Protect Yourself

Citizens Independent Bank values our customers' security and privacy. Our customers have the ability to interact with CIB in a variety of ways online including via our website, mobile site, online banking system, and mobile app. We have extensive security features and procedures in place to protect your information. It is also important that customers take steps to help ensure the safety of their information online. The following information will help you to protect your information when interacting with CIB online and with other websites.

Security Guidelines

While we maintain a high level of security on our systems, we are not responsible for any breach of security that is beyond our control. The information below includes steps and precautions you can take to help keep your confidential information safe.

Online Banking

- Do not share your login information with anyone else. If you think your information has been compromised, change your password immediately online and call us at 952-915-8525.
- Choose a hard to guess password by using random letters, numbers, and symbols. Do not use words that can be found in a dictionary or information related to you such as your name, address, birth date, etc. Use a unique password for each of your important accounts – do not use the same password for all of your online log-ins.
- Enable "Password Help" by logging into Online Banking then selecting "Options - Personal".
- Disable any "AutoComplete" or similar features on any computer you use for online banking.
- Do not write down your password or reveal it to anyone, including bank employees.
- Remember to log out when you are finished banking online, or are leaving the computer unattended.
- Avoid using unfamiliar computers to conduct any online banking as they may be compromised. Also be wary when using a network you don't know or trust such as free Wi-Fi at the coffee shop.
- Do not send sensitive information via email to Citizens Independent Bank; instead, contact us through the secure Message Center available within Online Banking.

Computer Security

- Learn to use the built-in security features that are provided with your Internet browser instead of disabling them.
- Keep your system and applications current with updates from the vendor's website. For example, use Microsoft's Windows Update feature and install any Critical Updates and Service Packs that are available.
- Use virus and spyware protection software and keep it up-to-date in order to detect new threats.
- Use a software or hardware firewall to protect your computer from network intrusion.
- Make sure that any wireless network you connect your computer to is secured and requires encryption.
- Do not download files, install software, or open email attachments from unverified or unknown sources.

St. Louis Park
5000 West 36th Street
St. Louis Park, MN 55416
952-926-6561

Robbinsdale
3700 W. Broadway
Robbinsdale, MN 55422
763-588-2715

Hopkins
10901 Excelsior Blvd.
Hopkins, MN 55343
952-935-3333

Plymouth
15650 36th Ave. North
Plymouth, MN 55446
763-550-9191

Citizens Independent Bank

- Business owners should perform an annual review to evaluate their security systems, procedures, and employee access to confidential information.

Protect Your Confidential Information

- Shred financial documents and paperwork containing personal information before discarding them.
- Protect your Social Security numbers. Don't carry your Social Security card in your wallet or write your number on a check. Give it out only if absolutely necessary.
- Keep your personal information in a secure place at home or in a safe deposit box.
- Sign up for e-Statements. By receiving your statements electronically, it prevents people from stealing statements from your mailbox and obtaining your account information.
- Utilize Bill Pay instead of sending checks through the mail which also reduces the chances that your financial information could be stolen.
- Sign up for direct deposit.

Security Features

Citizens Independent Bank employs the latest technology available to keep your online banking with us safe and sound. Our online banking services are routinely audited to ensure they comply with current banking regulations. While our Privacy Notice outlines the use, collection, and retention of client information, the following features help maximize the security of your online banking experience.

- All online banking data transmitted to us is encrypted, helping to make the data useless if intercepted. This secure connection is established before a User ID and Password can be transmitted.
- The login system utilizes multifactor authentication to ensure a secure connection.
- Account numbers are not visible through Online Banking. Instead, a "Pseudo Name" is used to represent each account.
- Password guessing (brute forcing) is prevented with an account lockout feature. Our systems will automatically lock a user out when an incorrect password is entered multiple consecutive times.
- Users are required to update their password periodically in order to minimize the risk of unauthorized access.
- The date of last access to the system is displayed after logging in so that users can verify that no one else has used their account.
- All Online Banking sessions have a time limit for inactivity, which will log a user out of the system in order to prevent someone else from accessing their information.

Reporting Fraud

Citizens Independent Bank does not solicit personal information by means of email or telephone. If you receive an unsolicited request for confidential information by phone or email from someone claiming to be an associate of the bank, do not respond to the message and please inform Citizens Independent Bank immediately by calling 952-915-8525.

St. Louis Park
5000 West 36th Street
St. Louis Park, MN 55416
952-926-6561

Robbinsdale
3700 W. Broadway
Robbinsdale, MN 55422
763-588-2715

Hopkins
10901 Excelsior Blvd.
Hopkins, MN 55343
952-935-3333

Plymouth
15650 36th Ave. North
Plymouth, MN 55446
763-550-9191

Citizens Independent Bank

Suspicious or Unauthorized Transactions on Your Account
Customer Service 952-915-8525

Lost or Stolen Debit Card, ATM Card, or Checks
Customer Service 952-915-8525
(M-F, 8:30am – 5pm CST)

800-535-8440 (Evenings and Weekends)

Lost or Stolen VISA® Credit Card or Suspicious Transactions
800-876-9119

Suspicious Activity with an Online Service
Customer Service 952-915-8525

Suspicious Email Received, but did not respond
Do not click on any links in the email and do not open any attachments. Immediately contact Customer Service at 952-915-8525 for further instructions.

Confidential Information Compromised
If you believe your confidential information has been compromised, such as by responding to a suspicious email or phone call and sharing your Social Security number, username, password, PIN, etc. please contact Customer Service at 952-915-8525.

Common Scams and Fraud

You can help protect yourself and your information by being aware of the ways fraud is committed.

Check Fraud

Usually, although not always, someone you don't know will approach or contact you with a request that involves cashing or depositing a check into your bank account. They will then ask you to use part of that money for what seems to be a legitimate purpose such as giving them a portion back in cash. The scammer is assuming that you think once the check is deposited, that it has cleared and cannot be returned or removed from your account. However, when you deposit a check the bank forwards that check to the originating institution. If the originating institution finds that the check is fraudulent, the check will be returned unpaid. The deposit will then be reversed from your account and you will be responsible for the full amount of the original check and any associated fees.

Sweepstake or Lottery Scams

You receive a letter, email, or phone call congratulating you on winning a sweepstakes or foreign lottery. In order to claim your prize check, you are asked to deposit the check and wire a portion to a foreign bank account to handle taxes, processing fees, or administrative fees. Sometimes you may be asked to send these fees before receiving your winnings. Similar to check fraud, the scammer is hoping to get their money before you realize that the prize check is fraudulent or that no prize is coming. A similar scam involves "winning" a government grant.

Service Scam

You receive a call from what appears to be a legitimate company such as your bank, cable company, or cell phone provider. They tell you there is a problem with your account and that they need to verify your information before the problem can be corrected. The caller may already know some of your personal information such as your name and address. They hope this will make you comfortable enough to share confidential information with them such as your account number, social security number, or birthday. You should never share confidential information on a service call that you did not initiate or request. Ask the caller what the problem is and then hang up. Call the company back using their

official service number as found on your statement or their website to confirm that the problem is legitimate and not a scam.

Phishing (fraudulent emails)

Scammers send emails that appear to be from a legitimate company. In the email, there are links to a fake website that imitates the company's actual website. The scammer is hoping to convince you to share your personal information by getting you to log into their fake website. The email will use persuasive language such as saying your account information has been breached and you need to log in and verify your confidential information. If you receive a suspicious email, do not open it or click on any links that it contains. Phishing can also occur via text message.

Citizens Independent Bank does not solicit personal information by means of email or telephone. If you receive an email or phone call requesting confidential information from someone claiming to represent Citizens Independent Bank, do not respond to the message. If you receive an unsolicited request for confidential information by phone or email from someone claiming to be an associate of the bank, please inform Citizens Independent Bank immediately by calling 952-915-8525.

Remember:

- If something sounds too good to be true, it probably is.
- Never deposit or cash a check for someone you don't know.
- You are liable for items you cash or deposit.
- Never be shy about asking for verification. Don't worry about offending someone, if they are legitimate they will be able to provide proper identification.
- If you are worried that a check you received may be fraudulent, bring it into the bank and ask a banker for help confirming it is genuine.
- Remember that a wire transfer is an immediate form of payment. If it is later discovered that the check was fraudulent, the wire cannot be reversed.
- Never give personal information to a stranger who contacts you by phone or email.

Gathering & Sharing Information

To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We collect your personal information, for example, when you:

- Open an account or apply for a loan
- Use your credit or debit card or make deposits or withdrawals from your account
- Give us your income information

We also collect your personal information from others, such as credit bureaus, affiliates or other companies. The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and income
- Account balances and payment history
- Credit history and transaction history

When you are no longer our customer, we continue to use your information as described in our Privacy Notice. We use this information for our everyday business purposes such as processing your transactions, account maintenance, responding to court orders or legal investigations and reporting to credit bureaus. This information is also used for

marketing purposes including joint marketing with other financial companies. All confidential information collected by Citizens Independent Bank may only be accessed by and disclosed to CIB employees and others with a legitimate business need in accordance with applicable laws and regulations. This information is also subject to physical, electronic, and procedural safeguards. CIB has established training programs to educate our employees about the importance of customer privacy and to help ensure compliance with our policy requirements. For complete details on how your information may be shared, please read our Privacy Notice.

Children's Privacy

The Children's Online Privacy Protection Act (COPPA) was passed to give parents increased control over what information is collected from their children online and how such information is used. The law applies to websites and services directed to, and which knowingly collect information from, children under the age of 13. Citizens Independent Bank's websites and online services are not directed to children under the age of 13, nor is information knowingly collected from them. For additional information on COPPA protections, visit the Federal Trade Commission's website: www.ftc.gov.

Your Rights & Responsibilities for Electronic Funds Transfers

Electronic funds transfers are electronic transfers of money to or from your deposit account. These transfers include, but are not limited to: online banking, bill pay, electronic check conversions, re-presented check transactions and fees, instant cash and check card, prearranged transfers, preauthorized loan payments, direct deposit, and TeleBANK. If you believe there is a mistake on your account statement, contact our customer service department as soon as possible. The bank must hear from you no later than 60 days after we sent you the first statement on which the error or problem appeared. We will determine whether an error occurred within 10 business days and will correct any error promptly. If necessary, however, we may take up to forty five days to investigate. If we decide to do this, we will credit your account within 10 days for the amount you believe is an error so that you will have use of the money while we investigate. If the error involves a point of sale debit card with the VISA logo, we will provide provisional credit within 5 business days.

For more information about your consumer rights under Regulation E and unauthorized electronic transactions please contact a banker at any location or Customer Service at 952-915-8525.

Additional Resources

Annual Credit Report
https://www.annualcreditreport.com

Consumer Protection Basics
http://www.consumer.gov/

Federal Bureau of Investigations
http://www.fbi.gov/scams-safety

Federal Trade Commission
http://www.ftc.gov

Social Security Administration
http://www.ssa.gov/