SANTA CRUZ COUNTY BANK

Put your money where your life is.

FFIEC Consumer Guidance

Account Authentication & Online Banking

Important facts

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

If you use online or mobile banking, you will be interested to learn that six federal financial industry regulators teamed up recently to make your accounts more secure. New supervisory guidance from the Federal Financial Institutions Examination Council (FFIEC) will help banks strengthen their vigilance and make sure that the person signing into your account is actually you. The supervisory guidance is designed to make online transactions of virtually all types safer and more secure.

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 both single and 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.

Layered security can substantially strengthen the overall security of online transactions…protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses.

The purpose of these layers is to allow your bank to authenticate customers and detect and respond to suspicious activity related to initial login and then to reconfirm this authentication when further transactions involve the transfer of funds to other parties.

Internal assessments at your bank

On the back-end, the new supervisory guidance offers ways your bank can look for anomalies that could indicate fraud. 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. Accordingly, your bank has concluded a comprehensive risk assessment of its current methods as recommended in this supervisory guidance. These risk assessments consider, 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 institution or industry.

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

- **Utilizing call-back (voice) verification,** e-mail approval, or cell phone based identification.
- **Employing customer verification procedures,** especially when opening accounts online.
- **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 protections under "Reg E"

Banks follow specific rules for electronic transactions issued by the Federal Reserve Board. Known as **Regulation E,** the rules cover all kinds of situations revolving around transfers made electronically. Under the consumer protections provided under **Reg E,** you can recover internet banking losses according to how soon you detect and report them.

Here is what the Federal rules require: If you report the losses within two days of receiving your statement, you can be liable for the first $50. After two days, the amount increases to $500. After 60 days, you could be legally liable for the full amount. These 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 particular 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 computer safer by installing and updating regularly your:

- 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.com
www.ftc.gov
www.usa.gov
www.idtheft.gov

If you have suspicions

If you notice suspicious activity within your account or experience security related events (such as a Phishing email from someone purporting to be from your bank), you can contact anyone at your bank and you will be quickly and courteously guided to the person responsible for such issues.