Changing Fraud Strategies: Fraud Fighters

September 20, 2021

Editor's note: This is the second post in a three-part series.

I recently read about a payment company that responded to emerging fraud schemes by doubling its staff associated with fraud mitigation. The talent the company sought for these roles are in high demand, so I took to the job boards to see what hiring strategies emerged in relation to the trending fraud schemes.

Back in March, I posted the first of a three-part series on changing fraud strategies. That post looked at shifting trends in payments fraud. In this post, I share what I found on the job boards to illustrate how the approach to fighting fraud might be shifting in response to the new types of fraud. (I'll continue that theme in the third post.)

Account takeover fraud
Many of the listings I saw made it clear that organizations want candidates with account takeover expertise. I read statements like "Candidate must be capable and driven to identify, mitigate, and resolve account takeovers" and "Job duties include monitoring accounts, queues, and transactions for possible account takeover and to prevent processing of unauthorized transactions."

Companies are also catching on that account takeover fraud can't be mitigated by a single department of fraud fighters such as information security—it takes collaboration across many lines of defense. In fact, a recent report on account takeover fraud noted the critical need for organizations to ensure that all internal departments understand the organization's liabilities in accessing company networks, databases, employee information, and financial data. Job postings with a focus on account takeover had statements like "will work cross functionally across the enterprise" and "partnering across the enterprise to unify and strengthen strategies to address account takeovers."

New account opening fraud
Sometimes grouped with application fraud, these schemes are hard to detect, leaving many businesses vulnerable. Let's face it, businesses naturally want new accounts. If creating new accounts becomes an area of friction, that can affect a company’s bottom line.

That's why mitigating this type of fraud involves balancing the confluence of forces at play, including privacy, customer service, sales, and compliance. Based on some of the job listings I reviewed, organizations are showing signs of adjusting to the rise of risk here. For example, one bank was hiring a salesperson who "must adhere to new account opening procedures to prevent fraud." There were many openings that listed such compliance responsibilities.

One position specifically wanted a subject matter expert in detection, investigation, and prevention of synthetic, identity, and new account application fraud. The job also required extensive collaboration across the enterprise and with law enforcement.
Online fraud
You immediately get a sense of how widespread and varied online fraud is when you look at the listings for companies that are "urgently" hiring fraud analysts or researchers. Some of these companies are in mortgage, health care reporting, home improvement retail, telecommunications, or, of course, e-commerce.

Interestingly, I saw more than just entry-level or intermediate positions for online fraud workers. One e-commerce company was seeking a "head of eCommerce fraud operations." The company said the candidate should "have a passion for managing people" while also wanting to build an organization. A multinational technology company was looking for a "manager of payments trust and safety," who would be tasked with tackling the biggest problems that challenge the safety and integrity of their products.

It takes more than talent
Organizations have a high demand for workers who can help the whole enterprise focus on fighting fraud and who also have analytical and decision-making skills and can make changes to strategies and systems. Of course, talent is only one part of the fraud fight. In the final post in this series, we will explore how technology is being used to tackle the fraud trends.

By Jessica Washington, AAP, a payments risk expert in the Retail Payments Risk Forum at the Atlanta Fed

- September 20, 2021 in
  - cybersecurity
- Permalink
- Comments