**RSA Conference™ eFraud Global Forum (eFG)**
**Europe**
**Tuesday, 23 January 2024**
**Agenda Topics**
**(Listed in Alphabetical Order)**
*NOTE: Subject to change*

**TUESDAY, 23 JANUARY 2024**
**8:15 -- Networking Breakfast**
**17:00 – 18:30 – Closing Remarks & Cocktail Reception**
**Please plan to attend the full day**

***KEYNOTE SPEAKER:***
**Prof. Dr. Mary Aiken** is a world-leading expert in Cyberpsychology - the study of the impact of technology on human behaviour. She is a member of the INTERPOL Global Cybercrime Expert Group, and an academic advisor to Europol's European Cybercrime Centre (EC3). Prof. Aiken will deliver a talk (and Q&A session) on "***The Cyberpsychology of Fraud,"*** outlining her cutting-edge research and work in areas ranging from cyber behavioural profiling to industry led active cyber fraud defence, informed by her forthcoming publication titled "The Enterprise Strikes Back.' She will also demo her award-winning consumer campaigns for the financial services sector focusing on scam awareness, prevention, and intervention, along with her international work with Government agencies addressing online fraud. Interesting fact - Prof. Aiken's work as a Cyberpsychologist inspired the CBS primetime series 'CSI: Cyber.'

**Best Practices in Scam Prevention and Detection**
What leading organizations are doing to reduce scams and the associated fraud, followed by an ideation session on best practices.

**Beyond the Hype: The Power of AI for Fraud Prevention & Detection**
This session will first provide an overview of what is real and what is hype in the current AI landscape, and what to expect in the coming months. The presentation will then focus on how AI is being used to detect and prevent fraud now, and how to prepare to adopt the power of what comes next.

| |
|---|
| **Financial Landscape Transformation: Navigating Payment Overhauls and Shifting Fraud Liability**<br>The financial industry is experiencing a profound transformation marked by significant payment modifications and evolving fraud liability regulations. This session delves into the challenges and opportunities arising within this dynamic environment. It places particular emphasis on the preparedness of affected institutions and the potential risks that come with swift transformation. |
| **Fighting Fraud In a World of Instant Transactions**<br>A panel of experts discuss best practices to combat fraud in a world of instant payments when speed and irrevocability present unique challenges to fraud leaders. |
| **Fraud Threat Landscape – Key Concerning Trends and How to Prepare**<br>A panel of experts share their key concerning fraud threats and trends. Panelists will offer recommendations on how best to prepare to defend from what is coming next. |
| **PSD3/PSR and the Regulatory Environment**<br>A review of the new relevant revisions in PSD3, including liability shifts and compensation. This session will also include an interactive discussion, led by subject-matter-experts on what to expect, what is real, and what do to next. |
| **Tackling Bank Impersonation Scams—A Cross-Industry Approach**<br>Working collaboratively with other financial institutions, 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 highlight a hot-off-the-press case study that demonstrates the power of collaboration – and how to achieve it. |
| **The Dark Web and Cybercrime Trends**<br>Learn about the latest trends and developments in cybercrime and how bad actors are leveraging the Dark Web to attack the e-commerce companies and disrupt the digital economy. Hear directly from Europol on the challenges that law enforcement agencies have in effectively fighting cybercrime across Europe and beyond. Tobias will also give fresh insights into Europol's role in the takedown of dark marketplaces and cover some additional law enforcement success stories and insight into uncovering criminal activity—along with advice for public-private partnerships on when and how to engage with law enforcement agencies. |

**The Great AI Enigma: Future-Proofing Fraud Prevention to Anticipate Attacks of the Future**
When your best customer is Chat GPT and your biggest threat is human click farms, how do you separate good and bad intent online? Traditional tried and tested fraud solutions are no longer enough. It's not about distinguishing bots from human traffic, or customers and fraudsters (scams have put paid to that). And in the age of AI, who is to say the selfie on screen isn't a deepfake anyway?

What does a next-generation approach look like? Why does customer journey orchestration matter and what does it really mean in practice? What are the practical steps business can take to leverage the AI tools that fraudsters are cashing in on, to prevent future attacks?

**The Role of Social Media/Big Tech in Fraud**
Social media is a hot bed of personal identifiable information (PII) and opportunities for scams, fraud and abuse. What are social media companies doing to reduce opportunities for fraud and scams originating in or fueling them in their platform? How are EU regulations such as the PSD3 or EU's Digital Services Act impacting how social media and big tech platforms respond to identifying bad actors and reducing opportunity for abuse? How can FI's and other entities, such as regulators and law enforcement, work more collaboratively with these tech giants? What possibilities do we see in sharing of device or customer data to prevent fraud and protect customers?

**The Role of Telcos in Fraud**
Online transactions now take place almost exclusively on mobile devices. In addition, many authentication methods involve messages sent to mobile devices for validation. As such, the mobile device is fertile ground for fraudsters. What are Telcos doing to protect their networks and their customers from rapidly evolving fraud schemes? How should Telcos and institutions work together to fight the common bad actor?

**The Seismometer of Scams: How Anti-Fraud Trends Predict Cybersecurity Disruption**
Online fraud is a testing ground for criminals to experiment with new techniques and technologies that can later become global cybersecurity threats. The anti-fraud community has been on the frontline of these emerging attacks, acting as the seismometer: light tremors have escalated to earthquakes in the past. However, two recent developments pose new challenges for cybersecurity: the rise of mobile device attacks and the de-technologization of scams and fraud. In this talk, we will explore these two trends, how they exploit the human factor, and how we can leverage the fusion approach to anticipate and prevent them.

**The Weakest link – Shifting Responsibility Towards the Customer - And Consumer Awareness Best Practices**

Financial institutions and other organisations no longer own “the key” to the customers valuables anymore. Today it is a joined ownership and responsibility. Fraud prevention leaders are aware of this and do their best to keep digital environments and processes secure. But are customers aware of their part? Since we’re in a scamdemic, it is clear they might not be (or have the knowledge) – they are the weakest link. It is our special duty of care as a bank or institution to create awareness on this topic for our customers, but how do you do that if most of them think “this will not happen to me?” This session will explore customer education/awareness best practices.  What works/what doesn’t work?