DIEBOLD NIXDORF PERSPECTIVE

An insider's guide to thwarting transaction reversal fraud

By David Phister, Director in Systems Product Management for Security, Diebold Nixdorf

In the security field, we've all heard some variation of the phrase *"We build a 10-foot wall, they build an 11-foot ladder"*. But what often gets forgotten is that criminals don't always build a *taller* ladder – sometimes it's a *different* ladder. So as the industry focuses on mitigating risks against skimming, black box and malware-based cyber attacks, criminals have reverted to lower-tech methods of stealing cash, the latest being transaction reversal fraud (TRF).

How does TRF work?

In a TRF attack, a fraudster makes a cash withdrawal at an ATM but tricks the host into thinking the cash was not dispensed, when in fact it has been taken. The ATM registers an error, and so the withdrawal typically does not get debited from the account. This type of attack thus does not target the accounts of individuals, but rather attacks the bank's funds directly.

Although TRF is a global problem, we've seen it surge in popularity in Europe over the last couple years as EMV and other anti-skimming defence mechanisms have taken hold. According to EAST, incidents of TRF across 11 European countries increased by 147% from 2015 to 2016, and another 88% from the first half of 2016 to the first half of 2017.

Take a closer look at your transaction policies

Tweaking your network's transaction business logic is a smart first defence against TRF. Many hosts automatically refund an account when there is an error in cash presentation, especially those with older terminals that may not have had every configuration and software update applied. We recommend that banks review their transaction business logic for debiting and crediting accounts when unknown or errored states occur; if an invalid state is detected, then the transaction should not be automatically reversed.

Take a closer look at your technology

If your terminals have recycling capabilities, they can use 'bank note validators' to confirm the return bundle value and respond accordingly. Smarter systems that can detect and correlate the states of multiple components (i.e. the card reader, cash module, cash slot camera, etc.) should focus on error condition processing to increase a system's ability to detect, prevent and be alerted to invalid or suspicious states. Certain errors are more indicative of fraud, and if those particular conditions are detected, the transaction code should not be reversed. Finally, monitoring and alarming are key to detecting potential fraud scenarios. Cash slot cameras, for example, can sense manipulation and respond with an alert.

The right software, monitoring tools and cash module innovations can help drastically reduce the opportunities for fraudsters to execute TRF attacks on your network. Smart dispensing and recycling solutions, like those employed on many Diebold Nixdorf terminals, are designed to automatically protect against TRF through intelligent deposit technology that is standard in the machines.

TRF is a low-tech problem, but if thieves have taught us anything over the past 50 years, it's that they'll use any and every method available to compromise ATMs – because where there's money, there's crime. ■

Learn more about Diebold Nixdorf's comprehensive, multi-layered approach to security at DieboldNixdorf.com/Security.

David Phister
Diebold Nixdorf

Diebold Nixdorf