What is Identity Theft?

Identity theft occurs when someone uses your personal information, without permission, in an attempt to commit fraud or theft. Thieves can take over your existing accounts or try to open new ones. You may not know you have been a victim of this crime until the fraudulent activity appears on your credit report, bills or bank statement.

There are many ways that criminals can obtain your information, ranging from the loss or theft of a wallet or purse, to dumpster-diving (stealing records from your trash). You may receive an e-mail that claims to be from a legitimate site (phishing); or your attempts to visit a legitimate website may be re-directed, instead sending you to a bogus website (pharming). Taking advantage of a possible key-stroke error, you may also get linked to a site that uses graphics, names and codes that appear to be the same as a legitimate site (website spoofing). Any information you share may be routed to Internet criminals.

ID Theft Victims Should Take These Immediate Steps:

Notify your creditors.

Ask to speak with someone in the security or fraud department; follow up in writing sent by certified mail, return receipt requested. Close accounts as necessary; select different passwords and PINs (Personal Identification Numbers) for new accounts opened. Your call also alerts the financial institution to a possible scam that may be targeting other customers.

If you believe your Patriot accounts have been compromised, contact Patriot Bank, N.A. immediately at **1.888.PATRIOT (728.7468)**. Forward suspicious e-mails to: **banking@bankpatriot.com**.

Contact one of these credit bureaus to place a "fraud alert" on your credit reports.

The company you call is required to for ward the information to the other two. Creditors will then be instructed to obtain your authorization before opening any new accounts. Ask for free copies of your reports and review them periodically.

Equifax:	**1.800.525.6285** or **www.equifax.com**
Experian:	**1.888.397.3742** or **www.experian.com**
Trans Union:	**1.800.680.7289** or **www.transunion.com**

File a complaint with the Federal Trade Commission.

You can contact them online at: **www.ftc.gov/idtheft**

call them at: **1.877.IDTHEFT (438-4338)**

or write them at:
Identity Theft
Clearinghouse, FTC,
600 Pennsylvania Ave. NW
Washington, DC 20580.

Remember to keep records of all your conversations and copies of all your correspondence.

How to protect your privacy and your identity

Review your credit report every 6-12 months. You are entitled to a free credit report once every 12 months from each of the nationwide credit bureaus.

You may order your report online at **www.annualcreditreport.com**, print a request form at: **www.ftc.gov/credit**

or by calling toll-free: **1.877.322.8228**

- Shred documents or any other identifying information before discarding them. This includes pre-approved credit card offers, charge receipts, checks, bank statements and insurance forms.
- Before disclosing any personal information make sure you know why it's needed and how it will be used; especially if you did not initiate the contact.
- Use secure personal identification numbers or passwords. Put passwords on all your financial accounts.
- Monitor and review all bank and financial account statements as soon as they arrive. Look for unexplained charges or withdrawals.
- Retrieve your incoming mail promptly; don't leave outgoing mail in your mailbox.
- Take receipts from ATMs, gas pumps and restaurants.
- Report lost or stolen credit and/or debit cards immediately.

On Your Computer:

- Update the virus protection software regularly.
- Do not reply to e-mail or pop-up messages asking for personal or financial information or click on links that direct you to another site.
- Don't e-mail personal or financial information.
- If you initiate a transaction make sure the site or message is secure. Look for a lock icon.
- Use a "wipe" utility program to overwrite your hard drive before disposing of a computer.

Patriot Bank, N.A. never requests personal information from customers via e-mail and never directs customers by e-mail to click on an icon or URL. We appreciate your business and will do everything that we can to protect your identity.