Frazer Bank
Electronic Banking Customer Awareness Program

(Customers are directed to the Customer Awareness link on the website, and all information is verified to make sure they are the same)

Frazer Bank's Commitment to Security

Each year more and more Americans have their identity stolen and the staff and management of Frazer Bank want to give you the information you need to help protect yourself against ID theft.

While we cannot guarantee that your ID will never be stolen, we will NEVER request personal information by email or text messaging including account numbers, passwords, personal identification information or any other confidential customer information.

Fraudulent emails may be designed to appear as though they are originated by Frazer Bank. Do not respond to any email communications which request any type of personal or confidential information and do not go to any links listed on that email.

Fraudulent call scams are becoming more and more prevalent. These calls come in many forms but tend to make promises or threats and even may ask you for your electronic banking credentials or pretend to be from the fraud department. Scammers can make any name or number show up on your caller ID. That is called spoofing and they could be calling from anywhere in the world.

These communications are not originated by Frazer Bank! Never give out any information that the Bank already has to a caller, text or email sender. If you contact us, we may confirm your identity but we will never contact you and ask for your debit card number or your full SSN. If we need to contact you, it will always be done in a manner that protects your personal, confidential information and we will clearly identify ourselves. One of Frazer Bank's top priorities is to safeguard YOUR confidential information and we work diligently to do so.

We always work with the local regulatory and law enforcement departments to be certain any type of illegal activity is stopped as soon as possible. We have multi-layer security to protect your confidential information and will continue to be vigilant in protecting it.

Immediately report any suspicious emails or websites to Frazer Bank by forwarding the message to info@frazerbank.com. If you suspect identity theft or have any questions regarding this notice, please contact Frazer Bank at 580-482-7700.

Online Banking Security

Frazer Bank is committed to protecting your personal information. Our Online Banking uses several different methods to protect your information. All information within our Online Banking uses the Secure Socket Layer (SSL) protocol for transferring data. SSL is a cryptosystem that creates a secure environment for the information being transferred between your browser and Frazer Bank. All information transferred through Online Banking has a 128-bit encryption which is the highest level of encryption. In addition to the security features put in place by Frazer Bank here are some tips on keeping your information secure.

- Never give out any personal information, including User Names, Passwords, SSN or Date of Birth.

- Create difficult/unique passwords which include letters, numbers & symbols when possible.
- Don't use personal information for your user names or passwords, like Birth Dates or SSN.
- Avoid using public computers to access your Online Banking.
- Do not use the password auto-save feature on your browser.

Mobile Banking Security Tips

- Don't Follow Links that you might get in a text message because it could be a phishing attack.
- Avoid Banking While on Public Networks due to public connections not being very secure.
- Use the Official Bank App when possible.
- Be careful of what you download.
- Keep track of your Mobile Device.

What is Identity Theft?

Identity theft involves the unlawful acquisition and use of someone's identifying information, such as:

- Name
- Address
- Date of Birth
- Social Security Number
- Driver's License
- Bank or Credit Card Account Number
- Personal Identifiable Number (PIN)

Thieves then use the information to repeatedly commit fraud in an attempt to duplicate your identity which may include opening new accounts, purchasing automobiles, applying for loans, credit cards and social security benefits, renting apartments and establishing services with utility and telephone companies. It can have a negative effect on your credit and create a serious financial hassle for you.

How do I protect myself?

- Report lost or stolen checks or credit cards immediately.
- Never give out any personal information, including birth date, SSN or Passwords.
- Shred all documents containing personal information, like bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings, and invoices.
- Review statements promptly and carefully and periodically check your credit report.

For more information about identity theft and other tips on how to protect yourself and your information please visit the following websites.

Computer Security:
www.onguardonline.gov

Federal Trade Commission for ID Theft:
https://www.identitytheft.gov/

FDIC Consumers Quick Links:
https://www.fdic.gov/consumer-resource-center

United States Department of Justice:
https://www.justice.gov/criminal/criminal-fraud

Federal Trade Commission for Scam Calls
https://consumer.ftc.gov/articles/phone-scams#howtorecognize

Equifax
PO Box 740256
Atlanta GA 30374-0256
www.equifax.com

To order a report: 866-349-5191
To report fraud: 800-525-6285

Experian
PO Box 2002
Allen TX 75013-0949
www.experian.com

To order a report: 877-FACTACT
To report fraud: 888-397-3742

Trans Union
PO Box 1000
Chester PA 19022
www.transunion.com

Customer Support: 800-680-7289

Request Free Annual Credit Report
www.annualcreditreport.com

Spoofed Caller ID Protection

What is Spoofing? Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often use neighbor spoofing so it appears that an incoming call is coming from a local number, or spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity.

How to avoid Spoofing

- Don't answer calls from unknown numbers. If you answer such a call, hang up immediately.
- Do not respond to any questions, especially those that can be answered with "Yes" or "No."
- Use caution if you are being pressured for information immediately.

- Never give out personal information such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious
- If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.

https://www.youtube.com/watch?v=PS3llQfRLD8

Debit Card Protection

Debit card usage has increased dramatically in recent years and fraudulent use of debit cards has also increased.

We at Frazer Bank have some suggestions for you for the care and usage of debit cards.

- NEVER give your debit card information when requested by phone, email or texting. We at neither Frazer Bank nor any other bank we know of will ever request information from you in this manner. Please contact us if you receive any such request.
- It is a good idea to pay by credit card if your card leaves your sight. An example might be when a waiter takes your card from your table in a restaurant.

  https://www.youtube.com/watch?v=d62JROArvHs

Regulation E: Electronic Fund Transfers

Regulation E establishes the basic rights, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services. The primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers.

Regulation E Points:

- Banks follow specific rules for electronic transactions issued by the Federal Reserve Board known as Regulation E. These rules cover all kinds of situations revolving around transfers made electronically. Under the consumer protections provided under Regulation E, you may be able to recover internet banking losses according to how soon you detect and report them.
- Regulation E protects individual consumers engaging in electronic fund transfers (EFT). Non-consumer (or business) accounts are not protected by Regulation E. As a result of Business/Commercial clients not being covered it is critical that they implement sound security practices within their places of business. (See Securing Your Business in the next sections)
- Our Regulation E policy is provided when new electronic services are provided or can be made available upon request.

Securing Your Business-Good Practices

Good practices can keep business/commercial client's information secure. These measures can prevent a business from experiencing losses or ID Theft such as Corporate Account Takeover in which criminals

steal your valid online banking credentials. Businesses also need to be aware of the prevalence of Invoice Fraud, which involves the fraudster sending a fraudulent email with new payment information in an attempt to redirect funds to them instead of the actual vendor. The attacks are usually stealthy and quiet and can lead to account-draining transfers.

Steps to protect your company can be:

- Use layered system security measures: Create layers of firewalls, anti-malware software and encryption. One layer of security might not be enough. Install robust anti-malware programs on every workstation and laptop. Keep the programs updated.
- Manage the security of online banking with a single, dedicated computer used exclusively for online banking and cash management. This computer should not be connected to your business network, should not retrieve and email messages, and should not be used for any online purpose except banking.
- Educate your employees about cybercrimes. Make sure your employees understand that just one infected computer can lead to an account takeover. Make them very conscious of the risk, and teach them to ask the question: "Does this email or phone call make sense?" before they open attachments or provide information.
- Block access to unnecessary or high-risk websites. Prevent access to any website that features adult entertainment, online gaming, social networking and personal email. Such sites could inject malware into your network.
- Establish separate user accounts for every employee accessing financial information, and limit administrative rights. Many malware programs require administrative rights to the workstation and network in order to steal credentials.
- Use approval tools, such as a token, when processing ACH files. Requiring two people to issue a payment file doubles the chances of stopping a criminal from draining your account.
- Review or reconcile accounts online daily. The sooner you find suspicious transactions, the sooner the theft can be investigated.
- If/When you receive an email from a vendor or biller with updated payment information, use a call back verification to ensure that new payment information is legitimate. Do not call the phone number on the invoice or email, use a contract or website to obtain contact information to make sure you aren't talking directly to a protentional fraudster.

Securing your Business-Self Assessment

Online Banking Business/Commercial clients are strongly encouraged to perform an annual Self-Assessment focusing on their online banking practices and network security. A Self-Assessment will evaluate whether the client has implemented sound business practices to address the five key principles outlined below.

Is your company keeping information secure?

Are you taking steps to protect sensitive information? Safeguarding sensitive data in your files and on your computers is just plain good business. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on five key principles:

- **Take Stock**. Know the nature and scope of the sensitive information contained in your files and on your computers.
- **Scale down**. Keep only what you need for your business.
- **Lock it**. Protect the information in your care.

- **Pitch it**. Properly dispose of what you no longer need.
- **Plan ahead**. Create a plan to respond to security incidents.

  The details for the Self-Assessment are provided by the Federal Trade Commission, Bureau of Consumer Protection at:
  http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business

A brochure can also be provided to you by a Frazer Bank employee upon request.

Unsolicited Client Contact

Frazer Bank will NEVER contact its customers on an unsolicited basis to request their security logon credentials such as the combination of the client's username and password. If you receive a request of this type, do not respond to it. Please call us immediately at 580-482-7700 or email us at info@frazerbank.com to report any activity of this nature.

Frazer Bank will only contact its customers regarding online banking activity on an unsolicited basis for the following reasons:

- Suspected fraudulent activity on your account.
- Inactive/dormant account.
- To notify you of a change or disruption in service or
- To confirm changes submitted to your online banking profile.

General Information

Personal Computers

- Always sign out or log off.
- Update software frequently and keep systems current.
- Use a current version of Antivirus software.
- Virus software definitions should be updated daily.
- Install and activate a personal firewall.
- Keep your operating system current.
- Activate the automatic update feature.
- Set you browser's security level to the default setting or higher.

Best Practices

- Keep your personal information private and secure.
- Check your account balance regularly.
- Do not access your account from a public location.
- If you suspect suspicious activity, take swift action.
- Be skeptical of email messages, for example, from someone unlikely to send an email such as the IRS.
- Do not open the suspicious emails and do not click on the links.

Websites

- Check your credit report.
- Pay using credit cards.
- Shred bank account, credit card, medical and other statements with personal information.
- Never click on suspicious links.
- Only give sensitive information to websites using encryption, verified through the web address that starts with https:// (the "s" is for secure).
- Use social media wisely and don't reveal too much.

Mobile Devices

- Use passcodes.
- Avoid storing sensitive information.
- Keep software up-to-date.
- Install remote wipe if the device is lost or stolen so it can be cleared off.

Using ATM's safely

- Protect your ATM card and PIN. If lost report as soon as possible.
- Choose a PIN different from your address, telephone #, and birthdate.
- Be aware of people and your surroundings.
- Put away your card and cash.
- Skimming device-observe the card reader, if it looks suspicious or damaged don't use it.

Additional Training

As new and emerging threats are reported, Frazer Bank may update/modify this document. Frazer Bank may also use statement mailers with information on ways to protect your information.

Frazer Bank Contacts

You are protected in a variety of ways when you use Internet Banking and electronic banking products; however, it is important to contact Frazer Bank in the event you think your personal or company's online access has been compromised. Also report any unauthorized or unexpected transactions immediately.

Your account is protected against fraudulent transactions in a number of ways, so monitor your account balances and transactions frequently. If you want to report suspicious activity in your account(s), or if you have questions about the security of your account(s), you can call us at 580-482-7700 or email us at info@frazerbank.com.

The security of your money and identity is as important to us as it is to you. Let's work together to protect it!!

Updated 9/28/2020-Reviewed 06/2026