RSA Conference 2022 eFraud Global Forum (eFG) Topics
Tuesday, June 7 Agenda
(Listed in Alphabetical Order)

NOTE: Subject to change

TUESDAY, JUNE 7, 2022
7:15 am – Continental Breakfast
5:45 pm – Closing Remarks & Cocktail Reception
Series of Peer-to-Peer Sessions during Lunch (topics not included)

Combating Impersonation Fraud
This session will cover the evolution and anatomy of impersonation scams (including brand impersonation) and what organizations can do to mitigate key risks to reduce the attack surface and address specific risks once detected.

Convergence Shift #RiskOps
To have a fighting chance against financial crime, financial institutions must have a platform that is comprehensive, preventative and collaborative. Merging online fraud detection, identity proofing, and user authentication creates digital trust across the entire customer risk journey and empowers teams to prevent fraud even before a transaction takes place. Join this future-forward discussion to learn:

- How risk engines bring disparate data sources together to facilitate modeling as well as the visualization of big data to support fraud investigations.
- The benefits of each type of data enricher: device, behavior, anti-phishing, and malware
- Tackling risk management with three key pillars: a comprehensive architecture, human-centered AI, and a collaborative analytics suite

Fighting Fraud with AI – A PayPal Case Study
PayPal's two-sided network industry-leading creates insights that help protect customers and merchants around the world. During this session PayPal will provide insights into how thousands of data elements are consumed by its risk models to accurately predict and detect potentially fraudulent patterns, while identifying common customers behaviors and enhancing their experience. Connecting more than 400 million active users with 32 million active merchants globally, its two-sided network puts PayPal in a distinctive position to collect thousands of data points - from the consumers, transactions, sellers and even cart details to understand the potential risk of each action performed across the platform. With this rich data, advanced AI and Machine Learning, PayPal has developed models that represents a true story-based approach.

Fraudster Abuse of Legitimate Services
Many fraud attacks are successful because the fraudsters merely abuse a normal function of a website or process. This includes services set up by business to make things easier or smoother for their customers. In this session we will review a variety of legitimate services abused by criminals who find loopholes and exploit them. We will explore how organizations are fraud-proofing these services, and we will engage attendees to share ideas (often simple ones) that make all the difference.

Fraudster Ecosystem & the Value of Understanding Fraud Attack Kill Chains
During this session we will first provide a review of the current fraudster ecosystem, including roles, partnerships, operations, etc). A leading organization will then share how they define fraud attack chains to develop strategies and controls to more effectively detect and prevent fraud. A deep dive into kill chain for ATO and gift card fraud will provide specific insight into the why and the how – and lots of ideas to consider for your own programs.

Fraud Threat Landscape
In this session experts from leading organizations will share the most current and concerning fraud threats – as well as their crystal ball predictions of what we can expect over the next 3 – 6 months…and how to prepare.

The International Takedown of Emotet
Law Enforcement agencies throughout the world, in partnership with private industry, worked for years to down the world's most damaging and costly malware known as Emotet. Law enforcement will present on the case and share the complexities behind the most comprehensive law enforcement action in the fight against cybercrime.

Mobile Malware Trends
In this session you will learn how threat analyses on evolving malware and timely implementation of countermeasures help to minimize losses for customers and the organization.

Money Mules War Games – Interactive Hands-On Workshop
During this interactive, hands-on exercise our team of experts will present a series of money mule scenarios. 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 determine if presented use cases are genuine or if they involve money mules. 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!

More Client Protection? What to Do About Scams
The volume of scams and the associated $ loss is greater than fraud. In many cases, banks don't have to make customers who are victims of scams whole. But now the UK passed guidance that UK banks should make customer whole. Recently, CFPB issued guidance to give customers more protection but it is a FAQ only, and therefore it is not enforceable. During this session we will discuss **what organizations are doing around scams** and whether or not they are changing their approach on making clients whole after scams.

Next Generation Fraud
Fraudsters are leveraging information gathered from attacks on one industry to exploit other industries. This session will discuss new attack techniques across a variety of industries (including healthcare and social media) – and why it is so important to include a broader (cross industry) view of behavioral patterns and fraud trends.

Preserving Trust in Today's Digital Economy
It is no surprise that digital transaction growth has been fueled by the introduction of newer digital models and an explosion of new providers offering financial services. Many of these new providers are not always familiar with the intricate regulatory requirements and risk controls necessary to operate a bank-grade trusted service, at scale. Ensuring preservation of the underlying trust model is paramount. Historically, consumers and businesses have looked to traditional financial institutions as their primary trusted provider for financial related activities. But now, with the introduction of PSD2 and open banking initiatives, new financial services platform and API providers are making it possible for any non-financial provider to embed bank-grade level financial products and services into their own offerings. This session will discuss some of these real-time challenges many are facing today as digital-first commerce and banking activities become the norm. We will also share insights as to how to companies are embracing these new innovations whilst balancing the ability to maintain the underlying trust model and prevent unnecessary friction in the new digital economy.

Target Cyber Security Takes on Cyber Fraud
The digital revolution has reduced the barriers of retail fraud and blurred the distinction between online and in store. Hear Target's Cyber Defense leaders share how they used a threat-driven approach to evolve their cybersecurity organization to integrate cybercrime fraud activities. Leading with well-established security best practices and capabilities, Target incorporated fraud within the security umbrella to apply structure and shift from traditional reactive fraud practices, to take a proactive approach while ensuring a great guest experience.

Tech Support Scam Case Study: Collaboration that Leads to Enforcement Action
During this session, Microsoft, Bank of America, USTelecom and the Department of Justice will share their part in developing a case for enforcement action against perpetrators of tech support scams.

Top Red Flags for Uncovering eFraud & Ransomware Both FATF & FinCen has provided guidance on how Financial Institutions can identify and mitigate risks of virtual currency (VC) transactions. However, as cryptocurrency adoption increases, so does the incident of cybercrime. How can organizations identify red flags that indicate that suspicious activity is underway?
USSS: A BEC Investigation and Indictment The United States Secret Service, Global Investigative Operations Center (GIOC) will give a detailed case study regarding a real-life Business Email Compromise case. The USSS will show both cyber and financial exploitative investigative methodologies that led to the indictment of an international based BEC actor. The session will show a real case-based link/network/incident analysis chart that details how the complex transnational case was laid out. Also, the USSS will give real time information regarding emerging trends and tactics in the world of cyber-enabled financial fraud.