Financial Crime
What’s Next?
October 10, 2019

Praveck Geeanpersad
Financial Crime Leader
prgeeanpersad@deloitte.ca
Financial Crime... an overall narrative

United States
- Convertible Virtual Currencies
- Sanctions
- Corruption

EU & UK + CA
- Collaboration amongst banks in the Netherlands and the Nordics
- Cost reduction an agenda item – HSBC point in case
- Changing customers’ expectations, regulations, new competition

Challenges in responding
- Increase the velocity and with agility
- Changes will be needed to leadership mindset & culture or DNA of the organization
- Emerging technology which are not mutually exclusive

Changing the way to change
- Intelligence led initiative
- The advent of Fin Crime Fusion
- Industry collaboration
- Public Private Partnerships
Suboptimal FinCrime Solutions and Regulatory Regimes

Criminals don’t distinguish between AML, cyber, fraud or geographies

- Cyber and financial criminals run sophisticated operations on a global scale, using agility and fast innovation
- Current prevention and detection efforts rely on point solutions, focused locally, and are conventional, rigid and compliance-based

True power of data & technology is not fully leveraged for automation

- Regulators have established a robust compliance regime which yields large amounts of data, yet current efforts fail to harness the data’s full potential
- This same regulatory regime overlooks the possibilities of modern technologies

Current approach attempts to review all to catch just a few

- Monitoring efforts rely primarily on linear rules that are relatively easy for perpetrators to predict and circumvent
- Lessons from counter-terrorism highlight the benefits of effectively leveraging intelligence to monitor suspicious activity

‘The current anti-money laundering regime is not fit for purpose’
(WEF Coalition to Fight Financial Crime)

- The illicit proceeds of criminal activity are estimated to be between 2% and 5% of global GDP (c. $1.6 - $4 trillion)
- Money laundering has far-reaching societal impacts feeding drugs, trafficking and organised crime
- The reputational damage of financial crime can severely compromise financial institutions
Compromised health-care data stolen to create money mule accounts

Could have been detected if cyber intel on compromised PII on the dark web was available during CDD

Synthetic identities created by combining PII from data breaches for account take-over or to take out loans

Combining data from CDD, transaction behavior and cyber intel on compromised PII makes it easier to spot anomalies

Large scale money theft by Advanced Persistent Threat (APT) to gain access to payment system through targeted phishing attack and lateral movement

Could have been detected if security alerts and fraudulent transactions were correlated real-time

⚠ EVOLVING THREATS
• Criminals don’t distinguish between cyber, fraud and AML
• Criminals run sophisticated, agile and innovative operations

⚠ SILOED CAPABILITIES
• Reliance on point solutions and manual effort
• Scarce expertise working in isolation
• Compliance-focused with static, easily avoided rules

⚠ DISCONNECTED DATA
• Separated data streams only cover narrow sections of the attack chain

---

1. Based on the "Skyscraper" hack of U.S. hospitals and pediatricians, Deloitte Threat Report, 2018
2. "Five Top Fraud Risks for Banks", American Banking Association, 2018
3. Carbanak and Bangladesh heist illustrate risk of money theft by APT
FinCrime Risks are Accelerating

- Regulatory pressure & innovation permission
- Changing market
- Digital disruption
- Cost pressure
- Global complexity
- Rapidly evolving threats & risks
- Sophisticated criminals & new threat actors
- Current landscape

New FinCrime Approaches Required

- How do we proactively and intelligently prevent financial crime?
- How do we best adopt tech-enabled approaches enterprise wide?
- How do we stay ahead and protect against new and evolving threats?

Client transformation journey

Build a foundation

Intelligence led fundamental change

Automate and optimize