Finance New Mexico
Article 271 December 10, 2012

Crooks Target Businesses with Creative Scams

By Fidel Gutierrez, Senior Vice President, Los Alamos National Bank

In an age when many products sell in cyberspace and the buyer and seller never meet, creative crooks are finding new ways to defraud businesses — especially web-based businesses and individuals selling items through online platforms.

One scheme involves counterfeit versions of a time-honored currency – the cashier's check.

Scammers commit cashier's check fraud using an authentic-looking cashier's check to buy a product. The seller deposits the check and her account is charged for the amount when the check bounces back to the bank as a fake.

Another version of this scam involves checks written for more than the sales price. The "buyer" typically asks the seller to remit the excess funds via a wire transfer or Western Union, offering a superficially plausible reason for the overpayment. When the phony check bounces, the seller is liable for the entire amount.

While this scam usually targets individuals, businesses can also fall prey. To protect themselves, businesses should accept only easily verifiable payment methods.

Counterfeit Checks

Scams directed at businesses often exploit new technology to commit classic crimes.

Some crooks use bogus checks they design on a computer and print out at home. Others steal checks from the mail — especially mail left in unlocked mailboxes or even overstuffed curbside mailboxes — and use them to make purchases or get cash before the bank alerts the victim that her account is overdrawn.

Some thieves "wash" the checks, removing the intended recipient's name and substituting their own. Stolen checks can also become templates for new checks bearing the account holder's account number and information.

Even a deposit slip provides enough information for a scammer to use the routing number and account number to divert money from the account holder's account to an account of his making.

When phony checks are used at a business, both the actual account holder and the business are victims. For this reason, many merchants are rejecting checks from people they don't know and accepting payment only by credit card, debit card or cash.

Repackaged Ripoffs

Two other common scams involve tampering with merchandise to obtain refunds or to get big-ticket items for small-ticket prices.

One ploy is to swap a price tag or bar code from an inexpensive commodity and place it on an expensive one, hoping an inattentive or distracted cashier doesn't notice the switcheroo. Or the scammer can attempt to attach the big-ticket bar code to something she bought earlier and returned it to the store for a refund.

Checkout clerks and returns department employees should be trained to compare bar code data against the item being returned or purchased.

Other thieves switch products in the store, putting expensive items in boxes that once held less expensive products. Cashiers should be alert to any box that looks like it has been opened or tampered with.

Crimes like this can devastate a business, especially a small one with limited resources. To riff off the cautionary adage, "seller beware."

Los Alamos National Bank uses encryption and multiple layers of security to protect customers from banking fraud. For more information about LANB, visit www.lanb.com.

Finance New Mexico is a public service initiative to assist individuals and businesses with obtaining skills and funding resources for their business or idea. To learn more, go to www.FinanceNewMexico.org. Sponsored by: