Comerica Bank

RAISE YOUR EXPECTATIONS.

How Are Fraudsters Stealing Your Identity?

One of the ways to avoid becoming a victim of identity theft is to learn how identity theft occurs and some best practices to protect your information. Identity theft occurs when someone obtains your personal information (Social Security number, credit card numbers, etc.) and then uses it to fraudulently apply for credit or open accounts without your knowledge. It can take time, money and patience to resolve.

Identity thieves get your Personal Identifying Information (PII) in numerous ways, including:

- **Stolen Wallet:** When your wallet is stolen, fraudsters could gain instant access to all the personal identifying information they need to steal your identity.
- **Change of Address:** This is a classic identity theft technique. Fraudsters change the address where you receive mail and divert your personal information into the wrong hands.
- **Skimmers / Handheld Skimmers:** Fraudsters can steal your personal information anywhere you use your card by swiping it when you are in the midst of a legitimate transaction, like making a purchase in a store or using an ATM. They can literally swipe your account information when you insert your card and then transmit your information to a nearby computer.
- **Online Shopping:** Fraudsters are experts at duplicating legitimate online storefronts. Before you know it, you've completed your transaction and inadvertently handed over the personal information they need to commit fraud.
- **Mail Theft:** Fraudsters scout for unlocked mailboxes and steal your mail – and your identity – right from your front door.
- **Phishing:** Fraudsters are busy impersonating legitimate businesses via email, online advertisements and text in order to acquire your personal information or install malicious software (malware). Once installed, malware can run programs on your online devices without your consent or knowledge, and transmit your personal information via the Internet.

What information is considered your Personal Identifying Information (PII)?

- Full Name
- Social Security Number (SSN)
- Driver's License, State-Issued ID or Passport Number
- Date of Birth
- Home Address
- Credit Card, Debit Card or Bank Account Numbers
- Secret Information (such as mother's maiden name, PIN or password)

The more Personal Identifying Information a fraudster has about you, the more your identity is at risk.

What to Do If You're a Victim of Identity Theft

If you suspect that you are a victim of identity theft, it is important to act as quickly as possible to minimize the damage to your finances and your credit standing.

1. **Notify your creditor or financial institution** of any identified unauthorized transactions on your account and ask to file a claim. If you are a Comerica customer, contact Comerica Bank at 877.881.8955, Monday – Friday, 8 a.m. to 8 p.m. ET.
2. **Create an identity theft report** by filing a complaint with the FTC at ftccomplaintassistant.gov or 877.IDTHEFT. Your complete complaint is called an FTC Affidavit. Take your FTC Affidavit to your local police or the police where the theft occurred, and file a police report. Don't forget to get a copy for yourself.
3. **Flag your credit reports** by contacting one of the three nationwide credit reporting companies and ask for a fraud alert on your credit report. An initial fraud alert is good for 90 days. As soon as one of the bureaus issues a fraud alert, the other two are automatically notified. Additionally, you should order a copy of your credit report and review the information carefully. If you see mistakes or signs of fraud, contact the credit reporting company immediately.

	Phone Number	Website
Equifax:	800.525.6285	equifax.com
Experian:	888.397.3742	experian.com
Transunion:	800.680.7289	transunion.com

4. **Contact the Social Security Administration** if your Social Security card has been lost or stolen and you would like to request a (replacement) new card. Contact the Social Security Administration at 800.772.1213 or visit socialsecurity.gov.

Comerica Bank®

RAISE YOUR EXPECTATIONS.

Tips to Help Protect Your Information and Identity from Being Stolen

Comerica Bank is committed to safeguarding the privacy of your personal information. However, there are some steps that you can take on your own to help protect your information from being stolen.

Protect your Personal Identifying Information (PII)

- When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home.
- Shred sensitive papers. Shred receipts, bank statements and unused credit card offers before throwing them away.
- Keep an eye out for missing mail. Fraudsters look for monthly bank or credit card statements or other mail containing your financial information. Also, don't mail bills from your own mailbox with the flag up.

Don't share your personal information

- Don't provide your Social Security number, account information, PINs or passwords to anyone who contacts you online or over the phone.
- Do not reveal sensitive or personal information on social networking sites (i.e., Facebook). If you post too much information about yourself, a fraudster could use it to answer challenge questions or guess your passwords on your accounts.
- Lock up your personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.

Take advantage of the security of online banking

- Monitor your financial accounts online regularly for fraudulent transactions.
- Consider enrolling in Comerica Web Banking® and utilize eStatements to reduce the likelihood of paper statements being stolen.
- Sign up for Comerica Mobile Alerts® to receive immediate text or email notifications on your account when a transaction is outside your normal activity.

Protect your computer, tablet and mobile device

- Create strong passwords that mix letters, numbers and special characters. Don't use one password for everything, and change them periodically.
- Use anti-virus and anti-spyware software, and a firewall on all of your devices that browse the Internet. Set the operating systems and web browser security system to update automatically.
- Use the passcode lock on your smartphone and other devices. This will make it more difficult for a fraudster to access your information if your device is lost or stolen.

Be cautious when opening emails and clicking on links

- The threat of cybercrime most often begins with "phishing." Cyber criminals attempt to infect your computer with malicious software. Malware includes viruses, spyware and key loggers that get inadvertently loaded on your computer, allowing the criminals to monitor, control and track your online movements, steal your passwords and compromise your accounts.
- Opening attachments, even those that appear to come from a friend or co-worker, can install malware on your computer.
- Type a site's URL directly into your browser. Links in email, tweets, posts and online advertising can send you to sites that masquerade as your favorite sites or appealing new sites but may automatically download malware without your knowledge.

Other Agencies

To remove your name from mailing lists, contact the Direct Marketing Association or complete the online Registration Form for Mailing Preferences:
Call: 212.768.7277, ext. 1888
Online: dmachoice.org

To remove your name from telephone solicitation lists, contact the Federal Government's National Do Not Call Registry:
Call: 888.382.1222
Online: donotcall.gov

To opt out of prescreened offers and marketing lists, contact the Consumer Credit Reporting Agency:
Call: 888.567.8688
Online: optoutprescreen.com

To file a mail theft complaint, contact the U.S. Postal Inspection Service:
Call: 800.275.8777 and ask to speak with a customer service representative
Online: postalinspectors.uspis.gov