Customer Security Awareness Program

Our Commitment to Security

As the number of consumers who fall victim to I. D. theft and electronic fraud increases, the staff and management of Logan Bank & Trust have pledged to take all necessary precautions to safeguard your confidential information, and to give you guidance on how you can protect yourself against ID theft, electronic fraud, and other common threats encountered by today's banking customers.

While we cannot guarantee that your I.D. will never be stolen, we will follow security guidelines to minimize this threat to you, beginning by NEVER requesting 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 Logan Bank & Trust. Do not respond to any email communications which request any type of personal or confidential information, and do not click on any links listed on the email.

Never give out any information that the Bank already has to a caller, text messenger, or email sender. 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 Logan bank & Trust's top priorities is to safeguard your confidential information and we work diligently to do so.

We 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.

Please report any suspicious calls, e-mails, or messages to Logan Bank & Trust by calling (304)752-1166, or by e-mailing support@lbandt.com.

The Internet & You

When shopping online, you should:

• Learn as much as possible about the product and seller.

• Understand the retailers' refund policies.

• Choose a secure password to protect account information.

- Use a secure checkout and payment process.

- If an offer sounds highly suspicious or too good to be true, it probably is.

Best Practices for Online Protection

- Maintain active & up-to-date anti-virus software

- Maintain spy-ware protection

- Set up automatic Windows (or other Operating System) updates

- Maintain firewall installed on the network

- Wireless networks are discouraged

- If you use a wireless network, it is suggested that you use password protection

Internet Banking Security

In recent years, the banking industry has seen significant changes in the internet banking threat landscape:

- Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise security and gain unauthorized access to customers' online accounts.

- Rapidly growing organized criminal groups have become more specialized in financial fraud, and have been successful in compromising an increasing array of controls.

- Fraudsters are responsible for losses of hundreds of millions of dollars resulting from online account takeovers and unauthorized funds transfers.

Logan bank & Trust's goal in providing this awareness program to our customers is to help protect your online account and transaction information from these types of incidents.

Logan Bank & Trust is committed to protecting your personal information. Our Internet Banking platform uses several different methods to protect your information. In addition to the security features put in place by Logan Bank & Trust, here are some steps you can take to keep your personal information secure:

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

- Create difficult passwords which include letters, numbers, and symbols whenever possible.

• Do not use personal information for your user names or passwords, like your Social Security Number, or Date of Birth.

• Avoid using public computers to access your Internet Banking accounts.

• Block cookies on your Web browser. When you surf, hundreds of data points are being collected by the sites you visit. These data get mashed together to form an integral part of your "digital profile," which is then sold without your consent to companies around the world. By blocking cookies, you'll prevent some of the data collection about you.

• Don't put your full birth date on your social-networking profiles. Identity thieves use birth dates as cornerstones of their craft. Try posting only the month and day, and leave off the year.

• Don't download Facebook apps from outside the United States. Apps on social networks can access huge amounts of personal information, which may not be kept securely.

• Use multiple usernames and passwords. Keep your usernames and passwords for social networks, online banking, e-mail, and online shopping all separate.

Below are the protections and liabilities for consumer transactions using Logan Bank & Trust’s internet banking:

• To access our Internet Banking service, you must use the User Name and Password you established when you activated your Internet Banking Customer Account.

• It is your responsibility to safeguard these credentials. Anyone to whom you give your Internet Banking ID and Password or other means of access will have full access to your accounts even if you attempt to limit that person's authority.

• You or someone you have authorized, by giving them your Internet Banking User Name and Password or other means of access, can instruct us to perform the following transactions:

• Make transfers between your qualifying accounts to the extent authorized.

• Obtain information that we make available about your qualifying accounts.

• Obtain other services or perform other transactions that we authorize.

• You must have enough money in any account from which you instruct us to make a payment or transfer. You also agree to the Terms & Conditions of your deposit account that you received when you opened your deposit account.

If you believe your Internet Banking **User Name** or **Password** or other means of access have been lost or stolen, or that someone has used them without your authorization, call us immediately at (304)752-1166 during normal business hours. After hours you may e-mail us at support@lbandt.com.

- Immediately contacting us by phone is the best way of reducing your possible losses, since not all email may arrive at their destinations. We will send an e-mail back to you as confirmation that we did receive it. Because e-mail is not secure, do not include any of your account or social security numbers with your e-mail. Your name, address, and a brief message as to what the problem might be is all we will need.

- If you have given someone your Internet Banking User Name and Password or other means of access, and want to terminate that person's authority, you must change your identification number and password or other means of access or take additional steps to prevent further access by such person.

- You are responsible for all transfers you authorize using the Internet Banking services under its Agreement. If you permit other persons to use your login credentials, you are responsible for any transactions they authorize or conduct on any of your accounts. However, tell us at once if you believe anyone has used your Access Code and accessed your accounts without your authority.

Telephoning is the best way of keeping your possible losses down.

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, Mother's Maiden Name, Driver's License, Bank or Credit Card Account Numbers. 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 to protect yourself from Identity Theft:

- Report lost or stolen checks or credit cards immediately.

- Never give out any personal information to anyone whose identity you can't verify, if at all.

- Shred any documents you don't need any more that contain personal information, like bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings, and invoices.

- Don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it.

Phishing

"Phishing" is a tool or method used for identity theft. It's when thieves act as if they are representing an organization and try to hook the consumer into providing personal or financial information. Once the consumer is hooked, the thieves can do lasting damage to a consumer's financial accounts. They can trick customers into providing their Social Security Numbers, Internet Banking Credentials, financial account numbers, and other personal information.

Thieves often pose as:

- Financial institutions

- Credit card companies

- Utility or other biller

- Internet service provider

- Government agency

- Prospective employer

How it Works

Consumers receive an email from an organization with which they do business. The email typically includes bogus appeals such as problems with an account or billing errors, and asks the consumer to confirm his/her personal information. Most emails ask recipients to follow an embedded link that takes them to an exact replica of the victim company's Web site. Graphics on the counterfeit site are so convincing that even experts often can have a hard time distinguishing the fake site from the real one. Despite the convincing appeals, consumers should not respond to unsolicited emails that direct them to divulge personal identifying information. Reputable organizations that consumers legitimately do business with generally do not request account numbers or passwords unless the consumer initiated the transaction.

Clues to identifying a "Phishing" e-mail

- Awkward greeting- A phish may address the customer with a nonsensical greeting or may not refer to the customer by name.

- Typos & Incorrect Grammar- This is a technique used by phishers to avoid email filters. The errors are intentional.

- Source code points to a different website than the alleged sender- The link looks official, but when your mouse curser rolls over it the link's source code points to a completely different web site. Remember that you can always type a URL into your web browser instead of clicking on a link.

- Urgent call to act- Different approaches include things such as "We're updating our records," "We've identified fraudulent activity on your account," or "Valuable account and personal information was lost due to a computer glitch." To encourage people to act immediately, the email usually threatens that the account could be closed or canceled.

Vishing - "Voice-Phishing"

An offshoot of traditional phishing techniques, "vishing" refers to phish attempts using phone calls or voice-mails. In this case, consumers receive a pre-recorded call identifying a specific local financial institution. The message informs the consumer that his or her personal bank accounts have been frozen. The message advises the consumer to immediately input their ATM or debit card number, expiration date, and PIN to reactivate the affected accounts. The CV2 (3 digit security code) from the back of the card may also be requested. The information obtained by the automated call will be used for unauthorized ATM withdrawals.

Smishing - 11SMS-Phishing"

You don't have to use a computer to be vulnerable to online scammers. Increasingly, cell phone and other mobile device users are being targeted with mobile spam that attempts to trick them into revealing personal information.

Known as "smishing," these text messages might ask a recipient to register for an online service- then try to sneak a virus onto the users' device. In addition to virus-like "worms," which can spread through and disrupt a network, other scams are surfacing.

Some messages warn that the consumer will be charged unless he cancels his supposed order by going to a website that then extracts such credit card numbers and other private data.

"Smishing" is derived from the familiar "phishing." The "sm" comes from SMS, the protocol used to transmit text messages via cellular devices.

Debit & Credit Card Fraud

Debit cards and credit cards have become the most convenient form for purchasing our everyday needs. They have replaced the actual need to carry cash and should be treated like cash. With the ever increasing volume of debit cards and credit cards so has fraud. Follow these steps to protect your cards:

- You should never loan your cards to anyone.

- Carry only the cards you use frequently.

- Never leave your wallet or purse in your vehicle.

- Safeguard your ATM access cards and PIN as you would checks and cash. Memorize your PIN- Don't write it on your card or In your checkbook.

- Be aware of your surroundings when using an ATM, especially at night. Consider having someone accompany you to the ATM when you make transactions after dark.

- Consider using another machine or coming back later if you notice anything suspicious or feel uneasy.

- When using an ATM, stand squarely in front of the machine to keep your transaction as private as possible. Shield your PIN entry with your hand for greater privacy. When waiting to use an ATM, please respect the privacy of those using the machine.

- Consider canceling your transactions, pocketing your card and leaving if you notice anything suspicious while using an ATM.

- Protect the sensitive magnetic stripe on the back of your card. Keep it from direct sunlight. Avoid leaving your card on or near electrical appliances, such as a TV or stereo. Do not carry your card next to another card's stripe as they may demagnetize each other.

- Report all crimes related to ATM activity to the owner/operator of the machine and to local law enforcement officials immediately.

- Always take your receipt with you at the conclusion of every transaction to assure your financial privacy. Keep your receipts and use them to check your monthly statement.

Non-electronic Security Tips

Tips for safeguarding your information (from the American Bankers Association) in the real world:

- Don't give your Social Security Number or other personal credit information about yourself to anyone who calls you.

- Tear up receipts, bank statements, and unused credit card offers before throwing them away.

- Keep an eye out for any missing mail.

- Don't mail bills from your own mailbox.

- Review your monthly accounts regularly for any unauthorized charges.

- Order copies of your credit report once a year to ensure accuracy.

- Before revealing any personally identifying information (for example, on an application), find out how it will be used and secured, and whether it will be shared with others. Ask if you have a choice about the use of your information. Can you choose to have it kept confidential?

- Do business only with companies that you know and trust, especially online.

- Don't open e-mails from unknown sources, and use virus detection software.

- Protect your PINs (don't carry them in your wallet!) and passwords; use a combination of letters and numbers for your passwords and change them periodically.

- Report any suspected fraud to your bank and the fraud units of the three credit reporting agencies immediately.

- To verify whether a call is legitimate, call Logan Bank & Trust or visit our website, using phone numbers or internet addresses from your bank statement or account documentation. Do not call back a number provided over the phone nor click on a link in an email.

- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know whom you're dealing with.

- Don't carry your Social Security card with you; leave it in a secure place. Carry only the identification and credit and debit cards that you need.

- Don't put your address, phone number, or driver's license number on credit card sales receipts.

- Social Security numbers should not be put on your checks.

- Shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.

- Secure personal information in your home, particularly if you have roommates or hire outside help.

- Secure your credit card, bank, and phone accounts with passwords. Avoid using easily available information like birth date, the last four digits of your SSN, or your phone number. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Use a password instead.

- Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold.

- Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that records are kept in a secure location. Ask about the disposal procedures for those records as well.

Corporate Account Takeover

There has been a shift in the online criminal world from primarily targeting of individuals to increased targeting of corporations. Financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses. Eastern European organized crimes groups are believed to be predominantly responsible for the activities that are also employing witting and unwitting accomplices in the United States (money mules) to receive, cash and forward payments from thousands to millions of dollars to overseas locations via popular money and wire transfer services.

How it Works

Typically compromise of the customer is carried out via a phishing e-mail which directly names the recipient correctly and contains either an infected file or a link to an infectious Web site. The e-mail recipient is generally a person within a company who can initiate funds transfers or payments on behalf of the business. Once the user opens the attachment, or clicks the link to open the Web site, malware is installed on the user's computer which usually consists of a Trojan keystroke logger, which harvests the user's corporate online banking credentials. Variations of this method have been used by criminal groups including messages impersonating the Better Business Bureau, US Court System, Microsoft Update, and UPS to name a few.

The customer's online credentials are either uploaded to a website from where the fraudster can later download them, or, if the bank and customer are using two factor authentication systems, the Trojan keystroke logger may detect this and immediately send an instant message to the fraudster alerting them of the secure web activity. The fraudster then accesses the financial institution through use of the captured username and password or through hijacking the secure web session.

The fraud is carried out when the fraudster creates another user account from the stolen credentials or directly initiates a funds transfer masquerading as the legitimate user. These transfers have occurred through wire or ACH that are directed to the bank accounts of willing or unwitting individuals. Often within a couple days, or even hours of recruiting money mules and opening accounts, money is deposited and the mule is directed to immediately forward a portion of the money to subjects in Eastern Europe by various means.

How to Prevent It

It is recommended that businesses utilizing Internet Banking for high risk transactions conduct a risk assessment of their individual risks and controls. This threat strongly relies on authorized Internet Banking users' being tricked into releasing their User Name and Password to a fraudster, visiting an infected website, or opening an e-mail containing a virus. Therefore, a comprehensive security training program for employees with wire transfers or ACH authorities is paramount to reduce your business' risk of being a victim of these types of attacks.

If Your Identity Is Stolen ...

If you become a victim of identity theft, contact:

- The fraud departments of the three major credit bureaus

- The creditors of any accounts that have been misused

- The local police to file a report

- Your local Logan Bank & Trust branch to cancel existing accounts held in your name and reopen new accounts

- Check Your Credit Report

Order a copy of your credit report from each of the three major credit-reporting agencies every year. Make sure it is accurate and includes only those activities you have authorized. By checking your report on a regular basis you can catch mistakes and fraud before they wreak havoc on your personal finances. Don't underestimate the importance of this step. You can request a free credit report from each of the three major credit bureaus through www.annualcreditreport.com.

Credit Bureaus

- Equifax- www.eguifax.com

Report Fraud: 800-525-6285

Order Report: 800-685-1111

Write: P.O. Box 740241

Atlanta, GA 30374-0241

- Experian- www.experian.com

Report Fraud: 888-397-3742

Order Report: 888-397-3742

Write: P.O. Box 2104

Allen, TX 75013

- TransUnion- www.tuc.com

Report Fraud: 800-680-7289

Order Report: 800-916-8800

Write: P.O. Box 1000

Chester, PA 19022

Logan Bank & Trust Contacts

Linda Disco
Head Bookkeeper
Logan Bank & Trust
PO Box 597
Logan, WV 25601
(304) 752-1166
ldisco@lbandt.com

Joy Lawson
Head Teller
Logan Bank & Trust
PO Box 597
Logan, WV 25601
(304) 752-1166
jlawson@lbandt.com

Karen Richardson
Asst. Head teller
Logan Bank & Trust
PO Box 597
Logan, WV 25601
(304) 752-1166
krichardson@lbandt.com

The information contained in this Policy is confidential and proprietary information of Logan Bank & Trust, and is intended only for use by Logan Bank & Trust Employees and Customers. Challenge questions can be implemented in a variety of ways that impact their effectiveness as an authentication tool. In its basic form, the user is presented with one or more simple questions from a list that was first presented to the customer when they originally enrolled in the online banking system. These questions can often be easily answered by an impostor who knows the customer or has used an Internet search engine to get information about the customer (e.g., mother's maiden name, high school the customer graduated from, year of graduation from college, etc.). In view of the amount of information about people that is readily available on the Internet and the information that individuals themselves make available on social networking websites, institutions should no longer consider such basic challenge questions, as a primary control, to be an effective risk mitigation technique.

Challenge questions can be implemented more effectively using sophisticated questions. These are commonly referred to as "out of wallet'' questions, that do not rely on information that is often publicly available. They are much more difficult for an impostor to answer correctly. Sophisticated challenge question systems usually require that the customer correctly answer more than one question and often include a "red herring" question that is designed to trick the fraudster, but which the legitimate customer will recognize as nonsensical. The Agencies have also found that the number of challenge questions employed has a significant impact on the effectiveness of this control. Solutions that use multiple challenge questions, without exposing all the questions in one session, are more effective. Although no challenge question method can mitigate all threats, the Agencies believe the use of sophisticated questions as described above can be an effective component of a layered security program.

Customer Awareness and Education

A financial institution's customer awareness and educational efforts should address both retail and commercial account holders and, at a minimum, include the following elements:

- An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access;

- An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials;

- A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically;

- A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found; and,

- A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events.