The State of Cybersecurity

Online Banking Authentication & Layered Security

Important facts about account access

Multi-factor authentication and layered security are helping assure safe Internet transactions for banks and their customers.

The Federal Financial Institutions Examination Council (FFIEC) has issued supervisory guidance titled “Authentication and Access to Financial Institution Services and Systems” to help banks strengthen their risk assessment practices. The goal is to make sure that the person signing into your account is actually you. This information was compiled by banking industry and cyber-security experts to make online transactions of virtually all types safer and more secure — now and into the future.

Understanding the factors

Online security begins with the authentication process, used to confirm that it is you, and not someone who has stolen your identity. Authentication generally involves one or more basic factors:

- Something the user ***knows*** (e.g., password, PIN)
- Something the user ***has*** (e.g., ATM card, smart card)
- Something the user ***is*** (e.g., biometric characteristic, such as a fingerprint).

Single factor authentication uses one of these methods; multi-factor authentication uses more than one, and thus is considered a stronger fraud deterrent. When you use your ATM, for example, you are utilizing multi-factor authentication: Factor number one is something you have, your ATM card; factor number two is something you know, your PIN.

To assure your continued security online, your bank uses mostly multi-factor authentication, as well as additional “layered security” measures when appropriate.

Layered security for increased safety

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. An example of layered security might be that you follow one process to log in (user/password), and then give additional information to authorize funds transfers.

The purpose of these layers is to authenticate customers and detect and respond to suspicious activity.

Layered security can substantially strengthen the overall security of online transactions and protecting sensitive customer information.

Internal risk assessments at your bank

The goal is to ensure that the level of authentication called for in a particular transaction is appropriate to the transaction's level of risk. Your bank conducts comprehensive risk assessments of its current methods and considers, for example:

- changes in the internal and external threat environment
- changes in the customer base adopting electronic banking
- changes in the customer functionality offered through electronic banking; and
- actual incidents of security breaches, identity theft, or fraud experienced by the industry.

This FFIEC Guidance addresses the expanded threat landscape and with banks will determine the appropriate authentication and layered security systems.

Enhanced controls for higher risks

Whenever increased risk to your transaction security might warrant it, your bank might use additional verification procedures, or layers of control, such as:

- **Utilizing call-back (voice) verification,** e-mail approval, or smart phone-based identification.
- **Employing customer verification procedures,** especially when opening accounts such as memorized secrets, look-up secrets, out-of-band devices, one-time passwords, biometric identifiers or cryptographic keys, etc.
- **Analyzing banking transactions to identify suspicious patterns.** For example, that could mean flagging a transaction in which a customer who normally pays $10,000 a month to five different vendors suddenly pays $100,000 to a completely new vendor.
- **Establishing dollar limits that require manual intervention** to exceed a preset limit.

Your liability protections under federal law

Federal laws provide strong protections if your credit or debit card is used to make unauthorized purchases.

Credit cards – The Truth In Lending Act limits consumer liability for unauthorized use of your credit card. If someone steals your credit card, then your liability is capped at $50 for unauthorized charges. If you report the loss before any charges occur, then you have no liability. Lastly, if someone uses your credit card number, but not the card itself, then you have no liability for unauthorized use.

Debit cards – The Electronic Funds Transfer Act limits consumer liability for funds stolen from your debit card account through fraud, such as skimming and for other unauthorized transfers, depending on how quickly you report the loss. Your liability can range from $50 to $500, or more. (visit www.ftc.gov for a full detailed explanation)

These federal protections can be modified by state law or by policies at your bank, so be sure to ask your banker how these protections apply to your situation.

Customer vigilance: The first line of defense

Of course, understanding the risks and knowing how fraudsters might trick you is a critical step in protecting yourself online. You can make your online banking experience safer by installing and updating regularly on all your devices:

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

You can also learn more about online safety and security at these websites:

www.staysafeonline.org
www.ftc.gov
www.usa.gov
www.idtheft.gov
www.federalreserve.gov

www.consumerfinance.gov
www.treasury.gov
www.fdic.gov
www.ncua.gov
www.occ.gov

What can I do?

If you notice suspicious activity within your account or experience security-related events please contact your bank. And remember your bank will never ask you to provide your account information — they already have it.