Online Banking Customer Awareness Program

Union State Bank is committed to protecting your personal information. Fraud through identity theft is growing day by day and our management and staff wants to do all it can to help you protect yourself in the current online banking environment. Below are areas that you need to be aware of:

Electronic Funds Transfer Act (Regulation E)

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.

For a complete detail explanation of protections provided and not provided under regulation E, please visit the following link / links:

- FDIC – Electronic Funds Transfers (Regulation E)
  - http://www.fdic.gov/regulations/laws/rules/6500-3100.html
- Federal Reserve
  - http://www.federalreserve.gov/boarddocs/supmanual/cch/efta.pdf

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.
- In general, these protections are extended to consumers and consumer accounts.
- If you report the losses within two days of receiving your statement, you can be liable for the first $50. After two days, the amount increases to $500. After 60 days, you could be legally liable for the full amount. These protections can be modified by state law or by policies at your bank, so be sure to ask your banker how these protections apply to your particular situation.
- Regulation E protects individual consumers engaging in electronic fund transfers (EFT). Non-consumer (or business) accounts are not protected by Regulation E.
- Regulation E is a consumer protection law for accounts established primarily for personal, family, or household purposes. Non-consumer accounts, such as Corporations, Partnerships, Trusts, etc., are excluded from coverage. Regulation E gives consumers a way to notify their Bank that an EFT has been made on their account(s) without their permission.

Phishing and Other Fraudulent Communication

Union State Bank will NEVER request personal information by phone, email, or text message including account numbers, personal identification information, passwords, or any other confidential customer information. Below are some points to remember:

- Do not give your login credentials to anyone. If you are contacted by someone who states they are calling from the Bank or you receive an email, you should not give them any information. You should contact the Bank in the event you notice suspicious account activity or experience customer information security-related events.
- Never provide Personal Financial Information including your Social Security number, account number or passwords, over the phone or the Internet if you did not initiate the contact.
- Never click in the link provided in an email you believe is fraudulent. It may contain some type of malicious software that can contaminate your computer.
- Do not be intimidated by an email or caller who suggests dire consequences if you do not immediately provide or verify financial information.
- If you believe the contact is legitimate, go to the company's website by typing in the site address directly or using a page you have previously bookmarked, instead of a link provided in the email.
- If you fall victim to an attack, act immediately to protect yourself. Alert your financial institution as soon as possible. Place fraud alerts on your credit files. Monitor your credit files and monthly statements very closely.
- Report suspicious emails or calls to the Federal Trade Commission through the Internet at http://www.consumer.gov/idtheft, or by calling 1-877-ID-THEFT.

Protecting Your Business

It is suggested that commercial online banking customers perform risk assessments and controls evaluations periodically to help identify potential threats and to determine the strength of their controls. This can be done as follows:

- Identify possible risks in the online banking environment.
  Reference: http://www.ic3.gov/media/2010/corporateaccounttakeover.pdf
- Educate your employees on the risks.
- Create and maintain proper user account controls.
- Review all transactions.
- Install and maintain proper antivirus/security software on all systems/networks that access online banking.

Alternative Risk Control Mechanisms

Customers may also implement additional control mechanisms to help alleviate their risk. Some examples are as follows:

Passwords:

- Avoid using personal information.
- Create a unique password for online banking that you don't use elsewhere.
- Do not use the password auto-save feature on your browser.
- Do not share your passwords or write them down.
- Change your password periodically.

- The Bank will NEVER ask for your password.

Personal Computers

- Always sign out or log off.
- Update software frequently and keep systems current.
- Virus software, “definitions” should be updated daily.
- Install and activate a personal firewall.
- Install and run most recent version of Antivirus software.
- Keep your operating system (OS) current.
- Activate the automatic update feature.
- Set your browser’s security level to the default setting or higher.

General 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. Should this happen, stop work and have a diagnostics performed immediately.

ID Theft Tips

- Shred receipts, statements, expired cards, and similar documents.
- Review statements promptly and carefully.
- Be positive of the identity of the requestor before divulging personal information. Only give personal information if you initiate the contact.
- Periodically check your credit report.

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 though the web address “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 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 – observe the card reader; if it appears damaged don't use it.

Customer Contact Information in the Event of Suspicious Activity

Union State Bank
205-884-1520
2019 Cogswell Ave
Pell City, AL 35125

Equifax
1-800-525-6285
P O Box 740250
Atlanta, GA. 30374

TransUnion
1-800-680-7289
P O Box 6790
Fullerton, CA

Experian
1-888-397-3742
P O 1017
Allen, Texas 75013

Other researched security links/references that customers can use:

Annual Credit Report
- http://www.annualcreditreport.com

Better Business Bureau – Data Security Made Simple
- http://www.bbb.org/data-security

Bureau of Consumer Protection
- http://business.ftc.gov/privacy-and-security/data-security

Department of Homeland Security Cyber Report
- http://www.cyber.st.dhs.gov/

Fraud Advisory for Businesses: Corporate Account Take Over
- http://www.fsisac.com/files/public/db/p265.pdf

FDIC Safe Internet Banking

- http://www.fdic.gov/bank/individual/online/safe.html

FTC- Privacy & Security
- http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm

ID Theft
- http://www.ftc.gov/bcp/edu/microsites/idtheft/

Internet Crime Complaint Center
- http://www.ic3.gov

NACHA
- https://www.nacha.org/Corporate_Account_Takeover_Resource_Center
- https://www.nacha.org/Fraud-Phishing-Resources

National Cyber Security Alliance
- http://www.staysafeonline.org/

OnGuardOnline
- http://www.onguardonline.gov/

Protecting Personal Information: A Guide for Business
- http://business.ftc.gov/multimedia/videos/protecting-personal-information

Small Business Information Security
- http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Sound Business Practices for Companies to Mitigate Corporate Account Takeover
- https://www.nacha.org/userfiles/File/Sound%20Business%20PracticesBusinessesFinal042811.pdf

United States Secret Service
- http://www.secretservice.gov/ectf.shtml

US-Cert-Cyber Security Tips
- http://www.us-cert.gov/cas/tips/