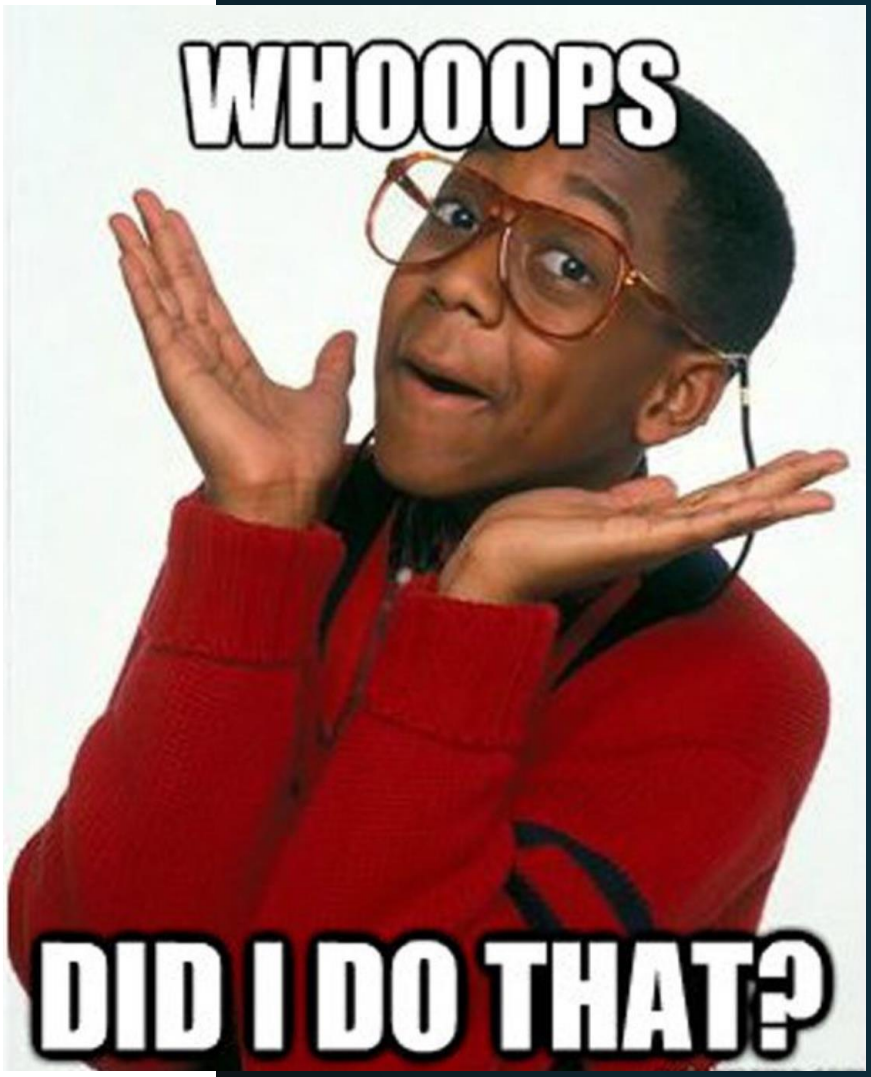
The Complex Relationship Between Cybersecurity & Fraud: Is Fusion Inevitable?

Cybersecurity Maturity

- Cybersecurity imperative was realized 25 years ago, brought on by an explosion of virus, spam, and bot attacks
- Enterprises rushed to solve the problem
- New industries were born

Oops

- Effectiveness of cybersecurity measures drove fraudsters to find new modus operandi
- Fraudsters quickly realized manipulating people was now easier than hacking technology
- Despite advances in device recognition and multifactor authentication, we're still trying to address these issues



The “Scampocalypse” Begins

- Exponential increase in Social Media and Digital Adoption worsens the people/process problem
- Customer becomes the primary, and easiest target
- The ironic solution: technology.
- Crimeware-as-a-Service erupts

The FRAUD Imperative

- It’s time for Enterprises to adopt the mindset they had toward cybersecurity in the early 2000’s to FRAUD
  - Consistent C-Level representation with accountability
  - Driving “FRAUD is everyone’s responsibility” culture
  - Adopting taxonomies, industry frameworks
  - Creating ISACs
  - Defense in depth
  - FRAUD PREVENTION by design

The Stop-Gap: Fusion

- No standard approach
- Data and Analytic Fusion is most essential
- Investigations and Testing very beneficial
- What else?

The Future

- Further alignment of Fraud and Cybersecurity
- Fusion as a culture
- “Identity is the new perimeter”
- When it comes to intelligence, sharing is caring

Wrapping Up

Fraud maturity has a long way to go

We will continue to use people/process to secure technology, and technology to secure people/process

When it comes to data, intelligence, and analytics, we must cast a broad net (internally and externally)

Adopting collaboration as a culture will continue to yield superior results

Is fusion inevitable?

Additional Reading

The CIAM Success Gap: Are We Missing the Most Important Metric?

- Explore how CIAM and Fraud teams can co-exist to achieve mutual success and the fundamental organizational changes that need to happen to make this possible

Cyber Fraud Fusion: CIAM & Fraud Teams Thriving Together

- Cyber fraud fusion centers foster collaboration between fraud, cyber and digital teams to respond to evolving threats effectively

Why Fraud Leaders Need a Seat at the Executive Table

- The prevalence of account takeover fraud is a core metric that is often missed when measuring the success of a customer identity and access management (CIAM) program. Find out how leaders can move past the perception of fraud prevention as a necessary loss to an imperative that is prioritized for funding

How Risk Signals and Data Modeling are Changing Enterprise Fraud Management

- While enterprise fraud management (EFM) platforms have traditionally focused on response capabilities, they have evolved to include risk signal generation and analytics to improve detection capabilities. Find out how organizations are maximizing the value of risk signals, such as behavioral biometrics, and data modeling as part of their EFM strategy

Any Questions?