How to Protect Yourself

Community Neighbor is committed to keeping your information secure. In order to safeguard your personal identifiable financial information and minimize your risk of becoming a victim of fraud or identity theft, there are a number of steps you can take to safeguard your information.

Personally Identifiable Information

- Always protect personally identifiable information, such as your date of birth, Social Security Number, credit and debit card numbers, bank account numbers, Personal Identification Numbers (PINs) and passwords.
- Do not supply your personally identifiable information to any person who is not permitted to have access to your accounts.
- Do not share your personally identifiable information over the telephone, through the mail or online unless you have initiated the contact or can verify the identity of the person or company to whom it is given.

Credit and Debit Cards

- Limit the number of credit and debit cards that you carry.
- Cancel all cards that you do not use.
- Keep all receipts from card transactions to compare to your statement.
- Sign and activate new cards as soon as you receive them.
- Report lost or stolen cards immediately.
- Beware of your surroundings when using your cards at ATMs and public establishments.

Mail

- Promptly remove your mail from the mailbox. If you will be away from home for an extended period of time, have the post office hold your mail until you return.
- Deposit all your outgoing mail in a post office collection box, hand it to a postal carrier, or take it to a post office instead of leaving it in your doorway or home mailbox where it can be stolen.

Credit Reports

- Under a federal law enacted by Congress, consumers in the United States are entitled to obtain one free credit report every 12 months from each of the three major credit bureaus (Equifax, Experian or TransUnion). It is advised to order a copy of your credit report annually and review it for accuracy. You can obtain your free credit reports by mail, by phone or online from a service that is run jointly by the three credit bureaus. If you order your credit report online, you must print it or save it to your computer, or it will be unavailable once you leave the screen. The free program applies only to the credit report itself. Credit scores are not included in the free credit report, but they can be purchased from the credit bureaus for a fee. Obtain your free credit report:
- Online at **www.AnnualCreditReport.com**
- By phone: 1-877-322-8228

- By mail:
  Credit Report Request Service
  P.O. Box 105281
  Atlanta, GA 30348-5281
- Check your credit report for accuracy and for any unauthorized bank accounts, credit cards and purchases. If you detect that something is wrong on the report, you can dispute it directly with the credit bureau. Credit bureaus have 45 days to respond when a dispute is filed.
- Look for anything suspicious in the section of your credit report that lists who has received a copy of your credit history.

Bank Account and Credit Card Statements

- Avoid lost or stolen statements in the mail by registering for e-Statements from CNB or your credit card company.
- Contact customer service immediately if a bank account statement does not arrive on time.
- Review your bank account and credit card statements promptly and immediately report any discrepancy or unauthorized transaction.
- Between statements, periodically review your CNB account activity through either Online or Mobile Banking.

Telephone and Internet Solicitations

- Be suspicious of any offer made by telephone, on a website or in an email that seems too good to be true.
- Before responding to a telephone or Internet offer, determine if the person or business making the offer is legitimate.
- Do not respond to an unsolicited email that promises some benefit, but requests personally identifiable information.
- Community Neighbor Bank never requests your bank card number, account number, Social Security number, Personal Identification Number (PIN) or password through email or text. If you should receive an email or text requesting such information that appears to be from CNB, do not respond to the email or text and contact us immediately at 1-800-805-9821.

Home Security

- Store extra checks, credit and debit cards, documents that list your Social Security number and similar items in a safe place.
- Shred all credit card receipts and solicitations, ATM receipts, bank account and credit card statements, canceled checks and other financial documents before you throw them away.

PINs and Passwords

- Avoid selecting PINs and passwords that will be easy for others to guess. “Strong” passwords that contain a combination of upper and lower case letters, numbers and special characters should be used when possible.
- Memorize your PINs and passwords and keep them confidential.
- Change your passwords periodically.

- Avoid using the same passwords on multiple websites.
- Do not carry PINs and passwords in your wallet or purse or keep them near your checkbook, credit cards, debit cards or ATM cards.

Wallets and Purses

- Do not carry more checks, credit cards, debit cards, ATM cards and other bank items in your wallet or purse than you really expect to need.
- Do not carry your Social Security number in your wallet or purse.

ATMs and Payment Terminals

- Do not use ATMs, in-store payment terminals, or unmanned payment terminals (e.g., vending machines, air pumps, parking meters, etc.) that appear to have been altered or are physically different from what you remembered or expected. Report any oddities to the owning store or financial institution immediately.
- As mobile and tablet payment options become more commonplace, be cautious when using these channels to make purchases from unfamiliar merchants.
- When visiting a location with multiple ATMs, and one machine has an "Out of Order" sign on it, do not use any of the ATMs at that location. Fraudsters and members of professional criminal organizations use this technique to drive card activity to the machine they may have compromised. ATMs that are legitimately out of service will usually have a graphic saying so right on the ATM screen.
- When using an ATM or any other unmanned payment terminal, use only machines from reputable banks or companies in reputable locations.
- Even if your transaction is completed normally, if something seems suspicious, it probably is! Use your best judgment.

Online and Mobile Purchases

- Only shop with reputable companies.
- Ask yourself, "Is it necessary for the company to request that information?"
- Before providing personal or financial information, check the website's privacy policy.
- Look for signs that the site is secure. This includes a closed padlock on your Web browser's address bar or a URL address that begins with "https." This indicates that the purchase is encrypted or secured.
- Never use unsecured wireless networks to make an online purchase.

Miscellaneous

- Use common sense and be suspicious when things do not seem right.
- Be suspicious of any proposed transaction that requires you to send an advance payment or deposit by wire transfer.
- Be cautious when using online services and mobile apps. Only download the CNB mobile app from trusted sources, such as the App Store℠ for Apple® mobile digital devices or the Google Play™ store for Android™ mobile digital devices.
- Be aware of common tactics used by fraudsters and identity thieves. Call CNB immediately at 1-800-805-9821 if you believe that you are a victim of identity theft involving one of your CNB accounts.