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 e-mail 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 anyone before you divulge personal information, only if you initiate the contract.
- Periodically check your credit report.

Websites:

- Check your credit report.
- Pay using credit cards.
- Shred bank account, credit card, physician 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

EvaBank
256-255-2000
1710 Cherokee Ave SW
Cullman, AL 35055

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

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

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

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/

FDIC Safe Internet Banking

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

FTC- ID Theft, Privacy, & Security

- www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm

Internet Crime Complaint Center

- www.ic3.gov

NACHA

- https://www.nacha.org/Fraud-Phishing-Resources
- https://www.nacha.org/content/current-fraud-threats-resource-center

National Cyber Security Alliance

- http://www.staysafeonline.org/

OnGuardOnline

- http://www.onguardonline.gov/

Small Business Information Security

- http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

US-Cert-Cyber Security Tips

- http://www.us-cert.gov/cas/tips/

The Cyberwire –cyber security news

- https://thecyberwire.com/