

Fraud Protection Awareness Series

Case Study: Consumer Fraud Scam Puts Company at Risk for Months

Please note that this case study represents an aggregation of actual scenarios brought to CoBank's attention, though company names have been changed.

Situation

Savvy Bank started receiving calls from consumers and banks that had received checks appearing to be from Proactive Company, which is a legitimate Savvy Bank customer. The checks were counterfeit and were being sent to consumers as payment for goods being sold on an online auction site. The checks were printed for amounts significantly higher than the price of the goods being purchased and usually arrived via overnight mail with instructions to deposit the checks and send a portion of the difference to a third party, minus an "inconvenience fee," via a retail money transfer service.

This scam ran from February to November. Every few months the consumer fraud victim base was changed, for example, from online auction purchase scams to work-from-home secret shopper scams, to car decal advertising scams. By the time activity had stopped, there were a total of 250 checks totaling almost \$1 million.



Discovery and Resolution





This large scale counterfeit check case did not result in any monetary loss for Proactive Company because they used a fraud protection service called "Positive Pay." This service allows account holders to review and decision exception checks every day. Due to this service, all the counterfeits appeared as exceptions and the company decisioned them to be returned with a FRAUD reason code.

Commercial customer fraud protections differ greatly from those of a consumer. While consumers are very well protected against fraud, commercial customers only have 24 hours to identify and return unauthorized items debiting their accounts. If the return deadline is missed, a lengthy manual claim process between banks is required. Recovery is never guaranteed and the dispute process can last 90 days or more. Due to this deadline, it is imperative to reconcile account activity on a daily basis and report any unauthorized items to your bank immediately.

How it Happened

Counterfeit checks always result from a compromised account number, which can occur in many ways. One of the most common methods is via intercepted checks that are mailed to recipients. Once an account number is compromised it will always be compromised.

Watch for These Red Flags

-  **Outgoing checks to vendors are left in an unsecured street-side mailbox.**
Fraudsters intercept checks to use for alteration and counterfeit purposes.
-  **Blank check stock is left on a desk in the lobby area in plain view of all people entering and leaving the building.**
Blank check stock should always be stored in a secure place out of sight. The account number can be compromised without any missing checks.
-  **Images of uncashed checks are sent out to customers or other vendors.**
Never email check images to external email addresses. There are many ways fraudsters can intercept and view emails and steal the account numbers.
-  **Account reconciliation takes place weekly.**
Account reconciliation for commercial customers must be daily in order to identify and report unauthorized items within the 24 hour return window.