STUDY ILLICIT 'EXFILTRATION' AND CRYPTOCURRENCY TO PREVENT FRAUD

Cryptocurrencies and cybercriminals aren't going anywhere. Here's how some fraud examiners discovered systematic patterns of attacker activity at a bank and instituted controls that protected the institution and helped a cryptocurrency exchange prevent future attacks.

COLUMNIST
PATRICK A. WESTERHAUS, CFE, CPA
CEO, CYBER TEAM SIX, LLC

Financial institutions, capital markets and government organizations are discussing, debating and developing a framework for how cryptocurrencies will fit within the financial services industry, and how to manage and regulate the risks of adopting technology.

Meanwhile, cybercriminals' evolving tools and techniques, which they use to quickly convert ill-gotten gains from customers' banks accounts into cryptocurrency, are challenging anti-fraud teams within financial institutions to keep up. And now Facebook's move into the cryptocurrency marketplace is heightening the tensions. (See "Washington Has Doubts About Facebook's Libra Payments Network," by Steven Russolillo, The Wall Street Journal, July 12, 2019, tinyurl.com/yyeuxehd.)

Cryptocurrencies and cybercriminals are here to stay. We can keep one step ahead by learning more about both that will help *all* organizations — not just financial institutions.

Toppling those silos

The usual challenge of developing fraud detection strategies to proactively identify bank account takeovers (ATOs) without creating too many false positive alerts is particularly difficult when layering on additional complexities like hunting for illicit money movement from bank accounts to cryptocurrency exchanges.

Creating these detection strategies requires a deep understanding of, and access to, near real-time cyberthreat data and an awareness of exchanges that cybercriminals frequently use.

Gaining this granular intelligence requires more than just developing working relationships with and/or co-locating anti-fraud and cybersecurity personnel within financial institutions and other organizations.

Even though the silos between anti-fraud and security teams within organizations are slowly breaking down, the skill sets they each maintain are vastly different. The division of labor, and lack of hybrid expertise and access to key data sets, unfortunately leads to less-than-meaningful dialogue on how to identify and prevent emerging cyber-enabled fraud trends. In the end, cybercriminals maintain the upper hand, and institutions are left trying to figure out what happened after crooks steal the money. We need to do more.

Many financial institutions — and the fraud examiners who work for them — acknowledge that they need to manage and mitigate cryptocurrency fraud risk, but they don't know where to start. They also wonder if it's worth their time and effort to develop strategies that in the end might only prevent a small percentage of the overall fraud across their product and customer bases.

We encountered this mindset before our cybersecurity intelligence team decided to study and quantify the problem. We knew from our previous law enforcement experience that banks need to spend time on emerging risks, especially given the rate at which cybercriminals are using cryptocurrencies to mask and move the proceeds of their ill-gotten gains.

After we 1) overcame data access challenges within banks (i.e., with transactional information, fraud claims data, etc.) 2) identified the right anti-fraud teams to partner with and 3) obtained permission to share the results with key external parties, we created:

- A real-time anomaly detection strategy with a low false-positive rate

and high fraud loss-avoidance impact (detailed below).

- A new layered security approach to make it harder for cybercriminals to use authentication loopholes (detailed below).
- A positive information-sharing experience with a U.S.-based cryptocurrency exchange that assisted in detecting the activity occurring on its platform.
- An information-sharing partnership with law enforcement.

Our approach

We began our study by running a simple query of a well-known U.S.-based cryptocurrency exchange in the retail transactional database and picked a year's worth of transactions from Jan. 1, 2017, through Dec. 31, 2017. The transactions totaled close to $1 billion, which we found extraordinary. However, the price of bitcoin during that period reached a high of $19,068 on Dec. 17, 2017 (buybitcoinworldwide.com/price), which could explain the enormous dollar amount transacted.

Then we queried the data against the fraud claims database and discovered millions in claims. Finally, we pulled the narrative from each investigation to determine a discernible pattern of how ATOs occurred for an ATO fraud strategy and information technology team (responsible for managing online authentication protocols) to test and implement a proactive anomaly detection strategy.

Results

The data revealed a systematic pattern of attacker activity at the bank that exploited online authentication protocols and account linking rules allowed by the institution. Cybercriminal attackers:

- Used a bank "whitelisted" cloud-service provider to mask their true Internet Protocol (IP) location. (Whitelists allow users more streamlined entry.)
- Exploited financial technology data aggregation services (e.g., Plaid and Yodlee) as platforms to affect the ATO of the bank accounts.
- Exclusively used Automated Clearing House to transmit stolen funds to the cryptocurrency exchange's wallet service, which is the equivalent of a bank account.
- Used micro-deposits (test deposits between financial institutions to link accounts to send money back and forth) or aggregator service logins (software that allows users to see entire financial histories) to link the exploited bank accounts to the destination exchange's crypto-wallets.
- Targeted retirement planning accounts (e.g., trust accounts) and other accounts with minimal online activity by customers.
- Used a "mule account" at the cryptocurrency exchange where the name on the exchanger account didn't match any of the authorized signers on the linked bank account.

After we provided our findings to the bank's ATO fraud strategy and information technology teams responsible for managing online authentication protocols, the bank implemented a real-time detection strategy, which searched for transactional pattern activity that matched the security loopholes detailed above. The strategy had immediate positive results (low false positives), and the fraudulent activity ceased.

Information sharing

We then contacted the crypto exchange and shared the attackers' tools, tactics and procedures, which allowed it to conduct an additional investigation on the addresses linked to the transactions we connected to exploited bank accounts.

The exchange proactively closed security gaps it discovered during its investigation. It also implemented fraud controls to identify account linking by monitoring for unusual micro-deposit activity. After the exchange and the bank completed their investigation, they shared the results with law enforcement.

Thwart cybercriminals' use of cryptocurrencies

It's no secret cybercriminals are using cryptocurrencies to hide their proceeds. Anti-fraud practitioners don't require a deep understanding of the cryptocurrency ecosystem to play an instrumental role in preventing cybercriminals from using this money exfiltration method.

Designing proactive and enhanced transactional monitoring on bank customers' accounts already linked, or attempting to be linked, to companies that facilitate exchange services for cryptocurrency can make a real difference in slowing down cybercriminals.

Our study included looking at the transactions with just one U.S.-based exchange, but we recommend you include many exchanges in your detection strategies to ensure comprehensive approaches. Several websites stay current on exchanges. We've found this to be a good resource: coin.market/exchanges.

Staying ahead of today's digital crimes is challenging and never-ending. Combat this fraud with proactive thinking and historical data studies. Stay in tune with cybercriminal's tools, tactics and procedures by collaborating with cyberintelligence teams and find mechanisms to share with external companies who play roles in the larger financial services ecosystem. ■ FM

Patrick A. Westerhaus, CFE, CPA, is CEO of Cyber Team Six, LLC. Contact him at patrick.westerhaus@cyberteamsix.tech.