

# Dualing for Control

August 2010



## Case Background

After a record year in 2009, fraud attacks against online business banking show no sign of stopping. Cyber criminals advanced their technologies and methods to continue stealing millions from online accounts, even as banks and businesses attempt to put more controls in place. Recent research from the 2010 Business Banking Trust Study reports in 80% of fraud attacks, money left the institution before it was noticed, leaving banks and businesses wondering which way to turn to fight the war against cybercrime.

Press, analysts, and associations have recently recounted story after story about fraudsters gaining unfettered access to corporate accounts by defeating strong authentication, even when one-time passwords are in use. And now fraudsters mastered the next step: defeating dual controls to successfully move money out of institutions unnoticed and seemingly fully “approved.”

When dual controls are employed in a corporate account, one online banking user must submit a transaction (a wire request, for example) and another user with the correct approval limits must approve the transaction before the request can be submitted to the institution.

## Fraud Incident Details

Circumventing dual controls has become a widespread phenomenon seen and reported by banks and businesses of all sizes across the country. This issue of Fraud Informer highlights two cases at two separate banks, one regional and one national, who recently experienced fraud attempts involving high dollar wire requests where dual controls were defeated.

Case #1: By infecting the computer of an online banking user at a small business with multiple Zeus banking trojans, a fraudster was able to steal the credentials necessary to bypass authentication and compromise the business’ online account undetected. Once logged in, the fraudster changed the user’s password to block access and immediately initiated two overseas wire transfers just under the company’s \$100,000 wire limit. Recognizing a second user was required to approve the transactions, the fraudster utilized the administrative rights of the compromised account to create a new user. Additionally, the fraudster increased the approval limits granting the new user permissions to approve the large dollar transactions. Logging in as the new user, the fraudster immediately approved both wires, effectively defeating the dual controls designed to protect the business against unauthorized transactions.

Case #2: A criminal compromised two separate online accounts at the same business. After defeating authentication and logging into the first account, the fraudster set up a wire transfer. The second compromised user, however, did not have a high enough approval limit to approve the wire. The fraudster attempted to change the limit on the second account, but was blocked from making the change. To bypass this, the fraudster completely deleted the second user account and then immediately and successfully recreated it with a higher approval limit. The fraudster proceeded to log in to the second account and immediately approve the wire transfer.

Both of these attacks took place within the span of a few hours, limiting the time the bank had to recognize and spot the account setup and user maintenance and react. In these two examples, the banks were successful in identifying the attack and no money ever left either institution.

Bonus: Other banks have reported fraudsters are manipulating the automated alerts companies set up for transfers or account maintenance. This allows them to set up new users, change approval limits and transfer money without anyone at the company noticing. Using the administrative privileges of the compromised account, fraudsters either redirect or delete email alerts. Some fraudsters will even compromise the victim’s email account to delete the alerts as they come in, keeping companies in the dark as money is siphoned out of their accounts.

# Dualing for Control

August 2010



## Prevention Tips

Dual controls are a good measure to have in place, but it is not a fail-safe control. Fraud Informer recommends the following actions to avoid falling victim to the types of schemes described above:

**1. Encourage business customers to limit the number of accounts with administrative rights to create and modify users.**

Users should only log into this account to perform user maintenance, and not for day-to-day online banking use.

**2. Watch for changing authorization levels.** For most businesses (but not all) changing a user's level of authorization is an uncommon occurrence. If other risky behavior specific to an account is observed in addition to changing authorization levels, banks should investigate. Behavioral analytics is a powerful approach to evaluate the level of risk of behaviors and activities for any given user (otherwise, banks can spend hours on 'false alarms').

**3. Beware of new users, created online, that are immediately used to request or approve large transfers.** New users with rapid-fire activity are extremely high risk. Banks should be prepared to identify and investigate accounts with new users added, prior to any transactions leaving the bank. Accounts with multiple high-risk behaviors should be top-priority for investigation.

**4. Be on the lookout for alert manipulation.** In combination with other risky behavior, redirecting or deleting alerting rules is a significant red flag and a good indicator that money may be transferred soon.

**5. Be prepared to act quickly.** These schemes took mere hours to unfold. Have policies in place and real time access to appropriate people who can confirm high-risk activities and accounts.

**6. Be prepared to swiftly adjust your definition and detection of risky or suspicious behavior.** Fraudsters are continually changing the schemes and techniques used to avoid detection. Fraud rules to detect any of the above high-risk behaviors will quickly become out of date. The most effective way for banks to stay nimble is to establish a pattern of normal behavior for each user in their corporate banking accounts and use behavioral analytics to determine risk-levels.

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.