

## On the Backs of Mules: Inside an Elaborate ACH Scheme

### Case Background

A community bank based in the U.S. Midwest recently intercepted an elaborate ACH fraud scheme involving unwitting mules and multiple financial institutions. With \$1B in assets, this case shows that fraudsters aren't solely targeting the largest institutions. This community bank (let's call it "CB" for short) is acutely aware that it must actively guard customer trust and its reputable brand against cybercrime.

### Fraud Incident Details

The victim was a nonprofit small business customer. Most likely using keylogging malware, the fraudster(s) were able to obtain the online account credentials of a fully authorized individual at the nonprofit. CB has three layers of online banking security that all failed: username/password, a challenge question, and the customer's unique PIN required to execute transactions. On the first day of the compromise, session logs reveal that the fraudster got oriented – looking at account balances, transaction history, and even modifying a pending ACH transaction – perhaps to test their privileges. The next day, they executed an ACH batch file containing 16 separate debit transfers – each of them under \$9,000 to stay undetected – for a total withdrawal of \$142,000. The transfers were sent to accounts at eight banks, all larger institutions, in states throughout the U.S. IP geolocation revealed fraudulent access to the compromised account almost simultaneously from both Oklahoma and Ohio, locations that were unusual for the victim, but not overly suspicious in their general proximity to the bank.

Recipient account owners were unwitting mules who thought they had been hired, albeit over the Internet, to do legitimate jobs. Most of the accounts were new and had been opened online. Mules were instructed to empty the funds from their account the day they arrived, to use Western Union to send the money to the fraudsters' bogus identities in Texas and Florida, but to keep 5% of the amount as "commission" payment for their services. [See the fraudsters fake employee handbook]

The victimized nonprofit had opted in to CB's business customer alerting on debit activity, so an email was triggered automatically. Unfortunately it was not read immediately, so the funds were already gone. CB scrambled to execute an ACH reversal file that same day. Quick action, luck, and direct follow up with the eight institutions resulted in blocking 12 out of the 16 transfers. Two of the mules were actually in their banks at the time trying to withdraw the funds, but were intercepted! One thought she was picking up a moving allowance to be relocated out of state; the other thought he was employed by an insurance company based in Switzerland.

### Prevention Tips

- 1. Bolster online account security measures.** As implemented, CB's login, challenge and PIN layers essentially amounted to three passwords easily compromised. Thresholds for challenges were based on simple geolocation rules that didn't trigger with the domestic access. Device ID cookies were subverted. Monitoring of online activity after the login could have revealed suspicious activity.
- 2. Don't wait for actual transactions to detect fraudulent activity.** Account reconnaissance occurred a day before the crime and could have been detected to prevent the fraud before it happened.
- 3. Beware of new retail accounts, created online, that immediately start moving large amounts of money.** Cooperate and collaborate with peers on known and suspected mules, who should be tracked. Mules often handle multiple fraudulent transactions at multiple institutions, and can flip from victim to criminal if they suddenly keep stolen funds for themselves.

For more information, please visit [www.guardiananalytics.com/fraud\\_informer/](http://www.guardiananalytics.com/fraud_informer/)

### About Guardian Analytics

Guardian Analytics is the technology leader in the prevention of online account fraud, providing real-time risk management solutions that protect online channels. The company supports the end-to-end online risk management process with rich analytics and behavior-based modeling. We offer an analytics-based software solution that addresses the entire risk management lifecycle.