

BITS

FINANCIAL SERVICES
R O U N D T A B L E

CONSUMER EDUCATION FOR ONLINE BANKING AND OTHER FORMS OF FRAUD

Consumer education is critical to preventing Internet fraud. Most individuals will take action if they believe it will decrease their chances of being victimized by fraud, as long as the action does not significantly inconvenience them. By educating customers, financial institutions can decrease their fraud losses.

The following are consumer tips to prevent fraud. Institutions can share this information with customers through various channels, such as postings at the branches, flyers sent with monthly statements, emails, through a Web site, and/or by request to a call center.

CONSUMER TIPS TO PREVENT IDENTITY THEFT AND OTHER FORMS OF FRAUD

- **Ensure you know the person/entity you are giving information** to over the Internet.
- At least once a year, **order copies of your credit report** from each of the three major credit bureaus, ensuring all of the information is accurate.
- **Monitor your accounts and monthly statements thoroughly**, ensuring that all the activity is accurate. If your account statements are late, immediately contact your bank(s) to ascertain if and when they were mailed. If your institution offers online banking, check your account periodically, rather than waiting for monthly statements. Reporting the fraud as soon as possible will assist in stopping further occurrences of fraud.
- **Always thoroughly tear or shred personal information**, such as pre-approved credit offers, that may contain account information, Social Security numbers, date of birth, etc.
- **Check merchant privacy policies** and only shop with those who have published privacy policies that you agree with.
- **Only do business with Internet companies that use a secure form** to capture private information, such as account numbers or credit card numbers. (The key or lock symbol on your browser status bar indicates whether or not a page is secure.)
- **Discard unused instant credit offers**, ensuring they are properly shredded/discarded if not used.

- **Ensure your computer(s) are equipped with anti-virus protection and firewalls** to help keep trespassers out. Update your anti-virus software frequently, and periodically check your firewall settings. Always back up your data.
- **Install security patches when issued by the software (operating system and browser) vendor.**
- **Shut off/disconnect your computer from the Internet when not in use.**
- **Never divulge personal information to anyone**, as identity thieves often obtain information through social engineering.
- **Avoid purchasing a product from a merchant or an auction site where the deal looks “too good to be true”** because it usually is.
- **Confirm the legitimacy of an online business by clicking on the solid lock or key symbol on your browser window**, which provides information about the merchant from the server certificate. If the certificate was issued by an independent certificate authority, due diligence has been performed on the business. If someone has cloned a site, the site will not have a certificate. If the certificate name does not match the site, do not use it and notify the institution.
- **Always protect your account information.** Don't write your personal identification number (PIN) on your ATM/Debit Card. Don't write your Social Security number and/or credit card number on a check.
- **When using your ATM, cover your hand when entering the PIN number** to protect the information from shoulder surfers.
- **Carry only those pieces of identification you absolutely need**, and keep them secure.
- **Always log off from your online banking session.**
- **If you suspect your identity has been stolen, contact your financial institution and the authorities immediately.** U.S. consumers should file a police report with their local police department and call the Federal Trade Commission at 1-877-ID-Theft. Complaints can also be reported to the Internet Fraud Complaint Center at www.ifccfbi.gov. Contact the three credit reporting agencies to place a fraud alert on your record. Maintain a log of all contacts you make with the authorities regarding the matter, including the name, title, phone number and police case number, in case future contact is required.