Meriwest Credit Union
Customer Awareness and Education

Meriwest Credit Union helps keep your personal and financial information protected.

The number of people who are victims of identity theft is on the increase as more consumers make use of electronic means to purchase products and pay debts. This increased use of electronic commerce has a coinciding increase in misuse, theft, and compromise of sensitive member information and loss of funds.

Fraudsters are utilizing increasingly sophisticated and malicious techniques to thwart existing authentication controls, gain control of accounts, and transfer funds. Fraudsters use various methods to steal the logon ID, password, and challenge question answers of financial institution customers. This information may enable fraudsters to access the customer's account and transfer funds to themselves through wire, ACH, and ATM or Debit card transactions.

At Meriwest Credit Union ("Meriwest"), keeping your personal and financial information secure is one of our most important responsibilities. You should feel safe knowing we will work with you to prevent fraud and identity theft. If something should happen, we will help you resolve it as quickly and easily as possible. In the event we should suspect or detect that unauthorized individuals gained access to your information and/or our information systems, we will react immediately to determine who has gained access, what information the intruder has, and the severity of the problem.

Please review these sections about protecting your accounts and information:

- **ACCOUNT SECURITY**
  Learn about our security features that protect your account(s), online banking, mobile banking, ATM cards, and Debit cards. Also, learn about ways you can enhance account and card security yourself.

- **PREVENTING/MITIGATING FRAUD AND IDENTITY THEFT**
  Get tips on safeguarding your account(s), computer, and personal and financial information. Take steps to stop fraud and identity theft before it happens.

- **DETECTING FRAUD**
  Learn fraud and identity theft signs and account monitoring resources.

- **REPORTING/RESOLVING FRAUD**
  Find out how to report fraud, what to do if you think your identity was stolen, how we monitor your account(s) and card(s), and what happens if a data compromise occurs.

- **FAQs - FREQUENTLY ASKED QUESTIONS**
  Get answers to some of your concerns.

Meriwest Credit Union
Customer Awareness and Education

Account Security

Tools and services that help protect your personal and financial information:

- **Meriwest Online Banking** - Sign up for free Meriwest Online Banking to securely view and perform account transactions, make bill payments, view eStatements, view eTax documents, set up account alerts, and more.

- **Meriwest Mobile Banking ("Mobile-Meriwest")** - Meriwest Online Banking and Bill Payer service can be accessed through the Mobile-Meriwest application ("app"). You can manage your accounts, transfer money, deposit checks, pay your bills, view graphs, locate ATMs, obtain a Quick Balance, set up fingerprint authentication, and more.

- **Meriwest eStatements** - Enroll in this free service available through Meriwest Online Banking to reduce your paper trail and eliminate the risk that your paper statement may be lost or stolen from the mail.

- **Meriwest eTax** - Receive your annual tax statements to reduce your paper trail and the possibility of mail fraud. This feature is available through Meriwest Online Banking eStatements by selecting the eTax tab.

- **View your cleared checks online** - View your cleared checks online to monitor for check fraud. The feature is available through Meriwest Online Banking eStatements.

- **Meriwest Bill Payer service** - Use our free Bill Payer service to pay and receive bills online to help reduce your paper trail and the possibility of mail fraud. You can set up bill reminders to track when your bills are due and/or paid. Bill Payer service is available through Meriwest Online Banking by selecting the Bill Pay tab.

- **Meriwest Account Alerts** - Receive information delivered by email or text to your cell phone about account activity by setting up balance, payment, transaction, account activity (deposits, withdrawals), and/or reminder alerts to help flag suspicious activity in your account(s). To set up Alerts, log in to Meriwest Online Banking, go to the **Account Management tab,** and select **Alerts**.

- **Meriwest Secure Message Center** - Send and receive account-related questions and answers securely and privately through a secure message service within Meriwest Online Banking.

- **Direct Deposit** - Have your funds such as payroll and government checks deposited directly in your account when you sign up for Direct Deposit.

- **Account Activity** - Check your account activity regularly through Meriwest Online Banking and Mobile-Meriwest to detect fraud earlier.

- **Review your account statement** - Review your statement when it is received to verify transactions. If you signed up for eStatements, you will receive an electronic notice when your eStatement is ready for viewing.

- **Meriwest ATM card and Debit card protection** - Receive ATM or Debit card protection through our network fraud detection system that monitors, manages, and mitigates card loss and fraud.

Key controls that Meriwest Online Banking utilizes to safeguard your information:

- **128-Bit Encryption** - When you access your account(s) and perform transactions using Meriwest Online Banking and Mobile-Meriwest, your information is protected by at least 128-bit encryption. Look for a "closed lock" icon  in your browser to determine if encryption is being used on any Web page you are viewing. The location of the “closed lock” may be different depending upon your browser type and version. Any Web address beginning with "https://" indicates the page you are viewing uses encryption. The "s" at the end of “http” stands for "secured."

- **Multi-Factor/Multi-Layer Authentication** - Meriwest Online Banking uses multiple authentication techniques when you access online banking services.

  - **Individualized Login ID** - When you sign up for online access as a new user, Meriwest Online Banking asks you to create a unique Login ID to access your account(s). This information is encrypted during each online banking session. Current online users have the option of creating a unique Login ID by selecting the Login ID option within Account Management.

  - **Individualized password** - When you sign up for online access, besides verifying your identity, Meriwest Online Banking asks you to create your own password to access your account(s). This information is encrypted during each online banking session. We strongly recommend that you do not use your Social Security number as a password. To create a secure password, please see Creating a Secure Password.

  - **Personal image and text** - In addition to your personal password, you will be asked to select a personal image and text. When logging in to future online banking sessions, you will be asked to verify your personal image and text **before** you enter your password.

  - **Additional authentication** - When you log in from a device with an IP address unknown to Meriwest Online Banking, or you perform sensitive online banking transactions, such as money transfers or changes to your account information, Meriwest Online Banking may ask you additional challenge questions to verify your identity.

- **Automatic lockout** - Your ability to log in to Meriwest Online Banking or Mobile-Meriwest will be disabled after several unsuccessful attempts to enter your password.

- **Extended Validation (“EV”) SSL Certificate** - The green address bar on Meriwest Online Banking is a security feature supported by newer browsers that allows you to validate visually that the website you are transacting with is a secure website.

- **Secure firewalls** - The banking servers that run all Meriwest website services are protected by numerous security devices including firewalls, intrusion detection and prevention, and log monitoring, to name a few, to help prevent unauthorized access to our network and prevent security breaches. Connections to the servers will be blocked from IP addresses known or suspected to be associated with fraudulent activities.

- **Session timeouts** - If you are logged in and not using Meriwest Online Banking or Mobile-Meriwest for several minutes, your session will "time out." To resume your banking activity, you will need to re-enter your User ID and Password and verify your personal image and text.

Protections offered relative to electronic fund transfers and the applicability to accounts with Internet access:

Your Meriwest account(s) and funds are protected as stated in our Electronic Fund Transfers Disclosure and Agreement. Electronic Fund Transfers ("EFTs") are electronically initiated transfers of money involving a deposit account at Meriwest and multiple access options, such as online account access, direct deposits, Automated Teller Machines ("ATMs"), and MasterCard® Debit Card.

Business Banking risk management notice:

Risk management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity, or availability of your account. As an additional measure to protect your business account, we suggest you perform a risk assessment and controls evaluation periodically. A risk assessment will help you identify where you should have controls to protect your account and if controls in place are adequate.

Business Banking corporate account takeover:

- **What is Corporate Account Takeover?**

  Corporate account takeover is a type of fraud where thieves gain access to a business' finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable. Corporate account takeover is a growing threat for small businesses. Cyber thieves target employees through phishing, phone calls, and even social networks. It is common for thieves to send emails posing as a financial institution, delivery company, court, or the Better Business Bureau. Once the email is opened, malware is loaded on the computer, which then records login credentials and passcodes and reports them back to the criminals.

- **Employee Education is Essential**

  Employee education of small business employees is effective in reducing the threat of account takeover.

- **How do you protect yourself and your small business?**

  The best way to protect against corporate account takeover is a strong partnership with your financial institution to understand security measures needed within the business and to establish safeguards on the accounts that can help the financial institution identify and prevent unauthorized access to your funds.

  Consider these tips to ensure your business is well prepared:

  - **Educate your employees.** You and your employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

  - **Protect your online environment.** It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically.

  - **Partner with your financial institution to prevent unauthorized transactions.** Talk to your financial institution about programs that safeguard you from unauthorized transactions. Some services offer callbacks, device authentication, multi-person approval processes and batch limits help protect you from fraud.

  - **Pay attention to suspicious activity and react quickly.** Look out for unexplained account or network activity, pop ups, and suspicious emails. If detected, immediately contact your financial institution, stop all online activity, and remove any systems that may have been compromised. Keep records of what happened.

  - **Understand your responsibilities and liabilities.** The account agreement with your financial institution will detail what commercially reasonable security measures are required in your business. It is critical that you understand and implement the security safeguards in the agreement. If you do not, you could be liable for losses resulting from a takeover. Talk to your financial institution if you have any questions about your responsibilities.

Online services security safeguards:

- **Firewall Protection**

  We use a protection mechanism on our website and online services known as a firewall to protect our computer systems and your information. Firewall is a general term for a device that is used to prevent unauthorized access to or from a private network. When you pass through the firewall, your IP (Internet Protocol) address is stored for security and tracking purposes. This IP address does not personally identify you, but allows communications on the Internet to be performed in a uniform and organized manner. The firewall uses the IP address to ensure our website and online services are only accessed from valid sources.

- **Secured and Unsecured Sites**

  Encryption transforms data into an unreadable format. A *secured site* is one that uses at least 128-bit encryption and Secure Sockets Layer ("SSL") technology to transmit information between you and Meriwest. SSL ensures information remains confidential. Encrypted, or scrambled, information effectively prevents anyone from intercepting and reading any information about you. *Please note that this encryption takes place only when you use your web browser from a secured site.*

  An *unsecured site* does not utilize SSL technology or encryption. Information sent to or received from an unsecured site can potentially be intercepted by anyone. When sending email, you should not include personal information if you are sending it from an unsecured site.

- **Internet Web Browsers**

  An Internet browser allows access and the ability to navigate information and service resources on the Internet. Most computers come with a browser already installed. Always update your browser when new versions are released since the updates often include new security features. Prior to upgrading, verify that the most recent version has been reviewed and is supported by Meriwest. To protect your information and take full advantage of Secure Sockets Layer ("SSL") technology, we recommend that you use a secure browser with at least a strong 128-bit encryption technology such as Microsoft Internet Explorer®, Mozilla Firefox®, and Safari®. You can download these browsers directly from the Internet. Because of security settings on most browsers, pop-ups may be blocked. Certain sites related to online banking, particularly Bill Payer service, eStatements, and Mortgage account access require the function of opening a new window or tab within the online banking session. It is recommended that the following sites be marked as "trusted" or "allowed" secure sites:

  - Bill Payer: https://billpay1.pscufs.com
  - eStatements: https://meriweststatements.meriwest.com

- **Meriwest Website**

  Our Meriwest website site is a *secured site* for all online services and for Live Chat with a Meriwest representative. It is an *unsecured site* for email.

  When you visit our website to view any pages, read product information, or use our online calculators and tools, you do so without telling us who you are and without revealing any information. While we do not collect identifying information about visitors to our website, we do offer the ability to provide contact information on our calculators as a member initiated option. We use standard software to collect information for the strict purpose of tracking activity on our website. This allows us to get a better understanding of how many people use our website and which pages and features are most popular.

  Our website is not targeted or marketed to children. Please see the section "Children's Online Information Privacy" below.

- **Meriwest Online Banking, eStatements, Bill Payer, and eTax Forms**

  Our Meriwest Online Banking site is a *secured site*.

  eStatements (account statements), Bill Payer service, eTax forms, and Meriwest Mortgage Account status are accessed through Meriwest Online Banking. Access to your account information using Meriwest Online Banking is protected using multi-layered authentication during the sign-in process. Authentication consists of your account number or Login ID, a personal identification number ("PIN"), and a picture selected by you. To protect you further, a timeout feature is used. This feature will automatically sign you out of Meriwest Online Banking after an extended period of inactivity. Additionally, there is an automatic lockout feature that will disable your ability to log into Meriwest Online after several unsuccessful attempts to enter your password. If you are locked out, you must contact Meriwest to restore your access.

  We recommend that you complete your online transactions and Logoff (Sign off the Secure Site) before going to other sites or turning off your personal computer. We also suggest that you do not go to other sites during your online banking session. Failure to Logoff could endanger the security of your information by potentially allowing others using the same computer to access information saved or cached in the memory of the browser.

- **Mobile Banking ("Mobile-Meriwest")**

  The Mobile-Meriwest site is a *secured site.*

  Meriwest Online Banking and Bill Payer service can be accessed through Mobile-Meriwest. Access to account information using Mobile-Meriwest is protected using multi-layered authentication during the sign-in process. Authentication consists of your account number/Login ID, a password, and your associated/established device. To protect you further, a timeout feature is used. This feature will automatically sign you out of Mobile-Meriwest after an extended period of inactivity. Mobile-Meriwest will also log you out of the current session if you attempt to use another mobile application while your mobile banking session is active. Additionally, there is an automatic lockout feature that will disable your ability to log into Meriwest Online after several unsuccessful attempts to enter your password. If you are locked out, you must contact Meriwest to restore your access.

  We recommend that you complete your online transactions and Sign Off before going to other sites, using other applications, or turning over access to your device. We also suggest that you do not go to other sites during your mobile banking session. Failure to Sign Off could endanger the security of sensitive information by potentially allowing others using the same access device to access information saved or cached in the memory of the browser or mobile device.

Meriwest Credit Union
Customer Awareness and Education

- **Loan Applications and Membership Applications**

  Our Loan Application and Membership Application features are on a *secured site.*

  To protect you when entering application information, a timeout feature is used. This feature will automatically sign you out of the application feature after an extended period of inactivity.

  We recommend that you complete your application session before going to other sites. We also suggest that you do not go to other sites during your application session. Failure to complete the application session could endanger the security of your information by potentially allowing others using the same computer to access information saved or cached in the memory of the browser.

- **Email**

  Our Meriwest website is an *unsecured site* for email. Our Meriwest Online Banking site is a *secured site* for Secured Messages ("email").

  There are instances where you may send us an email for a request and elect to provide us with information such as your name, mailing address, and/or email address. Sending information is always your option and this information cannot be collected unless you specifically elect to send it to us. This information is used internally only for fulfilling the request or for contacting you directly and is not given or sold to any other organization.

  We ask that you do not send confidential information such as social security or account numbers to us via an unsecured email. Such communications should be sent to us via the online banking secure mailbox, postal mail, or you may call us or visit one of our financial centers.

  If we respond to you via email, we will not include any of your personal information unless we send the email through our secured site.

- **Online Surveys and Drawings**

  We may conduct online surveys and drawings. Your survey responses will improve our understanding about your needs so that we can improve the products and services that we offer. If you complete a survey, you are transmitting the information that appears to you in the survey. You never transmit information that you do not enter yourself. All information in the survey is used for internal purposes only. We may conduct a drawing in association with a survey or a promotion. If we do, we will ask for your name and contact information (such as your telephone number or email address) so that we can notify you if you are a winner. Participation in surveys or drawings is always voluntary.

- **Aggregation Sites**

  Aggregation websites are Internet websites that allow you to consolidate account information from several sources on one site. To do this, an aggregation provider may request access to your information. You should ensure that the aggregator company has appropriate policies to protect the privacy and security of any information you provide or to which they are gaining access, and that you trust the aggregator company.

  If you provide information about your Meriwest accounts to an aggregator company, we will consider that you have authorized all transactions initiated by an aggregation site using access information you provide, whether or not you were aware of a specific transaction. Meriwest does not guarantee the operation, compatibility, or security of aggregator sites that you choose to utilize.

Links to information about protecting your accounts and information:

Basics of Phishing
Creating a Secure Password
Electronic Fund Transfers Disclosure and Agreement
Equifax - Report Fraud
Experian - Report Fraud
TransUnion - Report Fraud
Federal Trade Commission – Consumer Information
Federal Trade Commission – ID Theft Information
Federal Trade Commission - Report ID Theft
Free Annual Credit Report
Online Banking FAQs
Online Banking Security

Preventing/Mitigating Fraud and Identity Theft

Glossary of key terms:

- **Data Compromise** - An organized theft of ATM/Debit/Credit card information primarily from merchants through merchant data breaches, merchant third-party processors, computer theft, stolen storage tapes, ATM or other electronic skimming devices, or company insiders working for a merchant or merchant's contractor. Similar terms include card compromise and mass compromise.

- **Identity Theft** - Fraud committed using the identifying information of another person without permission where an account has been compromised and a new banking relationship has been established, enhancements or changes have been made to an existing banking relationship, or when any occurrence of account takeover has taken place.

- **Privacy Event/Breach** - A privacy event involves a situation where sensitive information that is controlled by Meriwest (or a third party acting on our behalf) is lost, misused (including inappropriately accessed), or disclosed to an unauthorized third party. The information may be in any form, including paper, electronic, and encrypted data.

How can you be sure that you are dealing with Meriwest and not an imposter?

A Meriwest employee will never call you or send you an email asking for your passwords, ATM or Debit card numbers, or other sensitive information. However, if you contact us, we may ask for personal identification and verifying information to ensure we are speaking to the correct accountholder.

General practices to protect your information and prevent ID theft:

Please do not hesitate to call us if you have any questions – we are here to help you!

- **Protect your personal credentials** (e.g., account number, Social Security number, ATM/Debit/Credit card numbers, PIN, password, access numbers, other personal information, etc.).

  Never divulge this kind of information unless you initiate the contact with a person or a company you know and trust.

  Do not provide personal or ATM/Debit/Credit card information on the telephone unless you initiated the call. If someone calls you, explains the call is on behalf of Meriwest, and asks for your account number, you should beware. Official Meriwest staff will have access to your information and will not need to ask for it.

  Do not write your personal information in a place where others can view it.

  Never keep your PIN, passcode, or password with your ATM/Debit/Credit cards. Doing so could allow access to your accounts if your card is lost or stolen.

  Use your own computer to access any online service where you are required to enter your user name and a password or use your Debit/Credit card. Other computers may have programs installed on them that capture your information. Be careful if you are using your computer on an unsecured wireless network, especially if you are in a public area.

- **Use a strong password and change it regularly**

- **Limit the information you carry**

  Do not carry more checks, credit cards, or other banking items than you expect to need. Do not carry your Social Security number in your wallet or have it preprinted on your checks. Choose passwords and Personal Identification Numbers (“PINs”) that will be hard for someone else to figure out – do not use your birth date, anniversary date, or home address, for example. Do not keep this information on or near your checkbook, ATM/Debit/Credit card.

Meriwest Credit Union
Customer Awareness and Education

- **Protect your mail**

  Promptly remove mail from your mailbox after it has been delivered. If you are going to be away, have your mail held at your local post office or ask someone you know and trust to collect your mail. Deposit sensitive outgoing mail in one of the Postal Services' collection boxes, hand it to a mail carrier, or take it to a post office instead of leaving it in your home mailbox.

- **Keep information secure in your home**

  Safely store extra checks and credit cards, documents that list your account information, and similar valuable items.

  Destroy pre-approved credit offers, receipts, and other information that could link your name to your account numbers. "Dumpster divers" pick through garbage looking for financial information.

- **Protect information on your personal computer/laptop**

  Use virus-checking (anti-virus) software on your computer and update it frequently. Some viruses known as Trojan Horses can capture important information stored on your computer such as passwords or documents and send them to someone else. For further protection, do not open emails from unknown sources.

  Never click on an email attachment if you do not know the person who sent it to you.

  Never click inside an email to visit a website. Type the address into your browser instead.

  Remember to Exit or Log Off when you have completed any online session.

- **Pay attention to your account statements and credit card bills**

  Review your account statements and follow the procedures to report errors. Contact your financial institution immediately if there is a discrepancy in your records of if you notice something suspicious, such as a missing payment or an unauthorized withdrawal. Also, contact your financial institution if a statement or bill does not arrive on time. It could be a sign someone has stolen account information and changed your mailing address.

- **Review your credit report once a year**

  Your credit report from a credit reporting agency will include identifying information such as your name, address, Social Security number, and birth date as well as details about credit cards and loans in your name. Make sure the report is accurate, including monitoring it for unauthorized bank accounts, credit cards, and purchases. Free annual credit reports may be obtained from Free Annual Credit Report.

- **Update your information and keep it current**

  Keep your information with us and other financial institutions current. It is important that we have current information on how to reach you. If we detect potentially fraudulent or unauthorized activity or use of an account, we will attempt to contact you immediately. If your address, telephone number, or email address changes, please let us know.

Secure your computer:

Protect your personal computers from hackers, viruses, and malicious programs.

- Install updated anti-spyware and anti-virus protection to help detect and remove viruses and spyware, which can steal vital information.

- Use a firewall when possible to help prevent unauthorized users from gaining access to your computer, or from monitoring transfers of information to and from your computer.

- Install operating system and software updates, sometimes called "patches" or "service packs," as soon as possible.

- Keep your Web browser current by installing updated versions, which are deployed with your security in mind. Verify that the version you are installing is supported by Meriwest prior to installing.

- Protect against malware by installing updated scanner software. Malware, short for "malicious software," includes viruses, spyware, and Trojans that are designed to infiltrate or damage a computer system. Malware is often used to steal personal and financial information and commit fraud. Be cautious when opening files and clicking on hyperlinks because you could expose your computer system to a virus that could hijack personal information, including login credentials.

  There are several easy ways to minimize the risk of malware:

  - Downloads from file sharing and social networking websites can be distribution points for malware. Never download any file or software from websites, unknown sources, or people you do not know and trust.

  - Attachments and free software from unknown sources should not be opened or installed.

  - Never click on hyperlinks from unknown sources or people you do not know and trust.

  - Never access a non-trusted website when you are logged into an online banking session; ensure that ALL windows are closed when exiting your online banking session.

  - Pop-up advertisements asking for personal or financial information are likely fraudulent, so it is better to close them.

- Updated security and system software can help protect your computer from malware threats.

Protect yourself when accessing Meriwest Online Banking:

- Always look for your personal image and text before entering your password when you log in to Meriwest Online Banking.
- Make sure you are at the Meriwest website when you log in to Meriwest Online Banking. Always look for the https:// in your browser. The "s" at the end of "http" indicates this is a secure browser website. If you are using a newer browser, it will also turn your address bar green.
- If you receive a suspicious email, do not click on any links or reply to it. Simply delete it.

To report a suspicious email that uses Meriwest's name, you can forward it to us at contact_center@meriwest.com. Please see Online Banking FAQs for additional information.

Protect against online fraud:

- **Monitor and review account activity**
  - Regularly monitor your Meriwest account(s) and ATM or Debit card activity to help detect if you have been a victim of fraud.
  - Review your statement as soon as possible after it is delivered, or available through eStatements, and immediately report any unauthorized transactions. For quicker and more secure access, consider subscribing to free eStatements to review your Meriwest account(s) securely.
  - Frequently review your account activity online to quickly detect fraud and identity theft earlier than if you receive paper statements in the mail. Receiving electronic statements can also reduce your risk of mail fraud.
  - For added protection, you can set up free Meriwest Online Banking Alerts to notify you about important activity in your account(s), which can help identify fraud quickly. To set up Alerts, log in to Meriwest Online Banking, go to the **Account Management tab,** and select **Alerts**.
- **Eliminate paper**
  - Reduce the amount of mail and paper with your personal information printed on it to reduce the chance of criminals stealing it. Subscribe to eStatements, electronic notices, and electronic bill payment.
  - Stop receiving paper account statements. View and download them online instead. Sign up for our free Meriwest Online Banking, eStatements, and eTax.
  - Sign up for Direct Deposit to have your funds deposited directly in your account without paper checks.

- **Safeguard your Social Security number**

  - Never provide your Social Security number to anyone unless you have initiated the contact and have confirmed the business or person's identity.

  - Do not use your full or partial Social Security number as a Personal Identification Number ("PIN") or a password.

  - If you must provide your Social Security number in an email or on a website, ensure that it is encrypted, and you know how the recipient will protect it.

  - Do not record your Social Security number on checks, Traveler's Cheques, gift certificates, etc., unless required by law.

  - Do not carry your Social Security card and be cautious of your surroundings when disclosing your Social Security number.

- **Protect against phishing, vishing, and spoofing**

  Phishing, vishing, and spoofing are all methods used to obtain your personal and financial information fraudulently. The form may be in an email, a text message, or a phone call. For example, a criminal may send you an email or text message that looks like it has come from Meriwest. The phony message may ask you to go to a website that also looks like the Meriwest website and provide your personal information, but the website is a fake. The Meriwest website will always show as a secure website. The message may even ask you to call a phone number and provide account information. Another example would be a call to you from an automated recording saying that your account has experienced unusual activity. The message instructs you to call the same phone number shown in the spoofed caller ID and give your information.

  To manage and mitigate card loss and fraud, we use a network fraud detection system for ATM and Debit card monitoring. If you receive a call or message from our fraud detection vendor and are in doubt about any message received, do not provide any information. Instead, contact us at 877-MERIWEST (877-637-4937) to verify the validity of the message. Please see Basics of Phishing for additional information.

- **Be aware of the following methods that may be used to obtain your information**

  - Being asked for personal or financial information via email is a red flag. We will never ask you to reply to an email or call a number with any personal or financial information, such as your Social Security number, account number, ATM or Debit card PIN, etc.

  - Urgent appeals claiming that your account may be closed if you fail to confirm, verify, or authenticate your personal or financial information. We will not ask you to verify personal or financial information in this way.

- Messages about system and security updates claiming that Meriwest needs to confirm important information due to upgrades and stating that you must update your information online. We will not ask you to verify information in this way.

- Offers that sound too good to be true often are. You may be asked to fill out a short customer service survey in exchange for money being credited to your account, and you are then asked to provide your account number for proper routing of the supposed credit. Although we do conduct surveys and award prizes, we will not request your information in this way.

- Typographical and other errors are often the mark of fraudulent emails or websites. Be on the lookout for typos or grammatical errors, awkward writing, and poor visual design.

Protect against mobile banking fraud:

- **Fake mobile banking applications ("apps")**

  Criminals may develop and publish fake mobile banking applications ("apps") attempting to steal your Meriwest Online Banking credentials. To help protect your account(s) and information, do not download or install a Mobile-Meriwest app if you spot any of these warning signs:

  - The developer or author of the application is not from Meriwest or one of our trusted vendors. You can call us to confirm if you have doubts.

  - The application is being promoted on a third-party website, somewhere other than the official application store for your mobile device.

  - There is a charge for downloading the application. We do not currently charge for mobile application downloads.

- **SMS smishing**

  Smishing is phishing that happens via SMS text message. A criminal sends a text message tricking you into replying with personal or financial information or clicking on links that will sneak viruses onto your mobile device. To guard against these scams:

  - Do not respond to a text message that requests personal or financial information. We will never ask you to respond in this way.

  - Verify the phone numbers that appear in a text message. Store all Meriwest phone numbers in your mobile contacts for a quick crosscheck or you can go to our website Contact Us page.

- **Stolen devices**

  Mobile phones and tablets offer convenience, but they are also easy to lose or steal, which can put your information at risk.

  - Password-protect your device so it cannot be accessed unless the password is entered.
  - Enable an automatic screen-locking mechanism to lock the device when it is not actively being used.
  - Consider using a remote wipe program. This will give you the ability to send a command to your device that will delete any data as well as help you locate the device.
  - Keep a record of the device's make, model, and serial number in case it is stolen.
  - If you use the Mobile-Meriwest application, contact us so that we can disable the application on your device.

- **Viruses, malware, and other programs**

  Viruses, malware, and other programs that steal your personal or financial information are also able to infect some mobile devices.

  - Some tablets may support traditional anti-virus products. Consider installing one supported by your device.
  - Back-up the device's data. This will allow you to restore the data if you need to wipe the memory to remove a harmful software threat.

Online access and mobile device security tips:

- **Secure your login credentials** - Secure all your login credentials (account numbers, access numbers, Login ID, User Name, Password, Passcode, PIN, etc.) to protect your personal and financial information:
  - Do not disclose your login credentials to anyone.
  - Do not store login credentials on your devices (e.g., computer, smartphone, etc.).
  - Be cautious about the websites you visit and the information you release.
  - Secure your online access and mobile device(s) by using strong Passwords:
    - Avoid using easy-to-guess passwords such as names or birthdays
    - Use between 6 and 20 characters - include at least one number and one symbol
    - Intersperse capitals with lower case letters
    - Change your password at least every 90 days
    - Make sure you can remember it
  - Regularly change your Password/PIN.

- **Protect your online access** - Use your own computer to access any online service where you are required to enter your user name and a password, or use your Debit/Credit card. Other computers may have programs installed on them that capture your information. Be careful if you are using your computer on an unsecured wireless network; especially if you are in a public area (please see the next tip).

- **Be cautious when using public wireless networks ("Wi-Fi")** - Do not use public Wi-Fi to initiate online banking transactions. Public Wi-Fi connections are not secure and your login credentials could be compromised. When initiating an online banking session from a mobile phone, ensure that your connection is at a least "3G" or higher as anything less (e.g., 2G) is not secure.

- **Think before you app** - Before you download applications ("app") on your computer and mobile devices, review the privacy policy and understand what data an app can access. Only download applications from a trusted source.

- **Protect your money** - When banking and shopping online or on your mobile device, check to be sure the websites are security enabled. Look for Web addresses with https://, which means the website takes extra measures to help secure your information.

- **Synchronize mobile devices** - Essentially, mobile devices are small computers with software that needs to be kept up to date, just like a PC or laptop. Make sure all your mobile devices have the latest security protections. This may require synching your devices with a computer. If using the Mobile-Meriwest application, be sure you are running the current version. The version can be verified by viewing the "About" option within the application. Visit the app store or contact Meriwest if you need to verify the current version.

- **When in doubt, do not respond** - Fraudulent texting, calling, and voicemails are on the rise. Just like email, requests for personal or financial information or a call for immediate action, are usually a scam.

Protect against ATM and Debit card fraud:

- **Sign your card immediately** - Sign the signature panel on the back of your ATM or Debit card as soon as you receive it.

- **Eliminate paper statements** - Enroll in our free eStatements available through Meriwest Online Banking rather than receive paper statements by mail.

- **Check your receipts** - Check your receipts against your account statement to verify your transactions. Report any unauthorized transactions immediately. Once you have reconciled your account statement, shred all receipts, and discard them at home.

- **Check your statement** - View your account statement to verify your transactions. Report any unauthorized transactions immediately.

- **Keep a list of all your card numbers** - Keep a list of your card numbers as well as of telephone numbers to call if your cards are ever lost or stolen. Make sure they are in a separate, secure place.

- **Be cautious** - When giving out your ATM or Debit card number, know who you are giving it to and why. Never provide account information to anyone who called you.

Use ATMs safely:

- **Use ATMs with surveillance cameras** - Meriwest ATMs may be monitored by surveillance cameras, which record activity in the area of the ATM.

- **Be aware of people and your surroundings, especially at night** - Look for well-lighted ATMs when transacting business at night, do not use the ATM if you notice anything suspicious, never give information to strangers at the ATM, never accept help from anyone at an ATM, and consider having a friend or family member accompany you to the ATM.

- **Put away your card and cash** - After completing your transaction, secure your card and cash immediately before exiting the ATM area. Count your cash later, in the safety of your locked car or home. Your ATM or Debit card is like cash, so keep it in a safe place.

- **Protect your privacy** - Keep your Personal Identification Number ("PIN") a secret, have your ATM or Debit card ready, stand close to the ATM and away from others in line, and shield the ATM keypad with your hand or body while entering your PIN.

- **Be aware of ATM skimming devices** - An ATM skimmer is a device attached to an ATM machine, or a fraudulent ATM machine altogether, used to illegally collect data from the magnetic stripe of your ATM or Debit card. The information, once copied, can be used by identity thieves to make purchases or withdraw cash from your account. These camouflaged devices have been installed on bank ATM machines, gas station payment machines, cash withdrawal machines, etc. at public venues. There have even been cases where thieves who are employees of restaurants and other businesses have used pocket-skimming devices behind the counter.

  Tips on how to protect yourself from ATM skimming:

  - Look for changes to the ATM machine such as an odd protrusion or off-color component on the ATM
  - Cover the keypad as you enter your PIN
  - If something looks suspicious, find another ATM
  - If a machine retains your card, report it to your financial institution immediately
  - Monitor your statements and immediately report any signs of fraud

Stay current:

Check trusted websites for the latest information related to online safety. Share the information with friends, family, and colleagues and encourage them to be Web wise.

Please see the "Links to information about protecting your accounts information" section for helpful information about protecting your accounts and information.

Meriwest Credit Union
Customer Awareness and Education

Detecting Fraud

Fraud and identity theft signs:

It is important to learn how to recognize suspicious activities that may indicate possible fraud or identity theft.

Fraud is an act that occurs when someone uses your account to make unauthorized purchases or fund transfers. It frequently happens when your account number or card was stolen.

The following may be signs of fraud:

- If you did not receive an expected bill or statement by mail
- If you receive a bill from an unknown payee/vendor/merchant
- If unexpected charges occurred on your account
- If there are charges on your account from unrecognized vendors
- If posted checks appear on your account significantly out of sequence. Please note that check images available through the eStatement module will be presented in the order that they are cleared/posted. This can be matched to your transactions within online banking.

Identity theft happens when a thief steals information such as your name, birth date, or Social Security number to open ATM/ Debit/Credit cards, loans, mortgages, and other accounts without your knowledge.

The following may be signs of identity theft:

- If you find new accounts on your credit report that are not yours
- If you receive ATM/Debit/Credit cards that you did not apply for
- If you are denied credit or are offered less than favorable credit terms for no reason
- If you get calls from creditors or debt collectors regarding merchandise or services that you did not buy

Monitoring Resources:

- **Free annual credit reports** - By monitoring your credit report, you can make sure that no one has opened bank accounts or applied and been approved for credit in your name using stolen information. Nationwide consumer reporting companies will provide you with a free copy of your credit report once every 12 months by visiting Free Annual Credit Report or by calling 877-322-8228.

- Get an explanation of your rights online from the Federal Trade Commission – ID Theft Information website. The Federal Trade Commission is the nation's consumer protection agency.

Meriwest Credit Union
Customer Awareness and Education

Reporting/Resolving Fraud

If you have been the victim of fraud or identity theft, use the contact information below to report:

- Lost or stolen ATM card, Debit card, or checkbook
- Suspicious email or phone calls
- Fraudulent or suspicious activity on your Meriwest account(s).

Immediately report a lost or stolen checkbook or fraudulent or suspicious activity on your Meriwest account(s) during business hours:

- Call us at: 877-MERIWEST (877-637-4937);
- Outside the U.S., call us at: (408) 363-3200;
- Contact your nearest Meriwest Financial Center; or
- Contact us at: contact_center@meriwest.com

If your checkbook is lost or stolen, provide the check number of the last check that was written or the name of the person or business to which it was written. If you subscribe to eStatements, digital copies of your checks are available through free Meriwest Online Banking eStatements.

Immediately report a lost or stolen ATM Card or MasterCard® Debit card 24 hours a day, 7 days a week:

- Call 800-682-6075;
- Outside the U.S., call (Collect) 206-352-3482; or
- Visit www.reportmycards.com

To Dispute a Card Transaction on your ATM Card or MasterCard® Debit card during business hours:

- Call us at: 877-MERIWEST (877-637-4937);
- Outside the U.S., call us at: (408) 363-3200;
- Contact your nearest Meriwest Financial Center; or
- Contact us at: contact_center@meriwest.com

ATM and Debit card tip:

If you are planning on traveling, especially outside of the country, be sure to notify Meriwest in order to protect your security and ensure no interruption of service or access to your account(s) through your card(s).

What to do if you think your identity was stolen:

- Contact Meriwest immediately to close any Meriwest accounts that have been tampered with or established fraudulently.

- The Federal Trade Commission - Report ID Theft website is a resource that makes it easier for victims to report and recover from identity theft. The website provides an interactive checklist that walks you through the recovery process and helps you

understand which recovery steps should be taken upon learning your identity was stolen. It also provides sample letters, specialized tips for specific forms of identity theft, and advice if you have been notified that your personal information was exposed in a data breach.

- At no cost, you may place a fraud alert on your credit file that lets creditors know to contact you before opening new accounts. Call, or visit online, any one of the credit reporting agencies listed below. This will let you automatically place fraud alerts and order a credit report from all three.

  Equifax - Report Fraud, 888-766-0008
  Experian - Report Fraud, 888-397-3742
  TransUnion - Report Fraud, 800-680-7289

- You are entitled to one Free Annual Credit Report from each of the agencies listed above. If you choose to receive credit reports, look them over carefully for suspicious activity like accounts you did not open or for balances that appear to be inaccurate. Also, look for inquiries from creditors that you did not initiate and look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report. Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next two years.

- Close other accounts that you know or believe have been tampered with or opened fraudulently. Please ask for the Meriwest ID Theft Affidavit and Information Packet when disputing unauthorized accounts.

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.

- File your complaint online with the Federal Trade Commission - Report ID Theft. The Federal Trade Commission ("FTC") maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing also helps the FTC gather more information about identity theft and the problems victims are having.

- For more information on identity theft, please visit the Federal Trade Commission – ID Theft Information or call 877-IDTHEFT (877-438-4338).

How Meriwest is notified of a data compromise:

When a data compromise affecting your Meriwest account(s) or ATM or Debit card occurs, we are notified by multiple sources, including MasterCard®, preferred vendors, and law enforcement agencies.

Meriwest Credit Union
Customer Awareness and Education

What to expect if a data compromise occurs:

To manage and mitigate card loss and fraud, we use a network fraud detection system for ATM and Debit card monitoring. We monitor your Meriwest account(s) and ATM or Debit card to attempt to identify any out-of-pattern activity and to identify any risk of fraud. When an account or card has been identified as being at risk for fraud, we will proactively close or block your account or card and may provide you with a new account or card if necessary.

Important things to know if your data has been compromised:

- Blocking your account or card is strictly a precaution based on our commitment to the security of your account or card.
- Reissuing a new account, ATM card, or Debit card may not always be necessary, but we will do so when required as a safety precaution.
- It does not mean that fraud will occur on your account, ATM card, or Debit card.
- It does not mean that you will become a victim of identity theft.
- If you suspect fraudulent activity, notify us promptly.

Depending upon what is compromised, our notification process will vary:

- **Meriwest account compromise**

  If your Meriwest account is compromised and we believe your information is not at risk, you will receive a phone call or a letter from a Meriwest employee informing you of the compromise and giving you the option to close your account and open a new one. If we believe your information is at risk, you will receive a phone call or a letter informing you that we are taking a proactive approach to protect your account by closing it and replacing it with a new one.

  If you have recurring charges, bill payments, or purchases on your account, contact any merchants and inform them of your new account number.

- **Meriwest ATM card compromise**

  If your Meriwest ATM card is compromised, you will receive a new ATM card with a letter informing you that we are taking a proactive approach to protect your account by closing your old ATM card and replacing it with a new one.

  Upon receipt of the new ATM card, follow the instructions on the front of the card to activate it. It is important that you immediately activate your new ATM card as the old card will expire shortly (regardless of the expiration date) after receipt of the new card. Immediately destroy your old ATM card.

  As a courtesy, we will use the same personal identification number (“PIN”) on your new ATM card as you had on your original, compromised ATM card. However, you change the PIN at one of our financial centers or by calling 877-746-6746 after you receive your new ATM card.

- **Meriwest MasterCard® Debit card compromise**

  If your Meriwest MasterCard® Debit card is compromised, you will receive a new Debit card with a letter informing you that we are taking a proactive approach to protect your account by closing your old Debit card and replacing it with a new one.

  Upon receipt of the new Debit card, follow the instructions on the front of the card to activate it. It is important that you immediately activate your new Debit card as the old one will expire shortly (regardless of the expiration date) after receipt of the new Debit card. Immediately destroy your old Debit card.

  As a courtesy, we will use the same personal identification number ("PIN") on your new Debit card as you had on your original, compromised Debit card. However, you can change the PIN at one of our financial centers or by calling 877-746-6746 after you receive your new Debit card.

  If you have recurring charges, bill payments, or purchases on your account, contact any merchants and inform them of your new Debit card number and expiration date.

FAQs – Frequently Asked Questions

- **What if I think my check, ATM card, or Debit card number is being fraudulently used?**

  Many times a single unauthorized charge is found to be a merchant error. Simply contacting the merchant might resolve the error quickly. However, if you think your check, ATM card, or Debit card number is being used fraudulently, call us at 877-MERIWEST (877-637-4937) or call the phone number located on the back of your card.

- **What has happened if I am notified of a data compromise?**

  We were notified that your account information may have been compromised and your Meriwest account, ATM card, or Debit card number was included in that compromised information.

- **How do I know if my account or card has been compromised?**

  If your Meriwest account or card has been affected by a compromise and we believe your account or card is at risk, you will be notified by a letter or a phone call from a Meriwest employee.

- **Where was the information compromised?**

  We are notified of compromised information from multiple sources, including MasterCard®, our partnered vendors, and law enforcement agencies. These notifications may not include the merchant name or location in the initial notification.

- **When did this compromise occur?**

  The compromise may have occurred over a period of time. This information is not always provided to us until further investigations are conducted.

- **Is it safe to use my new account or card?**

  We are confident that the steps we have taken will ensure the continued security of your information. Please use your new Meriwest account or card as you normally would.

- **What else do I need to do?**

  In addition to destroying your old cards and reviewing your recent charges or purchase transactions, notify any merchants who are using your old Meriwest account or card number for recurring charges, bill payments, or purchases. Provide them with the new Meriwest account or card information and, if appropriate, new expiration date. Also, evaluate your recent transactions and ensure they are all yours. If you see transactions you do not recognize, call the number on the back of your card or call us at 877-MERIWEST (877-637-4937) to report the fraud.

- **What type of tools are you using to monitor my account or card?**

  We employ a series of monitoring tools that look for unusual and fraudulent activity. For security purposes, we are not able to disclose all the specific types of tools or their operation. However, for ATM and Debit card monitoring, we use a network fraud detection system to manage and mitigate card loss and fraud.

- **Is there anything that I can do to ensure that fraud does not occur on my card?**

  Always know where your cards are. If you misplace them, call us immediately so we can block the card from use. Regularly monitor your account(s) for fraudulent activities. The Meriwest Online Banking and Mobile-Meriwest services provide you with a quick and easy method to access your account information, set up alerts, and have constant access and monitoring of your account(s).

- **Do I need to close my other Meriwest accounts or cards?**

  It is not necessary at this time to close other Meriwest accounts or cards. We monitor all products and accounts and will notify you if any additional action is necessary. We encourage you to put a password on your account(s), however.

Change in Customer Awareness and Education Document

We may revise this Customer Awareness and Education document at any time without notice to you by updating this posting. The latest document will be posted on the Meriwest Website and you should review the document each time you access the Meriwest Website. Certain provisions of this document may be superseded by expressly designated legal notices or terms located on particular pages at the Meriwest Website.

Last updated: April 2016