RSAC
eFraud Global Forum

RSA Conference 2020 eFraud Global Forum (eFG) Topics
Monday, February 24 Agenda
(Listed in Alphabetical Order)

NOTE: Subject to change

MONDAY, FEBRUARY 24, 2020
7:15am – Continental Breakfast
5:45pm – Closing Remarks & Cocktail Reception
Series of Peer-to-Peer Sessions during Lunch (topics not included)

Artificial Intelligence Based Verification & Fraud Detection

-What are the problems with current methods of identity verification?
-How can we utilize KYC data and AI for authentication and fraud prevention?
-What are the business, data and cultural challenges in developing such in approach?
-Will this work for real-time payments?

This session will focus on three different industry approaches to answer these questions and discuss best practices and challenges in developing and deploying these systems from the following three perspectives: 1) Starting from scratch, 2) Hybrid integration with current identification and fraud detection systems and 3) Data driven approach. *This session will answer the simple question: How do you do it?*

Ask the Experts

Buckle your seat belt! During this fast-paced Q&A session questions collected throughout the day will be discussed; experts in the audience will be asked to share their knowledge and insight. Answers will be allowed 3 minutes each.

Best Practices and Direction of Authentication

This session will bring together leading fraud prevention leaders from across the world to share their views on the direction of Authentication. Discussion will certainly include how organizations are tackling the MNO challenge as carriers are cutting off critical phone data.

Cross Industry Implications of Retail Fraud

The same fraudsters and fraud rings target retail companies and other industries simultaneously. Attacks are increasingly sophisticated and cross industries. Presentation reviewing different types of retail fraud that may be new to the audience. Examples will include exploits that are utilized cross company and cross industry. Follow-up with a panel discussion including representatives from retail, financial services/card issuer, card network, or payments services provider.

Deepfake Audio: A Threat to the Enterprise

Today, advances in machine learning and neural networks can produce audio and visuals with quality that begins to evade human perception. The democratization of these technologies is lowering the barrier of entry for malicious actors to quickly create realistic deepfakes utilizing publicly available (and sometimes private) datasets. During this session we will demonstrate how fraudsters can use 20 minutes of audio pulled from earnings calls, YouTube videos, TED talks and intranet training videos to create avatars of your executives; will reveal a new form of Fake President Fraud and how fraudsters are utilizing synthesized audio to call individuals in the accounts department to transfer large sums of money; and will discuss the evolving implications of deepfake technology on your brand reputation by distributing fake content on social media.

Fighting Fraud Use Case – How AWS Tackles the Problem

Protecting customers and company resources is a constant struggle, balancing prevention mechanisms against customer friction. Further complicating the battle, bad actors continue to evolve, aided by new techniques and technologies and at times supported by unknowing customers. In this session, fraud prevention experts from Amazon Web Services (AWS) will discuss how AWS tackles this problem, outlining strategies and best practices to prevent, detect, contain and remediate bad actors. Specifically, this session will address the following topics: Rules of the Game (Key Objectives, Constraints and Requirements): What's Your Strategy (How to Prevent, Detect, Contain, Remediate Bad Actors – Use of ML/AI); What's the Score (Key Monitoring and Measurements to ensure fraud mechanisms are performing well and legit impact is minimized).

Frictionless Banking Fraud

Banks offer their customers a simple authentication process to access their account and make payments on the fly. This could have direct impact on security measures the banks have in place to protect their customers. This leads us to the following question: "How could banks minimalize security checks, improve their customer experience and at the same time keep customers safe?"

How and When to Use Document ID Verification and Selfie Check

With the continued fraud challenges, new ways of establishing identity in the digital environment are more and more critical. This session will share use case experience of a digital banking leader who has implemented this technology and is able to provide valuable insights into what is helpful from a fraud detection aspect and customer on boarding.

Leveraging Phone Intelligence and Digital Footprints to Prevent Fraud

Identity fraud remains amongst the fastest growing crimes. Customer interrogations put in place to combat fraud are driving high levels of dissatisfaction and application abandonment due to the lack of speed and high levels of friction. While there is no silver bullet, during this session you will learn why intelligence from the phone represents the most reliable digital footprint to establish trust and reverse these trends. The discussion will cover the impact of the phone from initial contact and onboarding through the customer journey to reduce abandonment, establish ongoing KYC, add ongoing fraud controls, and improve coverage and inclusiveness of under-represented segments.

Machine-Learning Trouble Spots: New Payment Channels and Multi-Channel Integration Machine learning has earned its place as the main tool of modern fraud detection. But, it can fail for new payment channels lacking historical data. Learn how to protect new channels with other tools and re-introduce machine learning variations in stages as the channel matures. Multi-channel fraud protection is potentially superior to single-channel solutions. But, that promise is squandered by the many systems that simply share single-channel risk scores across channels. Join Ted in examining this lost potential and learn how to build multi-channel systems to achieve the full promise of machine learning applied to an integrated view of account behavior. (And, see how the same methods can be used to make other, surprising improvements.)
New eCrime Ecosystem During this session Law Enforcement organizations from across geographies will share a consolidated view of who are the different levels of players (and how they benefit across the hierarchy) and what are the most common and impactful fraud threats. Each panelist will share crystal ball predictions of what to expect in the coming months as well as how best to prepare.
Open Banking Fraud This session will explore how fraudsters are taking advantage of open API Banking – and what organizations need to know and do.
Roses Are Red, Violets Are Blue, Protect Your Payments with 3DS2! In this session we will review the use of EMV 3-D Secure (3DS) as a means to authenticate online payments, across a multitude of devices, with little consumer friction. The session will focus on 3DS 2.0 and how it enables lower friction and cart abonnement while providing card issuers with the means to secure and protect their customers. The session will also review the new 3RI and non-payment flow functionalities that can further help issuers protect their cardholders. Finally, the session will go over future challenges banks should expect and keep in mind as they think about their future payments authentication strategy.
Synthetic Identity War Games – Interactive Hands-On Workshop During this interactive, hands-on exercise our team of experts will present a series of scenarios in which an identity decision is needed: are you seeing a genuine person trying to open an online account or a completely bogus synthetic identity you should reject? By evaluating the data at hand as well as data than can be acquired to support your investigation process, you and your team (5-8 eFG attendees) will collaboratively use synthetic ID 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 take away new best practices!
The Many Faces of Social Engineering During this session we will pick apart a wide range of social engineering technique and will facilitate an open discussion on how organizations are tackling this broad problem that refuses to go away.

To Catch a Synthetic ID Thief

In this session, a leading FI will share how post closure triage of synthetic identities can uncover large networks of fraud actors and identify additional suspects prior to any fraud occurring on the accounts. The initial pilot was so successful that a new team of fraud analysts was formed, and the process has now been automated. This is information sharing at its best!