this panel of experts we'll discuss the current state of NAF detection, the industry's best practices, the various new layers of visibility available and how they jointly contribute to the war effort.

This is How We Build and Leverage the Holy Grail of Money Mule Intelligence
This presentation will dive into how a major financial organization has acquired massive money mule intelligence from multiple sources, processes it into a rich database and feeds into their downstream system for the use of multiple internal and external use cases. Intelligence includes fraud merchant intel, and much more. Many use cases will be shared!

RSAC®
eFraud Global Forum

2019 eFraud Global Forum Topics

Wednesday, March 6 Agenda
(Listed in Alphabetical Order)

NOTE: Subject to change

WEDNESDAY, MARCH 6TH
Session 1: 8:00am – 8:45am
Session 2: 8:45am – 9:30am
Session 3: 9:30am – 10:10am

Learning to Catch Lightning
Mobile bank fraud is difficult to detect and may go unnoticed until funds have been illegally removed from an account. Artificial intelligence (AI) models can dramatically improve fraud detection rates and detection times. In this session, we will discuss how AI was used to create a fraud solution for a financial institution to detect the proverbial needle in the haystack. We will focus on the AI model, a methodology for machine learning, and a model evaluation process. We will explore how data imbalance was addressed and how the model was created to produce realistic and actionable results.

Phishing: Insights from Recent Attack Campaigns against Email Users
This talk summarizes the insights from the latest evolution of phishing attacks as seen by Gmail. We leverage Gmail's unique vantage point to illuminate how phishing techniques targeting one group of users is drastically different from those targeting others. Drawing from concrete examples, we highlight the key differences we observed across some of the most interesting phishing campaigns we observed that affected Gmail users.

What's Next in AI for Fraud Detection?
Fraud detection was among the first commercial applications of machine learning, but new applications are blooming all around it — many using techniques not yet applied to fraud. So, what's next for fraud detection? Ted will identify which new AI tools and methods apply to fraud and which do not; and describe fraud-specific innovations likely to arrive in prototypes soon. Overcoming technical and business hurdles to applying new AI technology in real-world fraud operations will close the presentation on a practical note.