

Together We Can Increase Security

In an ideal world, we would not have to worry about money laundering, terrorist financing, identity theft, and fraud. But we do not live in an ideal world. By using more than one kind of authentication, we can significantly increase security.

We Must Be Mutually Vigilant

But even this increased security is not enough. In order to maximize security, we must work together, vigilantly monitoring Internet transactions and communicating with each other and the proper authorities whenever red flags appear. Only then can we hope to minimize money laundering, terrorist financing, identity theft, and fraud.



*More Than
One Kind of
Authentication*

CUSTOMER IMPRINT HERE

Authentication

“Authentication” is our means of determining that the persons or entities we’re dealing with are genuinely who they claim to be.

Why Use More Than One Kind of Authentication?

A common question account holders have is why we use more than one kind of authentication, especially over the Internet?

For the Security of All of Us

A recent federal financial institutions guidance states that effective authentication systems are essential to:

- Prevent money laundering, terrorist financing, identity theft, and fraud;
- Accomplish legally enforceable electronic transactions; and
- Satisfy account holder information safekeeping requirements.

The guidance notes that financial dealings with incorrectly identified or unauthorized persons over the Internet can result in financial loss and reputation damage due to fraud, disclosure of account holder information, data corruption, and unenforceable agreements.

More Than One Kind of Authentication is More Effective

The guidance states that authentication methods that depend on more than one factor are harder to fool than single-factor methods. Thus, multifactor methods are more reliable and better deterrents of fraud.

What Kinds of Authentication Are Available?

The guidance indicates that authentication methods are ordinarily based on one or more of the following factors:

- Something you know, such as a password or PIN;
- Something you have, such as an ATM card or smart card; or
- Something you are, such as a fingerprint or other biometric characteristic.

More Than One Kind of Authentication is Essential for Certain High-Risk Transactions

The guidance states that single-factor authentication is inadequate, and multifactor authentication is essential, for high-risk transactions involving access to account holder information or movement of funds to third parties. The guidance notes that single-factor authentication

methods, including passwords or PINs, have been widely used in Internet banking, but states that their adequacy should be reassessed in light of sophisticated and evolving new fraud techniques, including phishing, pharming, and malware. If a risk assessment indicates that single-factor authentication is inadequate, multifactor authentication should be implemented.

USA PATRIOT Act Identity Verification When a New Account is Opened Over the Internet

The guidance indicates that USA PATRIOT Act identity verification when a new account is opened over the Internet can include the following:

- *“Positive verification”* to determine whether the information provided by the applicant matches what’s available from trusted databases or other sources, such as credit reports.
- *“Logical verification”* to determine whether the information provided by the applicant is logically consistent, such as whether telephone area code, ZIP code, and street address are consistent with each other.
- *“Negative verification”* to determine whether the information provided by the applicant has been associated with fraud, such as by comparison with fraud databases.