

### **Customer Notice**

#### **Fraud Alert**

Scammers have come to rely on their victim's perception of "security" provided by cashier's checks, official bank checks and regular checks. Advanced graphics and printing technologies allow scammers to easily create fraudulent and hard-to-detect counterfeit checks in a matter of minutes, adding a sense of legitimacy to their scams. Fraudulent checks can appear to be very real that it is difficult for consumers, or even bank employees to detect.

Generally, if your bank credited your account, it could later reverse the funds if the check deposited is found to be fraudulent.

Online Auctions, Classified Listing sites and Overpayments, are some types of common scams. Scammers might visit an online auction or a classified listing site and offer to buy an item for sale or pay for a service in advance. Then they proceed to send you or deposit a check for an amount higher than your asking price. Once brought to their attention, they will apologize for the oversight and ask you to quickly return the extra funds purposely sent. The scammer's motive is to get you to cash or deposit the check and send back legitimate funds before you realize that the check you deposited is fraudulent.

## Be Suspicious about a check if:

- A check was deposited into your account for an amount larger than expected.
- The depositor is giving you detailed instructions in how to deposit the check.
- The fraudster will ask you to send money back in the form of a Wire transfer, Money order, gift card or any other form of immediate payment.
- If you are asked to deposit the check promptly and return any funds.
- The fraudster will insistently ask you to return any excess funds.

# Here are some ways to avoid becoming a victim:

- **Never provide personal information**, including your main identification number, account numbers or passwords over the phone or internet. If you did not initiate the communication, you should not provide any information.
- Never click in the link in an email that you suspect may be fraudulent. It may contain a virus that can contaminate your computer.
- Do not be intimidated by an email or caller who suggests dire consequences if you do not immediately provide or verify financial information.
- Never provide your password over the phone or in response to an unsolicited internet request. A financial institution would never
  ask you to verify your account information online. Thieves armed with this information and your account number can help themselves
  to your savings.
- Review your account statements regularly to ensure all charges are correct. If your account statement is late in arriving, call your bank to find out why. If your bank offers electronic account access, periodically review activity online to catch suspicious activity.
- When in doubt. Always contact your bank.

## Other Tips:

- Make sure the check is issued against a legitimate bank.
- Check with the bank that supposedly issued the check to make sure it is real.
- Scammers often communicate with their victims via text messages or e-mail.
- Determine if the amount of the check is corrected and as expected.

