temenos

# Protect Yourself from Identity Theft

The security of customer information is paramount for all financial institutions. A significant amount of time and resources are spent trying to protect customer information. But, with all that they do, they can't do it alone. They need your help. Below are a few areas where you can help protect your data.

- **Personal Information**

  It's easy to get comfortable sharing personal information online, but cybercriminals can do a lot of damage with just a little information. Hackers figure out your passwords and answer security questions in the password reset tools by using social media profiles. A best practice is to lock down your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Also, be wary of requests to connect with people you do not know.

  To be safe, never share identifying details, like your full name, address, or financial information, with strangers you meet online. It would be a good idea to be careful in creating usernames. There's no mandate that you have to include your real name. Also, be careful with how much information you share in online surveys or forms. Most of the time, little to no personal information is needed to complete them.

  Staying safe online can feel challenging, but it doesn't have to be. A couple of essential items to consider:

  - Protect your Social Security number. Do not email your SSN to anyone. Another thing to remember is don't carry your Social Security card in your wallet or anything else that shows your SSN.
  - Protect your Driver's license, State ID Card, Passport, or Military ID Card. Do not carry them all simultaneously.

- **Family**

  You can take all the safety measures on your home network, but if your family and other people using your network aren't doing their part to keep everything secure, your efforts might not be enough. Ensure that everyone who regularly uses your network knows how to help keep it safe. Kids can learn about cyber safety, too.

- **Computers and Mobile Devices**

  The best defense against viruses, malware, and other online threats is to use the latest security software, web browser, and operating system. A good suggestion is to turn on automatic updates on your devices to ensure your security software, web browsers, and devices are up to date. Critical fixes are included in updates to patch security holes that could have been detected in your programs or devices.

- **Passwords**

  Strong passwords are an excellent way to protect yourself from online identity theft. Unfortunately, even now, people are still using weak passwords. Examples of weak passwords are 123456, your dog's name, or your kids' birthdays.

  The most robust password is no good if you can't remember it. The most important thing to do when creating a password is to make sure it is something you can remember but hard for other people and malicious programs to guess. For example, an abbreviated sentence, or passphrase, is often better than a single word with numbers and symbols inserted. You can use a password management app to generate and store your passwords. A password manager can also help you generate unique passwords for your online accounts. Finally, for extra security, change your passwords frequently throughout the year.

- **Multi-Factor Authentication**

  Multi-factor authentication requires verifying your identity after you've logged in using your username and password. Occasionally, you'll be asked to verify your identity by entering a code sent by text to your phone or email. Other times, you'll have to answer a security question whenever two-factor authentication is available. It may take a bit more time to log in to your accounts, but it will reduce the likelihood that other people will be able to log into them, too.

- **Computer and Mobile Device Back-Up**

  Malware can inflict havoc on your computer, and if you become a victim, backing up your data is the best way to ensure you get your data back. In addition, when you back up your data, you can make sure security breaches are less problematic. A good example is if a hacker encrypts your data and demands a ransom to unencrypt it, it won't be that big of a deal if you backed it up recently.

- **Bank Statements and Bills**

  You should open your credit card bills and bank statements as soon as you receive them and check carefully for unauthorized charges or withdrawals. If you see any issues, you should report them immediately. You should also call if bills don't arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.

- **Credit Reports**

  Credit reports should be reviewed at least annually. When you review the report, you should check for changed addresses and fraudulent charges.

- **Credit Score**

  It would help if you always remembered your latest credit score. If your score went down significantly, you might have been a victim of Identify theft.

- **Pre-Approved Credit Offers**

  A good target for identity thieves is to steal pre-approved credit card offers in your mail. It will help if you have your name removed from credit bureau marketing lists. If you continue receiving pre-approved offers, you should call and verify the offer.

- **Shredding / Destroying Information**

  Another good practice is shredding or destroying papers containing your personal information. This includes credit card offers and checks that you don't use.

- **Public Wi-Fi**

  Try avoiding unsecured public Wi-Fi on any of your devices. You should know that you are vulnerable to predatory practices if you use them. If you must use it, avoid entering compromising information like your Social Security Number or financial information. A better option is to use a virtual private network (VPN) to browse when you're not at home. This will encrypt the data you send and receive, making it much harder to intercept.

- **Shopping Online**

  Before shopping online, make sure the website is secure. One way is to verify that the web address begins with HTTPS when you are at the checkout screen. The "s" at the end is critical because it indicates that your connection is encrypted. Don't purchase anything from a website that doesn't include encryption. Another item to look for is a tiny, locked padlock symbol. Additionally, you should think twice about saving your financial information on websites you buy from, even if you shop with them frequently. Storing your information on their website could make it easier for hackers to access it if the company's website or network suffers a data breach.

- **Corporate Privacy Policies**

  Privacy policies can be long and complex, but they will tell you how the site protects the personal information it collects. If you don't see or understand the website's privacy policy, you should consider not doing business with the company.

- **Multi-Step Authentication Thief:**

  A fraudster could send thousands of fake alert text messages, pretending to be the peer-to-peer platform or other financial institution offering convenient online banking services. Responding will prompt the con artist to call, claiming to be a fraud department and asking you to verify your account by sending a code to your phone.

  That multi-factor authentication code is sent to your verified number to confirm that you're attempting to access your account. Users should never give this number to anyone—your account can be compromised as soon as you provide the verification code. Financial institutions never ask for sensitive information via phone, email, or text. This includes requests for passwords, secure access codes, verification codes, PINs, or credit/debit card 3-digit security codes.

  Multi-Step Verification is highly recommended and often required for protecting accounts from cyberattacks. For example, some hackers run bots that use complex algorithms to try and gain access to your account by "guessing"

your password. Using upper- and lower-case characters and numbers makes these slightly more challenging to guess, so a secondary form of identification will make this kind of attack harder.

The second level of authentication could include a PIN, a confirmation sent via phone or email, or a passcode sent to your phone via text message, etc. Unfortunately, fraud and scams cause a real threat to convenient banking platforms and the financial security of not only you but your customers or members as well. You can avoid many of these pitfalls by staying updated on the latest schemes.

In other words, know your enemy and their tactics.

- **Phishing**

  A common goal of phishing, vishing, or smishing schemes is stealing your password. Phishing scams trick users into disclosing private account(s) or login information using fraudulent emails and websites. It would help if you always use caution when giving out your personal information. Con artists "phish" victims by pretending to be banks, stores, or government agencies. They do this over the phone, in emails, and postal mail. For example, scammers may sign up for peer-to-peer platforms that pretend to be you and pull money directly from your account. To create an account in your name, they would need access to account numbers, a social security number, and other forms of sensitive data often obtained through a data breach.

  Financial institutions typically don't ask for your SSN or other personal information over the phone and most make a point to emphasize that they do not ask for this information. Never send your SSN or credit card information via email. If you don't feel comfortable putting this information on a postcard, you probably wouldn't want to send it by email.

  It's best if you don't click on links or open any attachments or pop-up screens from sources you are unfamiliar with. Viruses and other forms of malware frequently spread because you click on a link from someone you know or don't know. If you receive a link that looks strange (for example, typos in the hyperlink), and you know the sender, contact them to ask if the link you've received was sent on purpose. We don't advise it, but if you can't wait for a response from your friend or family member, it's best to copy and paste the link into a reputable link checker, but don't click on the link.

  The safest option is, don't download the attachment because it has the potential to damage your home network. Drive-by downloads can install malware on your hard drive without you knowing or agreeing to download it. Additionally, a drive-by download might disguise itself as a standard system update or another innocuous "yes/no" question, and even the most cyber-savvy among us can be fooled. Due to this, it's a good idea to refrain from opening emails from addresses you don't know.

  You can also notify the company, bank, or organization impersonated in the email. The Federal Trade Commission (FTC) also set up an email to report phishing. The email address is spam@uce.gov.

- **ATM Machine**

  It would help if you always kept your PIN in a safe spot and didn't share it with anyone. Another good practice is always to finish your transaction thoroughly when withdrawing money from an ATM Machine. Don't use your debit card at a gas station or convenience store, as fraud operators can map your PIN to their device and use it to make purchases.

- **Malware**
  Fraudsters use malware to collect data through keylogging or man-in-the-middle malware which intercepts data via the victim's internet browser.

- **Fake Text**

  Frequently, these texts say you have won a prize, and you reply, and then they can hack your cell phone and steal your bank passwords.

- **Telephone Scams**

  Avoid the dreaded car warranty someone has purchased *fill in the blank* on your Amazon account or spam calls. These people are fraudsters out to get your account information or get you to make bogus payments.

  If you receive a call and are asked for personal information that seems inappropriate for the transaction, you should ask questions. Some good questions are:

- How will the information be used?
- How will it be shared?
- How will data be protected?

In the end, don't give your personal information if you're unsatisfied with the answers.

- **Internal Revenue Service (IRS) Phone Scams**

  The IRS will never make a collection call. These are primarily scammers that call asking for money on behalf of the IRS. If possible, avoid these calls. A few things you can do is ask for a badge number and let the person know you are recording their call, and you will turn the information over to the local Sheriff's Department.

In review, many resources and factors are available to you, the customer, when safeguarding your information. It is always paramount for a financial institution to have policies and procedures in place to ensure their client's information is well protected. With the combined efforts of the bank and the customer, personal security will be taken to the next level, and customer information will be well secured.