Studies show repeatedly that identity fraud happens much more often offline than online. However, INB feels it is important that you have the information necessary to safely conduct your personal business online. Follow this guide to learn how to prevent, detect, correct and report online fraud and identity theft.

PREVENT

Prevention is the most critical element to avoiding online fraud. Try to incorporate these items into your routine.

Prevent: General Online Security

- Shred all financial documents and paperwork with personal information, do not simply throw them in the trash.
- Protect your Social Security number. Don't carry your Social Security card in your wallet or write it anywhere. Give it out only if absolutely necessary or ask to use another identifier.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- Never click on links sent in unsolicited emails; instead, type in a web address you are already familiar with.
- Use firewalls, anti-spyware, and anti-virus software to protect your home computer -- and keep them current.
- Create passwords that are unusual: do not use your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- Keep your personal information in a secure place at home, especially if you employ outside help, have roommates, or are having work done in your house.
- Ordering online? Only use "secure" web pages (a web page is secure if there is a locked padlock in the address bar of your browser)
- Do not click on links or open attachments in emails unless you know the sender and were expecting the email.
- Place a "Fraud Alert" on your credit reports, and review the reports carefully.

    The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The following consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert. Choose one of the following:
    Equifax: 1-800-525-6285
    Experian: 1-888-EXPERIAN (397-3742)
    TransUnion: 1-800-680-7289

Innovis: 1-800-540-2505

- When your computer is not in use, shut it down or disconnect it from the Internet.
- Always sign off from your Online Banking session
- Avoid clicking on links provided in emails. It is always better to type the address into your browser
- Most computer files have filename extensions, such as ".doc" for documents or ".jpg" for images. Any file that appears to have a double extension, like "heythere.doc.pif" is extremely likely to be a dangerous file and should never be opened.
- Never open email attachments that have file endings of .exe, .pif, or .vbs. These are file extensions for executables, and are commonly dangerous files.
- Be careful and selective before providing your email address to a questionable website. Sharing your email address makes you more likely to receive fraudulent emails.

DETECT

Detect: Online Banking Security

Take advantage of online tools we have that automatically protect you, including:

Balance Alerts

- Check Clear Alerts
- Payment Alerts
- Online Statements
- Account History

Business Online Banking

- Alerts
- Account Reconciliation/PositivePay (Business customers only)

Detect: General Online Security

Despite all efforts to prevent it, identity fraud can still occur. The earlier it is detected, however, the swifter we can help you take action to stop it.

Be alert and take immediate action to the following:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you didn't make

Take advantage of free annual credit reports: Credit reports contain information about what accounts you have and your bill paying history. Free copies are required by law from the major nationwide consumer reporting companies: Equifax, Experian, and TransUnion. Visit www.AnnualCreditReport.com or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283.

- Review your financial and billing statements regularly and look for charges you did not make.
- Keep a list of all your credit card numbers and phone numbers in case of theft, and notify each card issuer immediately if theft occurs.

CORRECT

Correct: General Online Security

- Close any accounts that have been tampered with or established fraudulently.
- Call the security or fraud departments of each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.
- Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
- Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- Keep copies of documents and records of your conversations about the theft.
- File a police report. File a report with law enforcement officials to help you with creditors who may want proof of the crime.

REPORT

Report: Online Banking Security

Always report theft and fraudulent activity to your financial institution, no matter if you are a victim or suspect the activity.

Report: General Online Security

Report the theft to the Federal Trade Commission. Filing a report helps law enforcement officials across the country in their investigations:

Online: ftc.gov/idtheft
By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261
By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580