Identity Theft and Fraud Prevention

Community Bank of Pickens County values our customers and hope you never become the victim of Identity Theft or Cyber-Fraud. Because these are such fast-growing crimes, we want you to be aware of the basic precautions you can take to protect yourself.

Protect Yourself from Identity Theft

- Please contact us at once should you receive phone calls or e-mails of a suspicious nature regarding your accounts with us.
- Regularly check all of your bank and billing statements.
- If you see any possible errors or something you do not understand, call and inquire with our Bookkeeping Department at 706-253-9600.

Basic Precautions:

- Make sure your drivers license and social security numbers are not the same.
- Be careful not to carry too much personal information in your wallet or purse (i.e.: Social Security card, bank and credit card numbers with passwords and PINs).
- Do not give out personal information over the phone if you did not initiate the call.
- Destroy all pre-approved credit card applications if you are not going to take advantage of them.
- Make a copy of the contents of your wallet – then keep this information in a safe place.
- Online security – make sure your browser's padlock or key icon is active when sending or viewing personal or financial information. The icon usually appears on the bottom of the navigation bar of your browser window when using a secured site. As an added protection while on CBOPC's site, an "s" appears after the http – https//. DO NOT open the Community Bank of Pickens County website unless this "s" is present.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges.
- If you have not received a bill or statement you were expecting after the usual mailing time, contact the company or creditor to confirm your billing address and account balances.
- Never place outgoing mail in your personal mailbox. Use the post office or postal mail drops.
- Always exclude your social security and driver's license numbers from being printed on checks.
- Make sure your unused checks, bills, credit/debit card receipts, credit card applications you receive in the mail where you have already been pre-qualified and statements are shredded before discarding.
- Regularly order a copy of your credit report to check for any unusual or unknown items. For a free report, call toll-free 1-877-322-8228 or go to www.annualcreditreport.com.

General tips against Cyber-Fraud:

- Use Anti-Virus Software and keep it up to date. Look for Anti-Virus Software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.
- Use a Firewall. A Firewall makes you invisible on the internet and blocks all communications from unauthorized sources. This is especially important if you have a broad band connection.
- Use Common Sense – The internet is a great tool for information, but consumers should take appropriate precautions and be aware of the possibility that someone may be trying to scam them.

Internet fraud can be any type of scheme that uses the internet – chat rooms, email, message boards or websites – to deceive prospective victims. These schemes, scams and frauds take advantage of the Internet's unique

capabilities – sending email messages worldwide in seconds or posting website information that is readily accessible from anywhere in the world – to carry out fraud quicker than ever possible in the past.

- Phishing

Phishing is a high tech scam that uses spam or pop-up messages to trick you into disclosing your personal credit card numbers, bank account information, Social Security number, passwords or other sensitive information. The message claims to be from a business or organization that you deal with such as your Internet Service Provider, bank, online payment service, or even a government agency.

The message usually states that you need to "update" or "validate" your account information. It might threaten some consequence if you don't respond. It usually contains a link to what appears to be the bank WEB site but is in fact a bogus site created to STEAL your identity and account information.

Defense Tactics against Phishing:

- If you receive an email that warns you, with little or no notice, that your account will be shut down unless you reconfirm certain information, do not click on the email link. Instead, use a phone number or enter the web address yourself. Clicking on a link that looks legitimate may in fact direct you to a fraudulent website where crooks will steal your personal information. ***Remember, CBOPC or a government agency will never send you an alert asking you to disclose your personal information***.

- Spoofing

Web spoofing allows an attacker to create a "shadow copy" of any legitimate website. Access to the shadow web is funneled through the attacker's machine, allowing the attacker to monitor all of the victim's activities, including any passwords or account numbers the victim enters. The attacker can also cause false or misleading data to be sent to web servers in the victim's name, or to the victim in the name of any web server. In spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by "spoofing" the address of that machine. Phishing and spoofing often go hand-in-hand in internet fraud.

Defense Tactics against Spoofing:

- Be wary of unsolicited or unexpected emails from all sources.
- If an unsolicited email arrives, treat it as you would a phishing source. Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them.

If you become a victim of Identity Theft, immediately take the following steps:

1. Contact each of the credit reporting agencies to request a fraud alert be placed in your credit file.
   Equifax – 1-800-525-6285 www.equifax.com
   Experian – 1-888-397-3742 www.experian.com
   TransUnion – 1-800-680-7289 www.transunion.com
2. Contact your local police or sheriff's department and make a report. Be sure to record the report number and obtain a copy.
3. Notify all of your financial institutions and credit grantors.
4. Contact Government Agencies:
   The Federal Trade Commission:
   1-877-IDTHEFT (488-4338).
   Consider filling out an "ID Theft Affiadavit" available at www.consimer.gov/idtheftftc.gov
   Governor's Office of Consumer Affairs: 1-800-869-1123 www.georgia.gov

General tips against Cyber-Fraud:

- Use Anti-virus Software and keep it up to date.
- Use a firewall. It is especially important to run a firewall if you have a broadband connection.
- Use Common Sense. The internet is a great took for information, and to conduct on-line business, as long as consumers take appropriate precautions and are aware of the possibility that someone may be trying to scam them.
- You can file a complaint with the FTC against a company or organization that you believe has cheated you by contacting the Consumer Response Center by phone: toll free 877-382-4357.

Consumer Resources:
- The consumer information links below exist to assist customers in locating information about online security and providing guidance on how to file complaints when appropriate.

- Internet Crime Complaint Center – www.ic3.gov
- Financial Fraud Enforcement Task Force – www.stopfraud.gov
- On Guard Online – www.onguardonline.gov
- FDIC Consumer Protection – www.fdic.gov/consumers/theft/
- Microsoft Online Safety – www.microsoft.com/protect/
- Apple Product Security – www.apple.com/support/security/

The following are two really good sites that offer much more in depth information on identity theft and what to do if you become a victim of identity theft:

- www.ftc.gov/bcp/edu/mcrosites/idtheft/consumers/about-identity-theft.html
- www.justice.gov/criminal/fraud/websites/idtheft.html