Customer Safety and Awareness Policy

It is Relyance Bank's policy that the Bank will take all appropriate steps required to prevent identity theft and provide materials that instruct on guarding against identity theft. While the Bank cannot guarantee that a customer's identification will never be stolen, the Bank will not request personal information by e-mail or text message. Information that will not be requested via these channels includes account numbers, passwords, personal identification information (SSN, ID numbers, etc.) or any other non-public confidential information.

Fraudulent E-mails

Fraudulent e-mails may be designed to appear as if they are being originated by a creditable source such as the Bank. E-mail requesting any type of confidential information should not be responded to as the Bank will not request this information via e-mail or text messaging. Additionally, do not go to any link that may be imbedded in the e-mail as they are often times used to steal information from the user.

These types of communications are not originated by the Bank. Never give out personal information which the Bank already knows or has stored in their files and systems to any caller, or text or e-mail originator. If you have received any communication, it is best to call the Bank at (855)365-RELY to inquire about the request for information. When you call the Bank, your identity will be confirmed, but you will never be contacted and asked for your complete Social Security number or debit card number. Any contact initiated by the Bank will be conducted in a manner designed to protect your confidential personal information. When contacting you, employees of the Bank will clearly identify themselves to further ensure your confidential personal information is safeguarded.

Protection

The Bank works with local authorities and regulators to assure our customers that any time there is illegal activity taking place, it can be stopped as soon as possible. The Bank utilizes multi-layer protection in our security efforts to protect all customer confidential personal information. The Bank will continually employ Customer Due Diligence processes to diligently protect against the loss of confidential personal information.

Immediately report suspicious activity such as phone calls, text messages, or e-mails to Relyance Bank at CustomerSafety@relybank.com. If you suspect identity theft or would like to inquire about certain activity, contact the Bank at (855)365-RELY.

Online Banking Security

Relyance Bank is committed to protecting your confidential personal information. The Bank's online banking service utilizes several different methods to protect your information. All information that is stored within our online banking uses the Secure Socket Layer (SSL) protocol to protect your information from theft during data transmission. SSL is a cryptosystem designed to create a secure environment for your information as it is being transmitted between browsers and the Bank. Any information that is transmitted through online banking has a 128-bit encryption which is the highest level of encryption available. In addition to the security features of the Bank, it is important that you also consider these added suggestions for keeping your confidential personal information safe and secure.

Added Suggestions

- Never give out any personal information, including your user names, passwords, or date of birth.
- Create difficult/unique passwords which include letters, numbers, and symbols, when possible.
- Do not use personal information for your user names or passwords, like birth dates or social security number (SSN).
- Avoid using public computers to access your online banking.
- Do not use the password auto-save feature.

What is Identity Theft?

Identity theft is the practice of unlawfully acquiring and using someone is 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)

Identity thieves use the information to commit fraud on a repetitive basis. This is done in an attempt to duplicate your identity which could include opening accounts, applying for credit, obtaining credit cards, purchasing an automobile, renting an apartment, acquiring services through utility companies and phone companies, as well as applying for Social Security benefits. It can often times have a negative effect on your credit and cause a significant financial hassle for you.

How Can You Protect Yourself?

It is important to remember that protecting yourself is a vital part of preventing identity theft. You can do so by:

- Reporting lost or stolen checks or credit cards immediately.
- Never giving out any personal information, including birth date, SSN, or passwords.
- Shredding all documents containing personal information like bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings, and invoices.
- Reviewing statements promptly and carefully, and periodically checking your credit report.
- Not giving any of your personal information to any web sites that do not use encryption or other secure methods to protect your information.

You can obtain additional information about identity theft and how to protect yourself and your confidential personal identifying information by visiting the following websites:

*NOTE: By clicking the links below, you will be directed away from Relyance Bank's website.

Federal Trade Commission – computer security
www.onguardonline.gov

United States Department of Justice
www.usdoj.gov/criminal/fraud

Experian
www.experian.com
(888)397-3742

TransUnion
www.transunion.com
(888)909-8872

Equifax
www.equifax.com
(800)685-1111

Debit Card Protection

In the current environment, debit card usage has increased drastically over the past few years, and the fraudulent use of cards has increased as well. The Bank offers some suggestions to further safeguard you and your debit cards.

- NEVER give your debit card information when requested by phone, e-mail, or text.

Relyance Bank will not ever request information from you in this manner. Please contact the Bank if you receive any such request.

- It is a good idea to pay by credit card, if your card will leave your sight during the transaction.

An example might be when a waiter takes your card from your table in a restaurant. Debit cards are easier to process illegally than credit cards.

Regulation E: Electronic Funds Transfers

Regulation E is designed to protect consumers making electronic fund transfers. The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through electronic terminals, telephones, computers, or magnetic tape that instructs the Bank to either credit or debit a consumer's account.

The Electronic Funds Transfer Act (Regulation E) was issued by the Board of Governors of the Federal Reserve System and adopted in 1978 as an add-on to the Consumer Credit Protection Act. The regulation and law institute the basic rights, liabilities, and responsibilities of a consumer who utilizes the EFT system or services offered by the Bank.

Commercial and business account are not covered by the protection of the law or regulation. It is important for these customers to implement safe and sound security practices that are suggested in this program. This will reduce the risk to the companies in regard to theft and fraud.

Corporate Account Takeover

Corporate account takeover is also a form of identity theft that criminals utilize. It involves the theft of a business's online banking credentials. This attack is usually quite stealthy, and a business might not even realize it has taken place. Malware may be on a system and go unnoticed for weeks or months. The theft of monies from the stolen credentials may take days or even months to occur or be noticed. It is important to review accounts regularly to ensure suspicious activity is identified and reported.

Steps to Protect Your Company

- 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, and 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 any e-mail messages, and should not be used for any online purpose except banking, if possible.
- 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 e-mail or phone call make sense?" before they open attachments or provide information.
- Block access to unnecessary or high-risk websites. Prevent access to any websites that feature adult entertainment, online gaming, social networking, and personal e-mail. Such sites could inject malware into your network.
- Establish a separate user account 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. If your user permissions for online banking include administrative rights, do not use those credentials for day-to-day processing.
- Review or reconcile accounts online daily. The sooner you find suspicious transactions, the sooner the theft can be investigated.

Business Self-Assessment

Commercial or business clients that utilize online banking are strongly encouraged to complete an annual self-assessment that focuses on their online banking practices and internal network security. A self-assessment should be utilized to evaluate if the business has implemented sound business practices to address five key principles. Those principles are:

- 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.

Details on performing a 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.

Unsolicited Client Contact

The Bank will not contact its customers at any time for unsolicited reasons to request their security login credentials. The credentials include user names and passwords. If you receive a request for this information, do not respond. Please call the Bank immediately at (855)365-RELY or e-mail us at internetbanking@relybank.com to report any such activity.

The Bank will only contact its customers in regard to online banking activities on an unsolicited basis for the following reasons:

- Suspected fraudulent activity has occurred on your account
- Inactive/dormant account
- To notify you of a change or disruption in service
- 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 anti-virus 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 your 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 e-mail messages, for example, from someone unlikely to send an e-mail such as the IRS.
- Do not open suspicious e-mails and do not click on links.

Websites

- Check your credit report.
- Pay using credit cards.
- Shred bank account, credit card, medical and other statements containing 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 do not reveal too much.

Mobile Devices

- Use passcodes.
- Avoid storing sensitive information.
- Keep software up to date.
- Install remote wipe as a precaution against loss or theft.

ATM Safety

- Protect your card and PIN.
- If a card is lost, report it as soon as possible.
- Choose a PIN different from your address, telephone number or birth date.
- Be aware of people and your surroundings.
- Put away your card and cash.

- Observe the card reader. If it looks damaged or suspicious, do not use it. A skimming device that can read the magnetic strip and obtain all information stored on it may be attached.

As there are new and emerging threats reported, the Bank may update and/or modify this document. The Bank may also use account statements as a way to inform customers of how they can protect their confidential personal information.

Bank Contacts

Our customers are protected in a variety of ways when using our internet banking services. However, it is imperative that you contact the Bank in the event you think your personal or company's online access has been compromised. If you would like to report suspicious activity on your accounts, or if you have questions about the security of your account, you can contact the Bank at (855)365-RELY.

The security of your confidential personal information and your money are of the utmost importance to the Bank. Let us help protect it!