Keeping Your Money Safe: Overpayment Scam

Ashlie Hagemann, Fraud Supervisor

Businesses and individuals lose billions of dollars every year due to fraud. While PlainsCapital Bank has a seasoned fraud prevention team in place to protect our customers, we understand that the best protection is education. To that end, our Fraud Prevention Series, "Keeping Your Money Safe," highlights the latest fraud scams with helpful tips on how you can avoid them.

These days, online auction sites can help you buy or sell just about any product you need, regardless of location. Online auction sites are an increasingly popular way for people to earn some cash in exchange for items they may no longer need, such as furniture, fitness gear, or home technology. While you might be eager to sell your nonessential possessions for a profit, knowing about common fake check scams like the overpayment scam can help make sure you don't fall prey and guide you toward a successful transaction.

How Does the Scam Work?

Overpayment scams, also known as selling goods scams, target consumers selling high-ticket items through online auction sites or classified ads. It typically starts when someone you don't know replies to your auction posting and offers to purchase your item by check or a funds transfer service. They'll send you a check for an incorrect amount – often thousands of dollars in excess – and provide a false reason for giving you more than they owe. For example, they claim the additional funds are meant to cover shipping costs or it was a mistake. The scammer will ask the seller to deposit the check and wire back the difference, but when the bogus check bounces – possibly several days later – you're left without the "purchased" merchandise, your promised payment, and the money you wired the criminal.

As new digital payment methods develop, new variations of overpayment scams evolve as well. Instead of a traditional check, the scammer may use online services such as PayPal to overpay, often citing a fake receipt of payment and claim that funds are frozen until you wire or forward back the excess. The result is the same; you will never recover the "purchased" items, promised compensation, money sent to the scammer, or the opportunity to accept future offers on your sale.

Stay Alert for These Red Flags

Unscrupulous "buyers" use all sorts of bizarre and sometimes scary tactics to try to trick sellers out of money. In order to spots fraudsters attempting this scam, watch for these red flags.

- A fraudster requests access to your computer (computer repair company, etc.). If you give anyone access to your computer, be sure that your security and malware is up to date and run a scan immediately afterwards, even if you did not give out any of your online banking information. The fraudster could have loaded a virus or malware to your

computer to obtain access.
- Someone contacts you to say you are receiving a refund. They later get back with you, explaining that you were overpaid and need to return the overpayment via wire/ACH even if you see the “overpayment” funds in your account. Beware that the request may seem to come from someone reputable like the Better Business Bureau.
- A fraudster changes the wire instructions they originally sent you via email. Be sure to verbally verify all wire instructions by calling the requester of the wire at a known phone number.
- Look for out-of-area or unrecognizable phone numbers. If you don’t recognize their phone number or they call with multiple phone numbers, this could be a red flag you’re a target of an overpayment scam. Even if their phone number appears to be legitimate, be aware that scammers can “spoof” phone numbers to appear local, when they’re actually many miles away or in another country.
- Watch for muddied language. Poor spelling, random capitalizations, confusing sentence structure, and chunks of text copied and pasted from your listing may be clues to a potential scam. If the fraudster is located out of the country, it’s possible they used an online translator to communicate and fool you into thinking they’re local.
- A person calls you, claiming they are from the PlainsCapital Fraud Department, and asks you to verify a transaction and your identity by having you log into your online banking and then providing them the verification code that is text to you. The PlainsCapital Fraud Department will NEVER ask you for this information! If you have concerns about who you are speaking with, call your local branch and ask to be transfer to a fraud department employee.

How to Prevent an Overpayment Scam

While scammers are continuously developing their approach, there are steps you can take to protect yourself. The following are some tips to help you avoid overpayment scams.

- Investigate the unusual. If something smells “fishy” or doesn’t feel right, trust your intuition. Independently confirm your buyer’s name, telephone number, and street address to make sure you’re dealing with a legitimate buyer. If you’re suspicious about a request or the authenticity of a check, call their bank to confirm before you deposit.
- Never wire back funds. If you’re ever asked to wire back funds, terminate the transaction immediately, as this type of request can indicate you’re a target of an overpayment scam. Even if the crook provides a convincing reason to wire back the money, do not send them the merchandise, deposit the check, or send them money. There’s almost no legitimate reason for a stranger sending you money to request a

portion back.
- Reconsider buyers who can't justify why they can't meet in person. Be cautious of interested buyers who are suddenly unable to meet face-to-face as this could be a sign they're disguising themselves as someone else or they don't actually live nearby. They might also claim to be in another country and suggest someone they know in the U.S. can send you a check. If their reason for not meeting sounds too complicated to be true, it probably is.
- Resist pressure to act quickly. Because overpayment scam victims only have a short period of time before they realize their deposited check is counterfeit, scammers often fabricate reasons to rush the seller to cash the check, ship the merchandise, and wire back funds. An honest buyer shouldn't pressure you to expedite these steps; if their offer is good now, it should also be good when the check clears.
- Be alert that scams exist and can happen to anyone. Regardless of age, background, or income level, scams target everyone and they're on the rise. The Federal Trade Commission found consumers lost $406 million to fraud in 2017 and almost $1.48 billion in 2018. Overpayment scammers hunt for victims by scanning newspaper and online listings, and wait for someone to take the bait. If you believe you've been targeted in a overpayment or selling goods scam, report it immediately to fraud.org and the appropriate law enforcement agencies will investigate.

Keeping Your Money Safe

The criminals behind the overpayment scam can be extremely convincing. The best defense against falling prey is to stay alert, trust your instincts, and educate yourself about common fraud tactics.

PlainsCapital Bank's Fraud Department provides educational resources for businesses and customers to help detect and prevent fraud on their accounts. For more information about our fraud prevention efforts, visit our fraud resources page.