Fraud Policy

Fraud Awareness:

At Broxel, protecting customers is a priority. It is our goal to educate consumers on ways to safeguard their money and personal information and avoid becoming a victim of fraud. We believe that educating consumers about fraud is important so that they can take action to protect themselves. To educate yourself on the most common types of consumer scams, please see section Types of Fraud/Scams. Please keep in mind that new types of fraud scams pop up every day. Fraudsters are constantly creating new ways to defraud consumers. So, it's important to remember to always use common sense when sending money and using prepaid cards.

Fraud Prevention:

The number one rule in fraud prevention is to "know the person you are dealing with". Send money only to people who are known to you. Never send money or give your prepaid card details to a stranger or someone you do not know personally.

A fraudster's goal is to trick you into giving them money all the while knowing that you won't be able to recover your money once sent. The best way to stop them is to learn how they might try to trick you. That is why Broxel is committed to providing consumers with the information necessary to prevent them from becoming victims of fraud.

Remember that most consumer fraud starts with contact from a stranger. Protect yourself from being scammed by NEVER sending money to someone you don't know or have a legitimate business relationship with.

It is Broxel's goal to help prevent consumer fraud by educating consumers on the different types of consumer fraud/scams.

Types of Fraud/Scams

Below are some of the common type of frauds/scams that you should be aware of:

Identity Theft

Identity thieves use personal information (e.g., Social Security numbers, ID numbers, bank account information, credit card numbers, etc.) to pose as another individual. They may use this information to send an unauthorized transfer, open a prepaid access account or to drain an existing client's account. Please see below some common identity theft red flags.

Clues That Someone Has Stolen Your Information

- You see withdrawals from your accounts that you can't explain.
- You don't get your bills or other mail.
- Merchants refuse your checks and/or credit/debit cards.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You get a notice that your information was compromised by a data breach at a company where you do business or have an account.

Unfortunately, identity theft happens. But there are certain steps you can take to help keep your personal information from falling into the wrong hands. The following are ways to keep tabs on your identity and personal information to minimize your risk of becoming a victim of identity theft:

• Read your account statements carefully and often.

- Know your payment due dates. If a bill doesn't show up when you expect it, look into why.
- Read the statements from your health insurance plan. Make sure the claims paid match the care you got.
- Shred any documents with personal and financial information.
- Review each of your three credit reports at least once a year. It's easy and it's free.

For more information and tips on how to detect and prevent identity theft, please visit www.consumer.ftc.gov.

To report identity theft, go to www.ldentityTheft.gov for instructions and information on how to file a report.

IRS/Tax extortion scams

Have you received a phone call from a person claiming to be from a government agency asking for money to cover "back debts" owed to the IRS? They may say that you can wire the money or send a prepaid debit card to settle this amount owed - and if you don't, you will face jail time. Even though these calls may have a Washington, D.C. area code or misleading information on caller ID, rest assured that any "government employee" contacting you and asking for money upfront is a scammer.

Victim is contacted by someone claiming to be from a governmental agency saying that money is owed for taxes, and it must be paid immediately to avoid arrest, deportation or suspension of driver's license/passport. The victim is instructed to send a money transfer or purchase a pre-loaded debit card to pay the taxes. Government agencies will never demand immediate payment or call about taxes without first having mailed a bill.

Refund scams

Did you receive a call from someone claiming to work with the FTC? Was the caller promising to help you get a refund from the agency? This is a SCAM. Never send money or provide bank account numbers and other sensitive information to those promising you refunds. Remember; the FTC doesn't make outgoing phone calls to contact people, they don't ask consumers to provide banking or sensitive information, they don't ask you to send money, and if refunds are part of a FTC settlement, the FTC provides the funds by check. Even if the Caller ID says the name of an organization you recognize or trust, be skeptical. Scammers will use technology which can display legitimate numbers which coerce you into responding.

Charity scam

The victim is often contacted by email, mail or phone by someone asking for a donation to be sent by money transfer to an individual to help victims of a recent current event, such as a disaster or emergency (such as a flood, cyclone, or earthquake). Legitimate charity organizations will never ask for donations to be sent to an individual through a money transfer service.

In times of disaster, it's important to be aware of charity scams. There are many legitimate ways to provide support to help people impacted by floods, earthquakes, fires, other natural disasters or even man-made disasters. If you're eager to make a donation, give in a way that you have donated before or through a trusted organization or business where you fully understand how the funds are being collected and used. It is important to never send funds to someone you do not know.

Foreign lottery

Many local governments recently have issued a national warning about the continued defrauding of citizens taking place through a foreign lottery or sweepstakes scam. Be aware that if you receive a notice about winning a lottery, no matter how official it looks, and are required to pay a fee to claim your winnings - this is a scam.

Lottery/sweepstakes

Legitimate lottery or sweepstakes NEVER require people pay money up front. Get a letter, call, or email saying you won something (money or a prize), but before you can collect the prize you need to send money to pay for taxes, customs, or any fees? But you didn't buy a ticket or enter a sweepstakes. This is a SCAM. Don't send transfer

money to the people who are stating you have "WON" something but need to send them funds to collect your winnings.

Victim is told that they have won a lottery, prize or sweepstakes and that money must be sent to cover the taxes or fees on the winnings. The victim may receive a check for part of the winnings and once the check is deposited and money is sent, the check bounces.

Internet Purchase scam

The victim sends money for the purchase of item ordered online (e.g. pets, cars). Items are often advertised on Craigslist, eBay, Alibaba, etc. After the money is sent, the victim never receives the merchandise.

Have you found something online that interests you - a puppy, a car, an apartment for rent or any item for sale? Does the price for the item seem to be too good to be true and are you being asked to pay for the item through a money transfer? Unfortunately, this is a SCAM. Do not send money for the item to the seller. They may even send you a letter or e-mail of authentication telling you that you have purchased the item but need to wire funds first. Do not send the money. It is a SCAM. You will receive no merchandise. Once money is wired and received it cannot be recovered and unfortunately you will be at loss for any money transferred.

Buying a vehicle

Have you found a great vehicle online or in an advertisement with a price too good to be true? Are you being asked to send the down payment through a money transfer? Unfortunately, it's a SCAM. Do not send money for the vehicle to the seller or a payments representative. The vehicle purchase scammer may try to convince you to pay through MoneyGram to avoid sales tax and get a great price. They may even send you a letter or e-mail of authentication telling you that you have purchased the item, but in order to deliver it you need to wire funds first. You will not receive a car or truck. Once money is wired and received, it cannot be recovered and, unfortunately, you will be at loss for any money transferred.

Emergency scam

Victim is led to believe that they are sending funds to assist a friend or loved one in urgent need. Victim sends the money with urgency as the victim's natural concern for a loved one is exploited.

Relative in need

Did you receive a phone call from a grandchild or a family member? Or a "lawyer" or "police officer" suggesting they are with your family member? Are they in despair because they have been detained? Have they been in a car accident? Are they asking for money to pay fines or for car repair? Did a relative call because they need money for a family member in medical need or for medicine? THIS IS A SCAM! Use precaution when sending money in any of these situations. These callers can request that you send money anywhere in the world. If you cannot verify with your family member (calling their number you had before this call, not the "new number" the caller gives you) that they are requesting money and aren't sure about the transaction, do not send the money. You will be at a loss for any money that is sent.

Grandparent scam

This scam is a variation on the Emergency scam. The victim is contacted by an individual pretending to be a grandchild in distress, or a person of authority such as a medical professional, law enforcement officer, or attorney. The fraudster describes an urgent situation or emergency (bail, medical expenses, emergency travel funds) involving the grandchild that requires a money transfer to be sent immediately. No emergency has occurred, and the victim who sent money to help their grandchild has lost their money.

Loans

Did you receive a letter or e-mail about getting a loan? Were you asked to send money for loan fees, taxes, service fees, advance payments, or any other reason? This is a SCAM. Do not send money to a loan company to obtain a loan. If the money is wired and received it cannot be recovered. You will be at a loss for the money you have sent.

Check/money order

Get a check or money order in the mail with instructions to first cash it at your bank and then send some of the funds to someone else through a money transfer? If so, the check/money order is counterfeit and your bank will make you cover the loss. Be aware that counterfeit checks are very hard to identify. You may have been promised a percentage of the check for employment or because of an over payment. This is a SCAM. Do not send the money and do not cash the check.

Romance/Relationship Scam

Did you meet someone through a personal ad, e-mail, chat room or an instant message? Did they ask you to send them money for travel or to help them financially? Do not wire the money - this is a SCAM. Any money received by this person cannot be recovered and you will be at loss for any money sent.

Victim is led to believe that they have a personal relationship with someone they met online often by social media, in an online forum or on a dating website. The victim is often emotionally invested, often referring to the recipient as a fiancée.

Newspaper ads

Have you found something for sale in the classifieds or any type of newspaper ad? Did they ask you to pay for the item through a MoneyGram money transfer? This is a SCAM. Do not use a money transfer to purchase an item from a stranger. It is not safe to use a money transfer service when trying to purchase an item.

Elder abuse scam

A stranger begins a close relationship with you and offers to manage your finances and assets. Or, signatures on documents do not resemble your own signature. Don't get duped into parting with your money through financial abuse scams. Scammers will try to manipulate you into turning over property and/or money, and this can leave your cash, checking account or even life savings completely wiped out in one transaction. Financial abuse scams can take many forms, including telemarketing fraud, identity theft, predatory lending, and home improvement and estate planning scams. Never trust your money with anyone you don't know.

All the other above types of consumer fraud could also be directed towards elderly or senior individuals.

Advanced Fee / Prepayment scam

Victim is asked to pay upfront fees for financial services which are never provided. Victims often send a succession of transactions for payment of various upfront fees. Common methods could include: credit card, grants, loans, inheritance, or investment.

Anti-Virus scam

Victim is contacted by someone claiming they are from a well-known computer or software company and a virus has been detected on the victim's computer. The victim is advised that the virus can be removed and the computer protected for a small fee with a payment by either credit card or a money transfer. In reality, there was no virus on the computer and the victim has just lost the money they sent for the protection.

Employment scam

Victim responds to a job posting and is hired for the fictitious job and sent a fake check for job related expenses. Check amount exceeds the victim's expenses and victim sends remaining funds back using a money transfer. The check bounces and the victim is responsible for the full amount.

Extortion

Threats to life, arrest or other demands by scammers to unlawfully obtain money, property or services from a victim through coercion that they supposedly owe and threatens if they do not cooperate.

Fake Check scam

Victims are often sent a check as a part of a scam and told to deposit the check and use the funds for employment expenses, internet purchases, mystery shopping, etc. The check is fake (counterfeit), and the victim is left responsible for any funds used from the check. Remember, funds from a check deposited into an account should not be used until the check officially clears which can take weeks.

Immigration scam

Victim receives a call from someone claiming to be an immigration official saying there is a problem with the victim's immigration record. Personal information and sensitive details related to the victim's immigration status may be provided to make the story seem more legitimate. Immediate payment is demanded to fix any issues with the victim's record and deportation or imprisonment may be threatened if payment is not made immediately by money transfer.

Money-Flipping scam

Social media is being used to lure new victims into an old get-rich-quick scam where users are advertising ways to turn \$100 into \$1,000 by "flipping money". The pitch suggests investors can take advantage of quirks in the monetary system to leverage additional cash and turn a few hundred dollars into thousands. Once con artists have access to the cash, they often block the victim from contacting them via social media or phone number.

Military

Military service members are an appealing target for scammers for several reasons. They are abusing the wide-spread admiration for the military and posing as service men and women in order to trick people into sending them money.

Mystery Shopping scam

The fraudster contacts the victim through an employment website, or the victim responds to an ad about an employment opportunity to evaluate a money transfer service. The fraudster often sends the victim a check to deposit and instructs the victim to send a money transfer, keeping a portion of the check for their pay. The victim sends the money, the fraudster picks it up, and when the check bounces the victim is left responsible for the full amount.

Overpayment scam

The fraudster sends the victim a check that appears to be valid as payment for a service or product. Typically, the amount of the check exceeds what the victim expects to receive, and the fraudster tells the victim to send the excess back using a money transfer. When the check bounces, the victim is left responsible for the full amount.

Phishing

Communication impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the victim into providing personal information or passwords. A Phish is a fraudulent attempt, usually made through

email (although can also be made via phone or text), to steal your personal information or propagate malicious code or software onto your computer.

Rental Property scam

Victim sends money for deposit on a rental property and never receives access to the rental property or the victim may also be the property owner who is sent a check from the renter and asked to send a portion of the check back using a money transfer and the check bounces.

Social Networking scam

If a cybercriminal gains access to your social media accounts, they also gain access to your close friends and family. Criminals and con artists can take advantage of how much personal information people share online, and then use this information to make skillful and highly targeted pitches to their friends and family, often involving requests for money.

SMS/Smishing

Beware of texts that spark urgency, asking you to click on a link, taking you to a compromised site, or get you to unwittingly divulge some personal information that could be used against you.

Telemarketing

Telemarketing broadly covers almost any commercial transaction that involves the use of a telephone to place or receive calls between a consumer and a telemarketer or seller for the transferring of funds, such as cash-to-cash money transfers or funds loaded onto a prepaid card, as payment for goods or services offered or sold through telemarketing, often relating to a promotion for a "free" or heavily discounted vacation, prize or sweepstakes scams, or the sale of "bargain" magazines.

Fraud Education:

Protect yourself from fraud. Only send money to friends and family. Never send money to someone you do not know personally. Never share your prepaid card information with anyone. In addition, if you do know the person requesting money, always verify that they are who they say they are. If you do not recognize the number they are calling you from, call them back at their known phone number to verify their identity.

Many times, scammers create a sense of urgency to persuade people to transfer money quickly without having time to verify their story. Never send anyone money prior to verifying who they are or confirming the request is legitimate.

- <u>Always confirm any emergency situation</u> with another individual close to the situation or with the individual themselves by calling them back on a known phone number.
- Never send money via money transfer for an online purchase. Legitimate merchants will have methods of payment available on their website.
- Never send money via money transfer for a deposit or payment on a rental property if it is a person or business you do not know or have not established a business relationship with.
- Never send money via money transfer to claim lottery or prize winnings especially if you have never played the lottery and don't remember entering a sweepstakes or lottery. Always be suspect of foreign lottery winner notices.
- Never send money via money transfer to pay taxes. The IRS will never send a taxpayer a request via email or phone call to pay taxes via money transfer.
- Never send money via money transfer for a donation to charity. Legitimate charitable organizations will have different payment options available that do not require the need to send a money transfer.

- Never send money via money transfer for a mystery shopping assignment or a job opportunity. Legitimate employment opportunities will never require you to send money prior to taking an assignment or job.
- Never send money via money transfer for a credit card or loan fee. Established companies will not request a money transfer for payment of fees. They will have other payment options available for its customers.
- Never send money via money transfer to resolve an immigration matter. The government would never call or email someone to request payment via money transfer for an immigration issue.
- Never send money via money transfer to pay for something in response to a telemarketing call. It is illegal for telemarketers to ask for payment via money transfer from anyone in the U.S.

Your money is not the only target of fraud. Your personal data is also a target. Why? It's simple. Fraudsters rarely act under their own names. They mostly use third-party data. In order to do this, they acquire it by stealing the identity of other people.

Another method is to simply steal an ID card. This is why in case of loss or theft of your ID card or passport, you should immediately file a police report. You should also inform your bank. Taking these steps will help you to avoid the unpleasant surprise of finding out that someone took a loan or committed a crime using your data.

Phishing Emails

Passwords and IDs hold high value with cyber criminals. Sending phishing emails to a lot of random email addresses is one easy way scammers steal information from unsuspecting people. It's probably a phishing email if:

- The email is poorly written with misspellings and incorrect grammar or a familiar company name is misspelled.
- Your name isn't in the "To" line. This email has likely been sent to thousands of people.
- The sender's email address is suspicious; it might have a familiar company or government organization that is misspelled.
- The email doesn't use your name. Any financial institution you have an account with knows your name. Email beginning with "Dear valued customer," "To Whom It May Concern," or even "Hello," could be a sign of a scam.
- The URL is a fake. Hover over the "click here" or "take action now" link with your mouse. If you see a strange URL instead of a legitimate company website, don't click on it.
- You're informed that there's a security breach on your account, and if you don't take the action recommended in the email, your account will be suspended.
- The email asks for your personal credit card or online account information or takes you to a website that asks for it. Legitimate companies that handle your financial information will not ask you to do that.

If you receive a suspicious email:

- Don't open it; delete it immediately and completely. Make sure to delete it from your deleted emails folder as well.
- Don't ever click on any of the links in the email even if it's to "unsubscribe" from the sender. In addition, do not open any files attached to the suspicious email.
- Always remember that Broxel will never send you an email asking for your ID, password or personal information. If you're not sure whether an email is from us or not, please contact us to verify the request for information. In the meantime, do not open any links, click on any attachments, or provide any passwords or user IDs until you verify the legitimacy of the request.

Another money extortion technique is the action of the fraudsters trying to install malware on your computer. This enables them to take control of money when you are making an online money transfer. Malware can be unconsciously installed by opening a file attached to an email from an unknown recipient. This kind of software can change the recipient's bank account number when sending a money transfer online. It can be counteracted by checking the transfer details thoroughly during its authorization e.g. via text message.

Protecting yourself against consumer fraud

How do you protect yourself from scammers/fraudsters who want to take your money? You must learn their tricks, use common sense, and follow the tips listed below. It's up to you whether scammers can take your money. Always remember that the scammer can succeed or fail based on whether you participate in the scam. Here are some tips to remember to protect yourself from money transfer fraud:

- <u>Always know who you're dealing with</u>, especially if it's about an unsolicited prize or gift offer. Don't trust messages that come from unknown persons or entities.
- <u>Always research an offer</u> to be sure it's real. If it sounds too good to be true, it probably is.
- <u>Always remember that sending a money transfer is like sending cash</u>. Once you send it and it has been received by the beneficiary, you can't get it back.
- Never send a money transfer to someone you don't know.
- <u>Never send a money transfer to someone who asks you to deposit a check and then send them a portion</u> of the money back without waiting for the check to clear your bank account first.
- <u>Never send a money transfer to a relative in crisis without checking out the story first</u>. Ask questions to verify the person's identity.
- <u>Never send a money transfer to receive money</u> or something of value in return after the money has already been sent.

Fraud FAQs:

The more you know the less likely you are to become a victim of fraud. Here are the most frequently asked fraud-related questions:

1. What do I do if I've been scammed?

Contact your local police immediately.

Report suspected incidents of over-the-phone fraud or Internet fraud by submitting a report online to the National Consumers League's Fraud Center.

File a complaint with the Federal Trade Commission or call toll free 1-877-FTC-HELP

File a complaint with your Attorney General.

If you used Broxel to send money or used your prepaid card account as a result of a scam, contact us at 1 855-279-2720 or via email, or report fraud through our form online.

2. What do I do if I've been scammed online?

If you were a victim of fraud via the Internet, file a report with your local police and the Internet Crime Complaint Center (CCCC), a partnership between the FBI and the National White Collar Crime Center.

If you used Broxel to send money or used your prepaid account as a result of a scam, contact us at 1 855-279-2720 or via email, or report fraud through our form online.

3. What are the most common types of fraud?

Please see section <u>Types of Fraud/Scams</u> to see the different types of fraud/scams.

4. What are warning signs of money transfer fraud?

Someone you don't know asks you to transfer money to them.

Someone asks you to deposit a check and send them back a portion of the money.

Someone pretends to be a friend or relative and calls in a crisis, asking you to wire money right away.

Someone tells you you've won a prize or contest that you don't remember entering, and asks you to wire money to pay fees, taxes or customs.

5. Are there any risks with sending money transfers?

Yes, when you don't know who you are sending the money to. Sending a money transfer is the same as sending cash. Once you send it, you can't get it back as scammers typically pick up the money within minutes.

6. What are the warning signs of prepaid card fraud?

Someone you don't know asks you to give them your prepaid account information

Offers that ask you to pay an advance fee using your prepaid account to collect a prize or sweepstakes

You are asked to provide your prepaid account information for an online purchase.

Report Fraud:

Please contact Broxel if someone tries to scam or defraud you or if you have been a victim of fraud:

Call us at: 1 855-279-2720

Or you can email us at: reportfraud@broxel.com

You may also want to consider reporting fraud to the following authorities:

Contact your local police department and file a police report.

FTC Online Complaint Form

FTC toll free hotline: 877-FTC-HELP (877-382-4357)

National Consumers League's Fraud Center

Internet Crime Complaint Center (CCCC)