Combatting the Digital Fraudster in the Financial Services and Insurance Industry

Presenters: Michael Kennedy
Wendy Butler
Kevin Wilson

Fraud and Identity Theft

Identity Theft is increasing exponentially.

- Reports of identity theft to the FTC doubled between 2018 to 2020, and then doubled again from 2020 to 2021.
- The amount of losses related to the reported events increased from $3.3 billion in 2020 to $5.9 billion in 2021.
- The older the victim, the higher the average median loss.

Our clients' information is out there and available on the Dark Web for pennies. Fraudsters use this information daily to probe our systems to look for accounts owned by the individuals whom they have obtained PII.

The pandemic has decreased the face-to-face interaction with our clients and increased the expectation for the capability to complete most transactions online. Expanding digital capabilities without strengthening authentication and data controls leads to added risk.

Common Frauds

The insurance industry is targeted by versions of the common frauds seen throughout the financial landscape:

Account Takeover:

Online: Fraudster takes control of or registers a new online account.

Email Compromise: Fraudster gains control of client's actual email address and poses as client to gain access to account.

Call center: Fraudster poses as the client in contacting the call center to gain access to the account.

Family Fraud: Any fraud committed by one family member against another.

Elder Abuse: Financial exploitation of an elderly client through physical threat or abuse, manipulation or misrepresentation.

Financial Professional Misappropriation: Commission based pay structure can put pressure on Financial Professionals and lead to misconduct.

Internal Fraud: Can include manipulation of payments systems and can include bribery and corruption.

Controls

Fraud controls require constant reevaluation to address the everchanging landscape that bad actors create. There is no “silver bullet” to stop fraud. The best method continues to be a layered approach.

- ***Phone***
  - Voice Biometrics
  - Challenging incoming call data
  - Knowledge-based authentication
- ***Online***
  - Credentials
  - Multi-factor authentication
    - Identity Verification
  - Challenging source information
- ***Email***
  - Limit reliance as much as possible
  - Challenging source (compare against email on record and known fraud indicators)

Controls

It is important to track the activity of the client interaction as they move through the systems.

- ***Phone***
  - Number of calls
  - Reasons for calls
  - Analysis of calls
- ***Online***
  - Changing of login credential
  - Analysis of activity (Banking changes)
  - Challenging source information
  - IP addresses (foreign access from high risk jurisdictions?)
- ***Email***
  - Analysis of request (Red Flag indicators)
- ***Disbursements***
  - Challenge banking information
  - Analysis of activity

Controls

The best practice is to run detections on the collected data in the closest to real time scenario as possible. The closer the real time the more effective the protections across the various client interaction channels. Detections that can orchestrate notifications and restrictions based on the client activity across channels provide the best protection.

- ***Phone***
  - Notify CSR that an issue has occurred requiring enhanced authentication
- ***Online***
  - Restriction of online access with notice to client documenting concern
- ***Email***
  - Notice to processor requiring enhanced authentication
- ***Disbursements***
  - Notice to processor requiring specific action (Enhanced Authentication, Referral to Fraud Team)

Training: Especially important for processors and call center staff. Targeted training with specific examples of fraud trends should supplement general annual training.

Risk v. Cost

Organizations must conduct their own risk assessment. The correct fraud controls are not a one-size-fits-all scenario. An orchestration fraud control system requires significant investment in time, money and personnel to manage. What works for one may not work for all.

What is the yearly risk in dollars of fraud?

What is the organization's risk tolerance?

What is the potential impact to the organization's reputation?

What are the regulatory risks to the organization?

Challenges

Leaders responsible for fraud controls must be wary of the potential pitfalls to achieving success.

- You can be the victim of your own success.
  - A drop in successful frauds and/or dollars lost can give leaders a false sense of “Mission Accomplished.”
  - Your messaging matters: clearly explain the work it takes to achieve success.
- Fraud is an everchanging landscape that requires constant vigilance.
  - You must constantly assess and update technology.
  - Fraudsters will not just go away, they will update their methods and targets to attack gaps.
  - Staying the same means falling behind.
- Competition for resources is real.
  - You must learn to convey the inherent risk without seeming to cry wolf.
  - Understanding the company’s risk tolerance is important.

Questions?

