# *Online Banking Customer Awareness & Education Program*

First Bank of the Lake is committed to protecting our customers' information. Fraudsters have continued to develop and deploy sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Every day, cybercriminals are working relentlessly to install malicious software like viruses and spyware on your computers in an effort to damage your computer/software, use your email to spread malware, monitor online activities in an attempt to steal sensitive personal information and money or steal your identity. Don't be an easy target for them.

First Bank of the Lake will NEVER request personal information by phone, email or text messaging including account numbers, personal identification information, passwords or any other confidential customer information.

First Bank of the Lake is providing the below information for your use and action to help protect your online account and transaction information.

**Online Banking Security**

Online Banking is accessed through a Secure Socket Layer (or SSL), meaning all data transmitted to or from the bank's computer systems is encrypted and your money and privacy are protected. Several firewalls exist to prevent unauthorized access to the system and ensure your information is accessible only with an Internet Banking Username and Password.

In addition to the security features put in place by First Bank of the Lake, you can help protect yourself by taking the following actions to stay safe and secure your information:

- Be aware of suspicious emails asking for your personal information.
- Never provide any personal information such as Social Security number, Account number, Usernames or Passwords over the phone or the Internet if you did not initiate the contact.
- Do not use personal information as your Username or Passwords.
- Create hard-to-guess passwords that include upper & lower case letters, number and special characters.
- Change your passwords frequently and don't re-use the same passwords.
- Always sign out or log off of your online banking sessions.
- Avoid using public computers and Wi-Fi to access your online banking accounts.
- Ensure your computer has the most recent Anti-Virus software and is being updated daily.
- Ensure your computer or mobile device have the latest software version.

**Commercial Banking Online Security**

In addition to the information provided regarding "Online Banking Security", Commercial & Small Business account holders should institute additional measures in order to further protect their online banking information.

- Perform your own annual internal risk assessment & evaluation on all online accounts.
- Establish internal policies regarding employee internet usage**.**
- Educate your employees on the risks.
- Establish proper user account controls.
- Review all transactions.
- Ensure all company computers are equipped with up-to-date antivirus protection software and virus definitions are being updated daily.

**Identity Theft**

Identity theft occurs when someone uses your personal information such as your Social Security number, Account number or Credit Card number, without your consent, to commit fraud or other crimes. The following are tips to protect you against identity theft:

- Report lost or stolen checks or credit/debit cards immediately.
- Never give out your personal information.
- Review statements promptly and carefully.
- Shred all documents that contain confidential information (i.e. bank and credit card statements, bills and invoices that contain personal information, expired credit cards and pay-stubs.
- Check your credit report periodically.

**Check Your Credit**

Consumers can request one free copy of his or her credit report every year. Reviewing your credit report can help you find out if someone has opened unauthorized financial accounts, or taken out unauthorized loans, in your name.

- Equifax - 1-800-685-1111
- Experian - 1-888-397-3742
- Transunion - 1-877-322-8228

**Electronic Funds Transfer Act (Regulation E)**

Regulation E is a consumer protection law for accounts established primarily for personal, family, or household purposes. Regulation E gives consumers a way to notify their financial institution that an EFT has been made on their account without their permission.

Non-consumer accounts, such as Corporations, Partnerships, Trusts, etc. are excluded from coverage. A non-consumer (business account) customer using internet banking and/or bill pay is not protected under Regulation E. As such, special consideration should be made by the business customer to ensure adequate internal security controls are in place that commensurate with the risk level that the customer is willing to accept.

As a non-consumer customer you should perform periodic assessments to evaluate the security and risk controls you have in place. The risk assessment should be used to determine the risk level associated with any internet activities you perform and any controls you have in place to mitigate these risks.

**Definition of EFT**

An EFT is the electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions initiated through electronic-based systems. The term includes, but is not limited to:

- Point-of-sale transfers
- Automated Teller Machine transfers (ATM)
- Direct deposits or withdrawal of funds
- Transfers initiated by telephone
- Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal
- Transfer initiated through internet banking/bill pay

**Protections provided under Regulation E for consumers who use internet banking/bill pay**

If you believe an unauthorized EFT has been made on your account, contact us immediately. If you notify us within 2 business days after you learn of the loss or theft of your ATM/debit card or Personal Identification Number (PIN), the most you can lose is $50. Failure to notify the bank within 2 business days may result in additional losses.

**Unlimited Liability**

Unlimited loss to a consumer account can occur if:

- The periodic statement reflects an unauthorized transfer of money from your account, and you fail to report the unauthorized transfer to us within 60 days after we mailed your first statement on which the problem or error appeared.

**Exclusions from Protection**

The term EFT does not include:

- *Checks* - Any transfer of funds originated by check, draft or similar paper instrument or any payment made by check, draft or similar paper instrument at an electronic terminal
- *Check Guarantee or Authorization* - Any transfer of funds that guarantees payment or authorizes acceptance of a check, draft or similar paper instrument but does not directly result in a debit or credit to a consumer's account
- *Wire or other similar transfers* - Any transfer of funds through a wire transfer system that is used primarily for transfers between financial institutions or between businesses
- *Securities and Commodities Transfers* - Any transfer of funds for the primary purpose of the purchase or sale of a security or commodity, if the security or commodity is:
    - Regulated by the Securities and Exchange Commission or the Commodity Futures Trading
    - Purchased or sold through a broker-dealer regulated by the Securities and Exchange Commission or through a futures commission merchant regulated by the Commodity Futures Trading Commission
    - Held in Book-entry form by a Federal Reserve Bank or federal agency
- *Automatic transfers by account-holding institution* - Any transfer of funds under an agreement between a consumer and a financial institution which provides that the institution will initiate individual transfers without a specific request from the consumer:
    - Between a consumer's accounts within the financial institution
    - From a consumer's account to an account of a member of the consumer's family held in the same financial institution
    - Between a consumer's account and an account of the financial institution, except that these transfers remain subject to § 205.10(e) regarding compulsory use and sections 915 and 916 of the act regarding civil and criminal liability. (Refer to "Coverage in Detail" section below.)
- *Telephone-initiated transfers* - Any transfer of funds that:
    - Is initiated by a telephone communication between a consumer and financial institution making the transfer; and
    - Does not take place under a telephone bill payment or other written plan in which periodic or recurring transfers are contemplated.

**Regulation E - Coverage in Detail**

For a complete detailed explanation of protections provided under Regulation E, please visit the Consumer Financial Protection Bureau's (CFPB's) website:

- CFPB - Electronic Funds Transfers Act (Regulations E)

**Mobile Banking Safety Tips**

Managing your finances using a smartphone or tablet can be very convenient. However, you should consider these safety tips to protect your account information:

- Be proactive in protecting your smartphone and/or tablet by installing anti-malware software on the device.
- Research any application (app) before you download it. Fraudulent apps are often designed with names that look like real apps. It's best if you access an app using a link from the provider's website.
- Create a strong password or PIN for your mobile app and your device.

    - Use at least eight characters
    - Do not use your username, real name or company name
    - Do not use a complete word
    - Make it significantly different from previous passwords
    - Use a character from each of the following categories (some apps may limit symbols)
        - Uppercase letters
        - Lowercase letters
        - Numbers

- Use an auto-lock or time-out feature so your device will lock when it is left unused for a certain period of time.
- Upgrade your device to the latest operating system version.
- Do not jailbreak or root your mobile device. Doing so exposes the security controls and makes your device vulnerable to cyber-attacks.
- Check your account history periodically to make sure there are no fraudulent transactions.
- Take precautions in case your device is lost or stolen, before your device is lost or stolen. Avoid leaving your device unattended in public places.
- Consult your wireless provider to see if they provide a service to remotely erase your device or turn off access to your device and/or account in the event your device is lost or stolen.
- Always conduct your transactions in a safe environment. Use your cellular service or your own internet provider rather than unsecured/public Wi-Fi networks like those offered at coffee shops.
- Don't send account numbers or PIN in emails or text messages, because those methods are not necessarily secure

**Contacting the Bank**

Please contact First Bank of the Lake at our toll free number 1-888-828-0167 or directly by email at firstbk@firstbanklake.com with any questions or concerns you may have. If you believe your online banking account has been compromised or you receive suspicious or fraudulent mail, email or websites related to First Bank of the Lake, please contact us immediately.

**Other References to Assist You:**

**FDIC Consumer Protection**

**http://www.fdic.gov/consumers/**

**Consumer Action: Complaints**

**https://www.usa.gov/consumer-complaints#item-212527**

**US Department of Homeland Security**

**http://www.us-cert.gov/home-and-business/**

**Protecting Your Business: Start With Security**

**https://www.ftc.gov/news-events/audio-video/business**

**NACHA Fraud Resources**

**https://www.nacha.org/Fraud-Phishing-Resources**

**Federal Communication Commission - Business Cyber-planner:**
**http://www.fcc.gov/cyberplanner**

**Consumer Information: Identity Theft**

**https://www.consumer.ftc.gov/features/feature-0014-identity-theft**

**Federal Trade Commission: Identity Theft by Mobile Phone**

https://www.consumer.ftc.gov/blog/identity-theft-mobile-phone

**Federal Trade Commission: Tips for Using Public WiFi Networks**

https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks