PROVIDENCE BUSINESS NEWS
PBN
pbn.com YOUR SOURCE FOR BUSINESS NEWS IN SOUTHERN NEW ENGLAND | MARCH 2–8, 2018

GUEST COLUMN | STACEY NAKASIAN

The check fraud pandemic

CHECK FRAUD IS ON THE RISE and poses a real threat to local businesses. According to the 2017 Payments Fraud and Control Survey conducted by the Association for Financial Professionals, 74 percent of the companies surveyed experienced some form of payment fraud in 2016. That is the highest percentage for any year in the last 10 survey years. The survey also reports that check fraud continues to be the most commonly reported form of payment fraud, with 55 percent of the companies reporting instances of check fraud in 2016.

The increase and prevalence of check fraud can be explained by the availability of high-quality, low-cost document scanners and graphics software. Armed with such tools, a counterfeiter easily can produce a counterfeit check by scanning an original check and then manipulating the digital image to change the payee, check amount or other information without altering the drawer's signature and other features of the original check.

Given the quality of counterfeit checks produced using these methods, the checks are often paid and the counterfeiter long gone before the fraud is discovered.

Bank transactions are governed by the Uniform Commercial Code, which contains well-established rules about who bears the loss when a forged or altered check is paid. Under the UCC rules, in most cases the banks that accepted and paid the fraudulent checks will bear the loss, rather than their customers.

To address this risk, banks have developed programs to detect and prevent fraud losses and, as permitted by the UCC, customer agreements now commonly state that customers who decline such fraud-protection services will be liable for any loss the services could have prevented. Such agreements may be enforceable. As a result of these developments, commercial banking customers may face liability for check-fraud losses, even if they were not in any way at fault in allowing the fraud.

One of the most prevalent and effective check-fraud detection programs is "positive pay." A bank customer enrolled in positive pay will regularly (usually on a daily basis) transmit electronically to the bank a list of checks they have issued. The list will include for each check written the check number, the amount of the check and, in some cases, the name of the payee. As checks are presented to the bank for payment, the bank's positive-pay system compares the checks to the information previously provided by its customer. If the information does not match, the item is flagged for further review. Many banks also offer reverse positive pay. That service enables a bank customer to review checks presented to the bank for payment before they are paid to confirm the checks are genuine and unaltered.

Although these are by far the most common fraud-detection programs banks offer, account holders should review all programs to determine which are best suited to the account holder's business in light of the nature and extent of the banking transactions.

Of course, companies need to have internal protocols to prevent the creation of unauthorized or altered checks. But companies should also assess whether their bank accounts are adequately protected against losses due to check fraud. They should determine what fraud-protection programs their banks offer and evaluate which would best protect their business. And they should carefully review the terms of their account agreements to determine what exposure they might face if they do not participate in the available programs. ■

Companies need ... internal protocols to prevent the creation of ... altered checks.

Stacey Nakasian is a partner with Duffy & Sweeney in Providence. She can be reached at snakasian@duffysweeney.com.