Dear Valued Customer,

(Bank name) has published this guide to help raise consumer awareness of identity theft.

The security of your private information is very important to us. (Bank name) will never provide your confidential information to any source not affiliated with the bank. We will also never ask you for personal information through email.

The best defense against identity theft is to "be informed". We encourage you to share this guide with your family, friends, colleagues, and neighbors.

For more information please visit our Website at www.bankname.com.

Sincerely,

(Signature)

Name
Title
Bank Name

Logo

www.financialinstitution.com
Email: name@financialinstitution.com

MAIN OFFICE

7000 S. Main Street
Anytown, USA 10000

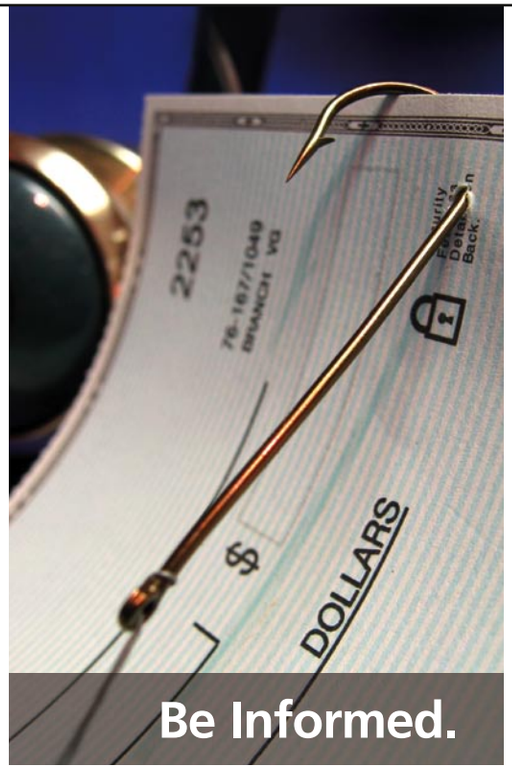
Phone: 555-555-1212
Fax: 555-555-1213

OTHER LOCATIONS

7000 S. Main Street
Anytown, USA 10000

Phone: 555-555-1212
Fax: 555-555-1213

Member FDIC *Equal Housing Lender*

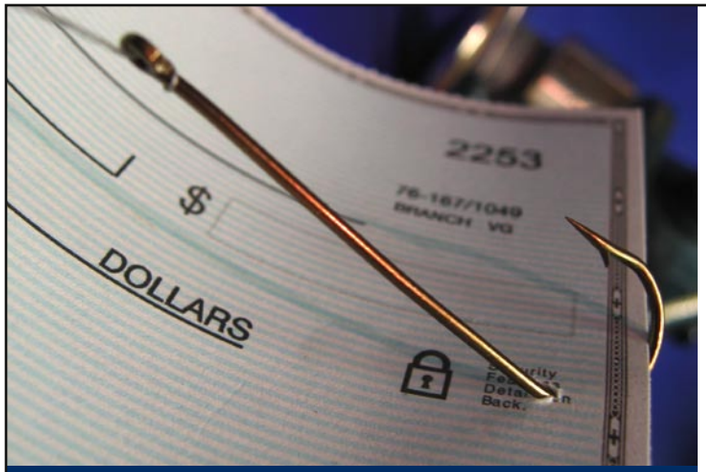


Be Informed.

Fraud Alert!

The best way to protect yourself against identity theft.

Logo



What is Identity Theft?

Identity theft occurs when someone uses your name, address, Social Security number (SSN), bank or credit card account numbers, passwords, or other personal information without your knowledge to commit fraud or other crimes.

While on-line banking and e-commerce are very safe with built-in security features for your protection, to avoid identity theft you should always be careful about responding to unsolicited requests for your personal financial information via the Internet, email, phone or mail.

Be Informed. Don't get "Phished".

One of the most common forms of stealing your banking account information is through a process called "Phishing". This is a scam that uses email to deceive you into disclosing personal information.

How to spot Phishing:

- The email and linking Website may appear authentic. *It may look just like our Website.*
- It may ask you to "update" or "validate" your account information! (*Bank name) will never ask for private information by email or unsecured Website.*
- Often it will threaten some consequence if you don't respond.

These are clear indicators that someone is "Phishing" for your information.

Steps to avoid being Phished

If you receive a suspicious email from (bank name) requesting personal information such as Social Security number, bank and credit card numbers, user names and passwords, follow these important guidelines:

1. Do not reply to the email, even if it appears urgent.
2. Do not use the links from the email to open any Web page.
3. Alert (bank name) immediately at 555-1212. Don't call any phone numbers appearing on the email.

Even though the laws are on your side, it's wise to take an active role in protecting your information.

REMEMBER!

(Bank Name) will never request personal or account information through email!

If you think you've been Phished, here's what to do now:

A. Contact (bank name) immediately at 555-1212.

B. Place a fraud alert on your credit report with the three major credit bureaus. Also request to review your credit reports for suspicious activity at that time.

Equifax: 1-888-766-0008
Experian: 1-888-397-3742
Trans Union: 1-800-680-7289

C. File a complaint with the Federal Trade Commission at www.ftc.gov.

For more information about protecting yourself against identity theft, visit our Website at www.bankname.com.

Logo