KPMG

Industry insights:

Account takeover fraud analysis

By **Adil Palsetia**
Partner, Cyber Security
KPMG in Canada
416-777-8958
apalsetia@kpmg.ca

Account takeover fraud (ATO) involves criminals acquiring a user's details to take over their online accounts and continues to cause real impact to both customers (users) and the businesses they use. As criminals become bolder and their methods more sophisticated, financial institutions (FIs) are becoming more adept at identifying, monitoring, and managing ATO fraud both before and after it occurs. One of the key ways FIs protect themselves is through the three lines of defense model (3LoD).

For a sense of today's leading practices and how the 3LoD fits in, KPMG consulted with several leading FIs to examine how top organizations are managing ATO fraud.

The first line of defense

An organization's first line of defense (1LoD) is typically comprised of its business units (BUs) and centres of excellence (COEs). These, in turn, are supported by an informed and enterprise-wide approach to ATO fraud governance. Many peer firms have established group-level governance structures to promote intelligence-sharing between BUs and facilitate the escalation of fraud or cyber security issues as they surface.

Clearly defined roles are also central to effective ATO fraud governance. Governance structures are commonly overseen by accountable individuals from both the 1LoD and second line of defense (2LoD) fraud policy and oversight teams. Larger FIs have also assigned specific fraud prevention roles (or individual fraud specialists) within their BUs to drive the risk assessment process, manage cases, monitor ATO fraud control effectiveness, and act as on-site ATO fraud liaisons. Several have combined anti-money laundering (AML), cyber security, and ATO fraud initiatives into multi-disciplinary 'fraud centres' to take advantage of overlaps and shared data and resources.

- **Assessing the risk.** To manage ATO fraud is to understand its origins, its actors, and where the organization is vulnerable to fraudulent activities. Technology can be an ally in assessing an organization's gaps and weaknesses. An increasing amount of FIs are leveraging machine learning and data analytics tools (both in-house or off-the-shelf) to perform real-time analytics, pinpoint synergies between fraud and Anti Money Laundering (AML) systems, and leverage non-transactional data for overall financial crime insight. Some are also combining data from multiple channels to construct more holistic, accurate, and real-time view of their ATO fraud profile, which also serves to reduce false positives.
- **Addressing the risk.** Several measures are proving effective in reducing ATO fraud attempts. Among these are risk-based or two-factor authentication systems and biometric security gates, the latter of which is gaining traction in higher risk channels. Live chat services, AI 'bots', and virtual services are also being deployed to give customers the tools and skills to manage ATO fraud on the transaction end. No matter the control or fraud prevention measure, however, there is a consensus among peer firms that fraud prevention measures, while critical, must not compromise the customer experience.

  It is worth noting that these initiatives are being aligned with industry efforts and wider advertising campaigns geared toward enhancing customers' cyber security practices. Where issues have occurred with commercial or business customers, leading FIs are working closely with the impacted client to better understand their risks and help prevent recurrences.
- **Incident response plan.** Investigations and incident response plans are crucial to remediating ATO fraud events quickly and mitigating damages to both the company and customer. To ensure those plans are not left to collect dust on a shelf, many FIs have assembled fraud operation teams consisting of people experienced in digital forensics, law enforcement, and data analytics. These teams are typically responsible for interacting with customers, law enforcement, and regulators during an event. In some cases, FIs have embedded other financial crimes within this function to ensure external communications are consistent and well informed.
- **Reporting on the risk.** Several FIs are using a series of measures to reflect customer experience (e.g. interventions and false positives) to help determine if anti-fraud measures are increasing customer friction. They are also reporting on loss budgets and how they are aligning with their quantified risk appetite statements, but this is not yet widely performed outside banks.

The second line of defense

The 2LoD informs, defines, and monitors 1LoD ATO fraud strategies. What is more, it ensures alignment between BUs, enabling the intelligent deployment of resources and information where needed.

- **A central strategy.** Successful ATO fraud prevention strategies are backed by well-structured policies and standards that provide organizations with a baseline from which to formalize minimum expectations and responsibilities. Importantly, these strategies are reviewed and updated on a regular basis, which allows for sufficient flexibility to allow each BU to align to the overarching framework.

  Effective ATO fraud strategies also detail the direction of the fraud function as it relates to fraud IT solutions, analytics, resources, future threats, and required capabilities. Additionally, they include fraud prevention and recovery initiatives that are tracked to ensure they are not only working but in step with the organization's vision.

- **Establishing a risk appetite.** How comfortable is the organization with risk? What risks are worth taking, and which are better left unexplored? Only when an organization's appetite for risk has been clearly defined (and communicated) can the appropriate fraud controls be implemented, monitored, and measured against specific key performance indicators (KPIs)

- **Risk assessment oversight**. The oversight of risk assessments completed by BUs helps build an independent view of risk while challenging 1LoD assumptions and control effectiveness. Understanding this, many peer firms allow their BUs to conduct self-evaluations and risk assessments in a centrally defined template, which are then reviewed by 2LoD teams who perform additional testing if required. Some 2LoD fraud defense teams take their oversight function one step further by holding sessions throughout the year to track KPIs, help ensure risk assessments are relevant and up to date, and review changes in the firm's external or internal environment.

- **An intelligence-led approach.** Many FIs have found value in looking beyond their four walls for fraud prevention insights and best practices in order to stay current with industry trends, fraud threats, and prevention or detection innovations. This intelligence is being shared with relevant BUs and used to inform (and adjust) ATO fraud game plans and controls on an ongoing basis. FIs are applying lessons from their fraud incident investigations and root cause analysis into the risk assessment process to help enhance controls within both the impacted BU and the organization.

  The sources for external intelligence can vary between industry consultants, law enforcement agencies, industry bodies, market peers, and fintech companies. Several FIs have also established an Intelligence COE at the group level to disseminate fraud intelligence throughout the organization and add support to the broader financial crime function. That said, these CoEs were most commonly embedded in peer firms that operate primarily in one country.

- **Testing and reporting.** When performed at the 2LoD, ATO fraud testing ensures 1LoD processes and controls are functioning as expected. Leading FIs have dedicated fraud and financial crime resources to performing a combination of schedule assurance on key areas of risk and targeted reviews in response to specific threats. Where fraud reporting is considered, many FIs agree that facilitating reports from BUs to the group level enables the organization to better monitor long-term trends. This also grants senior management a picture of overall fraud prevention performance and control effectiveness. Some FIs some have seen the advantages of adding KPIs for customer metrics, such as abandonment, false positives and intervention rates in addition to typical metrics such as net loss against budget and number of fraud incidents.

The third line of defense

If there is a theme among first and second-line defenses among leading FIs, it is that ATO fraud is not an issue that can be addressed alone. That is why a number of institutions have looked to third-parties for leading ATO fraud program frameworks and leading practices.

Independent audits have proven equally important in ensuring the right controls are in place and performing as anticipated. Using data analytics, these audits can analyze complete populations of data to enhance random or systematic sampling traditionally carried out by internal audit functions.

Additionally, having an integrated assurance framework has helped numerous FIs achieve greater comfort over their coverage of risks and controls. These frameworks help align third line of defense (3LoD) activity with 2LoD and 1LoD business monitoring to help identify gaps, overlaps, and duplications in assurance. And while it is not necessarily common practice, some FIs prepare one integrated report to their Board or Audit Committee on the risk type, as opposed to providing independent 2LoD and 3LoD reports.

Overall, financial institutions tell us this integrated assurance provides a holistic and aggregated view of risk assurance (aka a 'one truth') while promoting collaboration across the organization

As cyber criminals are becoming increasingly confident in utilizing the most sophisticated hacking techniques, including Account Takeover Fraud (ATO), financial institutions are feeling the pressure to employ equally sophisticated and thorough defense systems. The three lines of defense model (3LoD) enables an organization to leverage the expertise of its people, big data capabilities and third-party contractors to design a patchwork of solutions tailored to the organizations specific needs. By assessing gaps in cyber defense and then building out a holistic framework based on identifying, monitoring, and managing ATO fraud both before and after it occurs, financial institutions can feel assured the right controls are in place for the continuous improvement of their cyber defense capabilities.

kpmg.ca/rethinkrisk
#rethinkrisk