ANY LOSS PREVENTED IS ADDITIONAL PROFIT FOR YOUR BANK

SECURITY OFFICER'S BY-WORD

By
Charles M. Towle
Senior Vice President

Suggestions on How To Prevent Losses From The Internet Buyer Scam

In the Internet Buyer Scam, often originating out of Nigeria, a seller of an item over the internet is conned by the buyer into accepting a worthless check for a larger than required payment and sending the buyer or an accomplice the extra funds. This scam has been so successful that crooks everywhere are seizing the opportunity as well. The scam is growing exponentially and is likely to affect all banks multiple times over the next few months. Banks need to take immediate steps to curtail these scams.

Customer education and customer knowledge are the most effective ways to curtail these scams.

1. Training your employees is your first defense against these scams. When customers ask, "When will the funds be good?" some bank personnel respond with the date the funds will be available for withdrawal under the Expedited Funds Availability Act. Customers may blame your bank if they feel your employee told them a check would be "good" after X days. Make certain all of your employees understand the difference between "When will I know the check is good?" and "When will your bank allow me to withdraw funds from this deposit?" The answer to the first question is "You will never know for sure. In some cases, the customer, as the endorser, remains liable for several years." Available funds and good checks are different. Make sure your employees can and do explain both to the customer, regardless of how the customer asks the question.

2. Provide notice to your customers that these scams exist. Try to make sure they know that any transaction in which they deposit a check and then send part of the money to someone else - particularly a stranger - is risky. If a transaction involves depositing a check and then sending part of the money to a stranger in a foreign country, it is almost certainly a scam which will cause a financial loss. Warn your customers with statement stuffers, website warnings, and posted notices. Try to get press releases in the local papers.

3. **When a customer is making a large cash withdrawal, sending a wire or purchasing a large Cashier's Check, give the customer information regarding these scams.** That knowledge may prevent a loss to both the customer and the bank.

4. For large Cashier's Checks being deposited, have the tellers (or other employees) call the bank on which the check is purportedly drawn and verify that that the drawee bank made that check to that payee for that amount. (The time you take will almost certainly prevent large losses to both your bank and your customers well in excess of the extra cost of making the calls. These scams are happening hundreds of times daily all over the United States)

5. For business customers that have significant balances, you should encourage them to use a positive pay program. This allows your bank to return large "fictitious" checks within the required midnight deadline. The frequency of these scams makes this a necessity.

6. If your employees think something is odd or suspicious, verify any deposited item. If it is a Cashier's Check, you should verify it with the bank it is drawn on. If it is a check drawn on a business account, you should verify with both the bank and the business. Verify the check number, amount, and payee. **However, even after verification, do not promise your customer that the check is good; let them know that the check can still be returned for various reasons beyond your control.**

Increase and Hold Large Deposits with BANK DEPOSIT GUARANTY BONDS ! !