INTERNET BANKING AUTHENTICATION
Keeping Your Banking Information Safe in a Digital World

Understanding the Risks

According to the Federal Financial Institutions Examination Council (FFIEC), there have been significant changes in the threat landscape recently. 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, increasing availability and permitting their use by less experienced fraudsters. Malware surreptitiously installed on a personal computer (PC) can monitor a customer's activities and facilitate the theft and misuse of their login credentials. Such malware can compromise some of the most robust online authentication techniques, including some forms of multi-factor authentication. As a result, cyber-crime complaints have risen substantially each year since 2005, particularly with respect to commercial accounts. Fraudsters are responsible for losses of hundreds of millions of dollars resulting from online account takeovers and unauthorized funds transfers.

Protecting Your Account
Authentication

There are a variety of technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, and others.

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN).

Mutual authentication is a process whereby customer identity is authenticated and the target Web site is authenticated to the customer. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack. The spoofed sites are so well constructed that casual users cannot tell they are not legitimate.

TnBank utilizes several authentication methods for your protection. You will be required to enter your access ID. At this point, we utilize mutual authentication by displaying the unique picture you selected when you enrolled for internet banking. If you do not see the image you selected, do not proceed with the login attempt and contact TnBank immediately. If you recognize your image *and* our computer recognizes your IP address, you will be granted access to your account(s). If you are logging in from a different IP address that the Bank's computer does not recognize as one you have previously used, you will be asked to answer one or more security questions to verify your identity. These security questions were selected by you when you enrolled.

Protecting Your Account
Layered Security

Layered security is characterized by the use of different controls at different points in a transaction process so that a

weakness in one control is generally compensated for by the strength of a different control. Effective controls that may be included in a layered security program include, but are not limited to:

- fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- the use of dual customer authorization through different access devices;
- the use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;
- enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times);

TnBank utilizes several of the above security measures to protect its customers. Our fraud monitoring service constantly monitors activity on all accounts and will flag patterns of activity which are outside of the usual pattern for that customer. If unusual activity is detected, we may contact you to determine whether the activity is legitimate. Please note that TnBank will never independently contact you to ask for your online banking username and password. If we contact you, we will positively identify ourselves as Bank employees. If you are concerned about the possibility of fraud, you may wish to call us back and ask to speak to the individual who contacted you.

Additionally, the Bank has set transaction volume and dollar limits on electronic and point-of-sale activity which should limit exposure to potential fraud.

For our business customers, another layer of security is required to send money out of your account via ACH. Most customers will be required to separately verify that the requested activity is legitimate prior to the Bank making these types of payments.

Customer Awareness
Steps to Protect Yourself

Understanding the risks and the various channels that fraudsters use to steal your information is an important first step. You should also make your computer as safe as possible by regularly installing and updating the following:

- Anti-virus software
- Anti-malware programs
- Firewalls
- Operating system patches and updates

You can also visit the following websites to learn more about online safety and security:

staysafeonline.org

ftc.gov

usa.gov

idtheft.gov

Business customers should also perform periodic internal assessments to ensure the highest level of possible security for their accounts. Those assessments should take into consideration the business' internal controls such as policies, procedures, system administrator access, and transactional risk levels, among other things.

Your Protections Under Regulation E

TnBank follows regulatory guidelines for disputed electronic transactions. These guidelines are found in Regulation E, issued by the Federal Reserve Board. Under those guidelines, consumers may recover losses associated with electronic transactions based on how quickly they are reported to the Bank. It is important that you notify us as soon as possible if you identify activity on your account which you suspect is fraudulent.

If You Have Questions or Concerns

If you notice suspicious activity in your account or experience security-related events, you should immediately contact TnBank at (865) 483-9444.