RSA Conference™ eFraud Global Forum (eFG) Canada
Tuesday, October 24, 2023
Agenda Topics
(Listed in Alphabetical Order)
NOTE: Subject to change

TUESDAY, OCTOBER 24, 2023 **8:15 am – Continental Breakfast** **5:00 pm – Closing Remarks & Cocktail Reception** **Please plan to attend the full day**
Automation and Data are Key to Fraud Detection, Prevention, and Response In a dynamic threat environment, where daily impacts by evolving attackers reach billions, it's vital to prioritize automation and effective data management in current and future strategies to battle fraud. Reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) is key in mitigating the substantial financial fallout from cyber fraud.
Best Practices to Improve Scam Detection (including Consumer Education) Leading organizations will share what they are doing to reduce scams and the associated fraud. This session will include a focus on Consumer Education.
Digital ID Update This interactive session will provide an update on the progress and fraud implications of government issued ID digitization.
Fraud Implications of Deep Fakes and Generative AI How fraudsters are using these advanced tools, and how fraud prevention teams can use them to fight back. Presentation will include: • The evolution of Deepfakes and AI-driven fraud • What a leading financial institution is doing now to detect these advanced threats; as well as what they see coming in the horizon, and their strategy to prepare for the future risk. This discussion will include tangible work on fraud controls.
Fraud Threat Landscape A review of the current key concerning fraud threats, as well as of the most important trends. Panelists will offer recommendations on how best to prepare to defend from what is coming next.

How to Maximize Collaboration between Financial Institutions, Telcos and Law Enforcement
Working collaboratively with law enforcement and with the telcos to successfully fight and defeat fraudsters is a critical component of fraud prevention strategies at private sector organizations. This session will explore how best to create a cohesive process between these important components of the fraud ecosystem.

Impact of Customer Identity and Access Management (CIAM) on Cyber-Fraud Outcomes
Application fraud, account takeovers, and other identity related fraud are growing across channels. Countering these threats requires stronger identity-proofing, authentication, and lifecycle management. Weakness in any component of CIAM leaves the door open to threat-actors but increasing friction for customers will cost you business buy-in. This talk will arm you with information to evaluate and plan your own customer focused CIAM enhancements and help you make the case for investment within your own organization.

Know Your First Party Fraud Enemy
This session will review top trends of First Party fraud, including Crypto scams, BEC (invoice redirection fraud), Fast Payment scams and collusive mule scams. A detailed look at the bad actors as well as their techniques/MO's will be provided.

Managing Online Fraud
Digital Transformation has fueled a considerable growth in digital transactions volume along with vulnerabilities. Fraud (first and third-party), account takeover and synthetic ID continue to be a major problem for all ecosystem stakeholders (merchants/retailers, issuers, acquirers, processors and financial institutions) outpacing digital transaction growth. How to onboard customers or merchants and how to continuously monitor them continues to challenge the ecosystem. This session will review fraud trends in Canada and North America, will provide insights into best practices and will facilitate an interactive conversation to promote an exchange of ideas.

Mobile Operator Services for Fraud Detection and Prevention
Properly secured, mobile services provide reliable two-factor authentication and assist in identity verification. Access to real-time mobile account, device, and network data assists in satisfying KYC requirements, detects application fraud, and prevents account takeover fraud by securing vulnerable two-factor authentication processes (e.g., SMS OTP) from SIM Swap fraud.

Red Teaming for Fraud
A cybersecurity vulnerability assessment (e.g., red team test) is required before any internet facing product goes live. A cybersecurity vulnerability assessment is technical in nature. What about testing from a fraud perspective? Shouldn't internet or payment products require a fraud threat assessment before going live? Does your bank have a risk-based culture and are they ready to incorporate Fraud Red Team? During this session, TD Bank will share their strategy for injecting fraud threat assessments before go-live, including the value proposition and lessons learned on how to get funding from the business.

Reducing Authorized Push Payments Fraud Using Conversational AI Authorized push payment fraud is difficult to prevent because the victims are tricked into sending the money themselves. While regulators and banking corporations work together to effectively fix this problem, new technologies and solutions are needed. A modern, game changing approach makes it possible to significantly reduce the success rate of APP fraud by harnessing one simple principle - real time communication with the end user.
Threat Landscape: Perspectives from Canadian Centre for Cyber Security and Canadian Anti-Fraud Center