Customer Awareness Training *for* Internet Banking Services

Recently, BankTennessee 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 authentication mechanisms 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. Various complicated types of attack tools have been developed and automated into downloadable kits. Fraudsters are responsible for losses of hundreds of millions of dollars resulting from online account takeovers and unauthorized funds transfers.

Banks are providing the following security awareness information for your use and action to help protect your online account and transaction information.

BankTennessee

www.banktennessee.com

Protections and Liabilities for Consumer Transactions Using BankTennessee's Internet Banking Program

To access our Internet Banking service, you must use the ID and/or other means of access we establish. It is your responsibility to safeguard the ID and Password. 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 ID and Password or other means of access (even if that person exceeds your authority), 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 or credit 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.

Statements

Your Internet Banking payments and transfers will be indicated on the monthly statements we provide. Please notify us promptly if you change your address or if you believe there are any errors or unauthorized transactions on any statement, or statement information.

Unauthorized Transactions or Loss or Theft of Your Internet Banking ID or Password

If you believe your Internet Banking ID or PIN or other means of access have been lost or stolen or that someone has used them without your authorization, call us immediately at 901-854-0854, during normal business hours. After hours you may e-mail us at banktennessee.com, or write us at BankTennessee, 1125 West Poplar Ave., Collierville, TN 38017. Immediately contacting us by phone is the best way of reducing your possible losses, since not all e-mail 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 ID 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 may terminate your Internet Banking Agreement at any time upon giving Bank written notice of the termination. If you terminate, you authorize us to continue making transfers you have previously authorized until we have had a reasonable opportunity to act upon your termination notice. Once we have acted upon your termination notice, we will make no further transfers or payments from your Internet Banking Account. If we terminate your use of your Internet Banking Account, we reserve the right to make no further transfers of payments from your account including any transactions you have previously authorized.

You are responsible for all transfers you authorize using the Internet Banking services under this Agreement. If you permit other persons to use your Access Code, 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.

For Internet Banking transactions, if you tell us within 2 business days, you can lose no more than $50 if someone accessed your account without your permission. If you do not tell us within 2 business days after you learn of the unauthorized use of your account or Access Code, and we can prove that we could have prevented the unauthorized transaction if you had told us in time, you could lose as much as $500 or more. Your liability for unauthorized loan transactions through the Internet Banking service will not exceed $50.00.

Also, if your statement shows Internet Banking transfers that you did not make, tell us at once. If you do not tell us within sixty (60) days of the mailing date of your statement, you may be liable for the full amount of the loss if we can prove that we could have prevented the unauthorized transactions if you had told us in time. Should some emergency such as extended travel or hospitalization prevent you from contacting us, a reasonable extension of time will be allowed.

Limitation of Liability for Internet Banking Services

If we do not complete a transfer to or from your consumer account on time or in the correct amount according to our agreement with you, we will be liable and used primarily for personal, family, or household purposes. Our sole responsibility for an error in a transfer will be to correct the error. You agree that neither we nor the service providers shall be responsible for any loss, property damage or loss, whether caused by the equipment, software, or by Online browser providers such as Netscape (Netscape Navigator browser) and Microsoft (Microsoft Internet Explorer browser), or by Internet access providers or by online service providers or by an agent or subcontractor of any of the foregoing. Neither we nor the service providers will be responsible for any direct, indirect, special or consequential economic or other damages arising in any way out of the installation, download, use, or maintenance of the equipment, software, the BankTennessee Internet Banking services or Internet Browser or access software.

In this regard, although we have taken measures to provide security for communications from you to us via the BankTennessee Internet Banking Services and may have referred to such communication as "secured," we cannot and do not provide any warranty or guarantee of such security. In states that do not allow the exclusions or limitation of such damages, our liability is limited to the extent permitted by applicable law.

Additionally, BankTennessee will not be liable for the following:

- If, through no fault of ours, you do not have enough money in your account to complete a transaction, your account is inactive or closed, or the transaction amount would exceed the credit limit on your line of credit.

- If you used the wrong Access Code or you have not properly followed any applicable computer, Internet, or BankTennessee user instructions for making transfer and bill payment transactions.
- If your computer fails or malfunctions or the Internet Banking service was not properly working and such problem was or should have been apparent when you attempted such transaction.
- If, through no fault of ours, a bill payment or funds transfer transaction does not reach a particular creditor and a fee, penalty, or interest is assessed against you.
- If circumstances beyond our control (such as fire, flood, telecommunications outages or strikes, equipment or power failure) prevent the transaction.
- If the funds in your account are subject to legal process or other claim, or if your account is frozen because of a delinquent loan, overdrawn account, or suspected fraud.
- If the error was caused by a system beyond the BankTennessee's control such as a telecommunications system, or Internet service provider.
- If you have not given BankTennessee complete, correct, or current information so BankTennessee can process a transaction.

Billing Errors

In case of errors or questions about your Internet Banking transactions, telephone us at the phone numbers or write us at the address set forth above as soon as you can. We must hear from you no later than sixty (60) days after we sent the first statement on which the problem appears.

- Tell us your name and account number.
- Describe the transaction you are unsure about, including the transaction confirmation or reference number if applicable, and explain as clearly as you can why you believe it is an error or why you need more information.
- Tell us the dollar amount of the suspected error.

The following two paragraphs apply only to consumer accounts (an account belonging to a natural person and used primarily for personal, family, or household purposes):

If you tell us orally, we may require that you send us your complaint or question in writing within ten (10) business days. We will tell you the results of our investigation within ten (10) business days after we hear from you and will correct any error promptly. For errors related to transactions occurring within thirty (30) days after the first deposit to the account (new accounts), we will tell you the results of our investigation within twenty (20) business days. If we need more time, however, we may take up to forty-five (45) days to investigate your complaint or question (ninety (90) calendar days for new account transaction errors, or errors involving transactions initiated outside the United States). If we decide to do this, we will re-credit your account within ten (10) business days for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within ten (10) business days, we may not re-credit your account.

If we decide after our investigation that an error did not occur, we will deliver or mail to you an explanation of our findings within three (3) business days after the conclusion of our investigation. If you request, we will provide you copies of documents (to the extent possible without violating other members' rights to privacy) relied upon to conclude that the error did not occur.

a. BankTennessee will never contact any customer and request electronic banking credentials. If you get a call asking for your credentials, hang up and call us!

b. If you are an BankTennessee commercial online banking customer we suggest you periodically evaluate the possible risks to your account. Some key areas to check are:

- Who has access to the internet banking PC and credentials?
- Is (Are) the internet banking PC or PCs secured after normal business hours?
- Do you have up to date antivirus and anti-malware software on the PC?
- How often do you change the internet banking password and who knows the password?
- Is there a firewall active on your PC?

Tips to Reduce the Risk in Internet Banking

- 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. Yes, you'll have to enter passwords more often, but it's a smarter way to surf.
- Don't put your full birth date on your social-networking profiles: Identity thieves use birth dates as cornerstones of their craft. If you want your friends to know your birthday, try just 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. Some unscrupulous or careless entities collect lots of data and then lose, abuse, or sell them. If the app maker is in the U.S., it's probably safer, and at least you have recourse if something should ever go wrong.
- Use multiple usernames and passwords: Keep your usernames and passwords for social networks, online banking, e-mail, and online shopping all separate. Having distinct passwords is not enough nowadays: If you have the same username across different Web sites, your entire romantic, personal, professional, and e-commerce life can be mapped and re-created with some simple algorithms. It's happened before.

For any Internet Banking problems, concerns or if something doesn't look right, call us at 901-854-0854.

Thank you for being our customer!

BankTennessee
MEMBER FDIC

For Our Business Customers

Tips to Avoid ACH Fraud

These recommendations are to protect for business customers that want to protect their online banking credentials and strengthen ACH (Automated Clearing House) and wire security procedures.

Account Controls

- Recommend educating customers about account features that may protect their accounts, such as check cashing limitations and automated payment filters.
- Recommend reconciliation of all banking transactions on a daily basis.
- Recommend customers initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.

21 Best Practices to Protect You and Your Business

Recommended for corporate customers to secure computer systems

1. If possible, and in particular for customers that do high value or large numbers of online transactions, carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.
2. Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credential such as usernames, passwords, PIN codes similar information. Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack their computer.
3. Install a dedicated, actively managed firewall, especially if you have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
4. Create a strong password with a least 10 characters that includes a combination of mixed case letters, numbers and special characters.
5. Prohibit the use of "shared" usernames and passwords for online banking systems.
6. Use a different password for each website that is accessed.
7. Change the password a few times each year.
8. Never share username and password information for Online Service with third-party providers.
9. Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other services.
10. Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
11. Ensure virus protection and security software are updated regularly.
12. Ensure computers are patched regularly particularly operating system and key application with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.

13. Consider installing spyware detection programs.
14. Clear the browser cache before starting an Online Banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preferences menu.
15. Verify use of a secure session (https not http in the URL) in the browser for all online banking.
16. Avoid using an automatic login features hat save usernames and passwords for online banking.
17. Never leave a computer unattended while using any online banking or investing service.
18. Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.
19. Customers must familiarize themselves with the institution's account agreement and with the customer's liability for fraud under the agreement and the Uniform Commercial Code as adopted in the jurisdiction.
20. Stay in touch with other businesses to share information regarding suspected fraud activity.
21. Immediately escalate any suspicious transactions to the financial institution particularly, ACH or wire transfers. There is a limited recovery window for these transactions and immediate escalation may prevent further loss by the customer.

For any Internet Banking problems, concerns or if something doesn't look right, call us at 901-854-0854.

Thank you for being our customer!

BankTennessee
MEMBER FDIC