FARM CREDIT

FRAUD PROTECTION AWARENESS SERIES

Fraud Tip #7 – Consumer Scams

As part of our continuing commitment to our customers' security, this quarter's article on payments fraud deviates from fraud schemes that affect businesses to those that prey on consumers. Business and consumer fraud schemes share many of the same characteristics, so being aware of the techniques used to defraud consumers can also help you identify those targeted at businesses.

Unfortunately, consumer scams are even more prevalent than business scams. While the elderly may be the prime targets of consumer scams, they are not the only victims. People from all walks of life – regardless of income, occupation, age or education – are victimized by scams every day. These scams, which are boundless in their creativity, succeed because the scammers have convinced their victims that their requests are legitimate and that they can be trusted.

Types of Consumer Fraud Scams

- **Online marketplace/auction scams:** A targeted buyer negotiates a final purchase price for an item that seems exceedingly low. The negotiations are often completed offline from the auction/marketplace site through personal email or text messages. The seller requires payment through a money transfer company, such as Western Union or MoneyGram. After the buyer remits his or her payment, the purchased product is never delivered, because the sale posting was not real. The funds paid cannot be recovered.

- **Phony check/overpayment scams:** A counterfeit or altered check is sent to a victim as payment for an internet marketplace purchase, an apartment deposit or some other purchase. The check is for an amount considerably higher than the agreed-upon price. The scammer, claiming this was a mistake, asks the victim to deposit or cash the check and return the excess funds (minus an inconvenience fee) through a money transfer service.

  Several days or weeks later, the check will be returned to the victim's bank unpaid ("bounced") because the authentic-looking check was either stolen and altered, or a counterfeit. The funds paid cannot be recovered.

- **Lottery/Sweepstakes/"Nigerian 419" scams:** The fraudster communicates with the target victim by email, telephone, fax or direct mail, informing them they are a winner in a multi-million-dollar lottery or sweepstakes, such as Publishers Clearinghouse. However, the winner must pay an "upfront fee" or "taxes" to claim the prize, using a money transfer service.

  In "Nigerian 419" scams (referring to the Nigerian law that outlaws fraud), a scammer offers a victim a share of a large sum of money, often in the tens of millions, in exchange for help in getting the funds out of a foreign country. The victim must pay certain fees or expenses, using a money transfer company, in order to secure the larger sum.

  In both cases, the award or money share is never delivered, and the fees paid through the money transfer service cannot be recovered.

- **Romance scams:** A scammer targets dating web sites with the goal of establishing a romantic relationship with a victim far away. After the relationship has developed, often with the use of fake family photographs and pledges of undying love, the fraudster asks the victim for money for travel expenses so they can finally meet in person – but the travel and meeting never happen. Depending on the depth of the relationship, a victim could also be influenced to send money for other needs, such as a medical operation or temporary living expenses. Of course, the money sent cannot be recovered.

- **Emergency scams:** A fraudster poses as a relative or friend and requests money for an emergency situation, such as a robbery in a foreign country, an auto accident, posting bond in an arrest, etc. Typically, the funds must be sent quickly using a money transfer service. A particularly insidious variation on this scam is known as the "grandparent scam," in which the supposed relative in trouble is a young adult grandchild, and the victim is a grandparent. Fraudsters use social media such as Facebook to identify their victims in these scams. Once sent, the "emergency" funds cannot be recovered.

- **Tech support scams:** The victim is contacted by email or telephone by a fraudster posing as a tech support associate with a well-known software or security company, such as Microsoft. They say that they have discovered malware on the victim's computer and request remote access to fix the problem. They also may offer antivirus software for purchase. With remote access, the scammer can access the victim's personal information, place malware on the victim's computer or obtain credit card information if the customer is persuaded to purchase software from them.

Why Consumer Scams Are Effective

- *Consumer scams often depend on the creation of an emotional bond – a great price on a high-demand item, the prospect of a huge sum of money or a long-sought romance.* Scammers are adept at weaving convincing tales that draw their victims in emotionally and cause them to overlook the obvious red flags of fraud.
- *Similarly, scammers are effective in creating a strong sense of urgency – the need for the victim to act immediately before something terrible happens or a great opportunity is lost.* This is a prime manipulation technique used by fraudsters, so beware if you are being asked to do something immediately.
- *Counterfeit check scammers rely on federal banking laws, which require banks to make deposited check funds available to account holders within a matter of days.* Just because funds are available does not mean that a check has cleared and that the funds are legitimate.
- *Scammers are tech-savvy. Depending on their level of sophistication, fraudsters can use their skills to take control of existing email accounts or create convincing "spoofed" versions of legitimate ones.* Spoofing involves creating a fictitious email address that closely resembles the actual one, so at a glance, the email appears to be from a legitimate sender.

How to Detect, Prevent and Protect Yourself from Consumer Scams

- As the money transfer companies caution, **never** use a money transfer service to pay for an online marketplace or auction purchase, regardless of how trustworthy the seller may seem, or whatever protective measures they may offer to put in place.
- Never send funds using a money transfer service to someone you don't know and don't trust implicitly. If a request is legitimate, there will always be other methods by which the funds can be sent. If a money transfer is the **only** option, require ID validation for the receiving party.
- Always verify emergency requests. A quick phone call or text to a known phone number will often help determine if the emergency is real.
- Be extremely cautious with unsolicited checks or checks written for higher amounts than expected. Checks can still be returned as counterfeit even if your bank makes the funds available quickly.

- Closely examine the address from which you received an email with an offer or request for funds to ensure it is accurate – with no added punctuation or misspelling in an address that might seem familiar – and avoid clicking embedded links or attachments in unknown emails.
- Use your gut instinct. If a situation or offer seems strange or too good to be true, look at the facts and ask yourself why you have concerns.

As you consider this information focused on consumer fraud, please also bear in mind your important role in the fraud detection and reporting process in your business. Your vigilance in reviewing your accounts and transactions is vital to fraud prevention and detection. Fraud schemes – as well as loss recovery efforts and outcomes – can be complicated. Early detection and prompt reporting of a fraud incident is critical because the passage of time might adversely affect the potential recovery of a fraud loss or the outcome of a customer claim. Your attentiveness is often the first line of defense for fraud, and if a fraud incident occurs, your diligence might aid in a potential loss recovery.

We hope you find this fraud protection information helpful, and thank you for your ongoing attention to protecting yourself and your business from fraud.