

ID THEFT AND FRAUD PROTECTION



For branch locations and more information, visit www.ChemicalBankMI.com



UNDERSTANDING IDENTITY (ID) THEFT

Crimes involving ID Theft or impersonation are on the rise and are now the most frequently reported type of crime to the Federal Trade Commission (FTC). ID Theft occurs when someone pretends to be you when committing a crime. ID Theft can be committed in person, over the telephone or Internet, through the mail or through texting.

Criminals are continually developing new ways to exploit or defraud organizations and consumers. This includes attempting to access online bank and brokerage accounts or steal credit information.

TYPICAL DANGERS FACED WHEN USING THE INTERNET

- Viruses and worms: programs that self-replicate or are sent over the Internet by email and can damage your PC
- Trojans: programs that, unknowingly, compromise computer security by intercepting passwords and sensitive information
- Phishing: using a false name, website or address for fraudulent purposes
- Hacking: unauthorized access to a PC via the Internet

Chemical Bank uses leading-edge technology to aid in fraud detection. We continually monitor for fraudulent web sites and work to shut them down as soon as possible. We also monitor account activity to detect fraudulent credit, debit card, or online banking transactions and notify customers when we suspect fraud. Additionally, we participate in industry consortiums made up of some of the largest financial institutions in the United States, allowing us to address emerging issues in online fraud.

Since these schemes are perpetrated outside of our control, **it is imperative that you, as a customer, regularly monitor your accounts and report any suspicious activity immediately.** When fraud has been committed, we will work with you to block the affected account and restore access to your credit/debit cards or online banking accounts.

I SUSPECT ID THEFT - NOW WHAT?

If you are concerned that someone has gained unauthorized access to your personal information, please call us immediately at 1-800-867-9757 so we can take steps to help protect you. You should also report your concerns to:

- Your local law enforcement agency
- The Federal Trade Commission identity theft hot line at 1-877-438-4338
- The Internet Crime Complaint Center at <http://www.ic3.gov/default.aspx>
- The Social Security Administration fraud hot line at 1-800-269-0271
- Your credit card companies. Remember, knowing where to find your credit card information and toll-free contact information will help in an emergency
- National credit reporting organizations to place a fraud alert on your credit bureau reports:

Equifax 1-888-766-0008
Experian 1-888-397-3742
Trans Union 1-800-680-7289

OTHER HELPFUL LINKS

<http://www.ftc.gov/idtheft>
<http://www.equifax.com>
<http://www.transunion.com>
<http://www.experian.com>
<http://www.ic3.gov/default.aspx>



CONTACT OUR CUSTOMER CARE CENTER AT 1-800-867-9757 IF:

- You have disclosed sensitive information in a phishing attack,
- You suspect an email or web site is fraudulent,
- You suspect unauthorized activity on your online account or your bank account,
- You received a text message, voicemail or phone call directing you to call and provide sensitive information such as credit card or account number.

For more information, visit Chemical Bank's Security Center at <http://SecurityCenter.ChemicalBankMI.com>.

10 RULES TO PROTECT YOURSELF

1. Install security software including an up-to-date virus scanner.
2. Protect sensitive data when sending it over the Internet.
3. Be sure you know WHO you are dealing with.
4. Be careful with sensitive data and media.
5. Choose a secure password.
6. Only use programs from a trustworthy source.
7. Use up-to-date program versions.
8. Run a security check on your PC.
9. Activate the browser's security settings.
10. If it sounds too good to be true it probably is!

YOUR COMPUTER

- Install and use a firewall program on your personal computer. A firewall helps prevent hackers from accessing your computer.
- Install security protection software on your computer and update it regularly.
- Use the automated update feature in your Operating System to download and install the latest security patches.
- Make sure personal and financial information stored on your personal computer is protected with a strong password or encryption.
- Avoid automatic sign-on features that save your user name and password; and always sign off when you're finished.

EMAIL

- Watch out for "phishing" or "spoofing" emails that may look like they are legitimate messages, but are not. The sender attempts to get you to reveal confidential personal information to use for identity theft. **Chemical Bank will never contact you via email to ask for or to validate any personal information.**
- Forward emails requesting your private information to SecurityCenter@ChemicalBankMI.com.
- Never open any email attachment, Web link, or file if the source is not trustworthy or cannot be confirmed.

US MAIL

- Pay attention to billing cycles for bills you receive regularly. If you do not receive a bill from your service provider(s) in a regular manner, an identity thief may have diverted your bill.
- Promptly remove mail from your mailbox.
- Only place outgoing mail in post office collection boxes, or consider using Online Banking with Bill Pay to send payments. Making payments online can help prevent mail fraud while saving you time and postage.
- Shred all credit card solicitations you do not want.

CREDIT AND ATM CARDS AND ACCOUNTS

- Immediately report any lost or stolen cards.
- Shred all receipts and bank and credit card statements before disposing of them.
- Regularly review your credit report from all three major credit bureaus to ensure that no one has opened new credit card or other accounts in your name.
- Limit identification information and carry only those cards you will need.

YOUR SOCIAL SECURITY NUMBER

- Don't print your Social Security number or driver's license number on your checks.
- Keep your Social Security card in a safe place instead of carrying it in your wallet.

SECURE EMAIL

We offer customers the ability to send us secure emails. It is the best way to communicate with us and the **ONLY** way to be sure your confidential information (account numbers, tax ID numbers and financial statements) is delivered safely. We at Chemical Bank feel it's our responsibility to protect the sensitive business information we share. You only need to register once and from then on, will be able to receive or initiate encrypted emails with Chemical Bank.

To login, create an account or learn more, select the Secure Email or Contact Us links on our website, www.ChemicalBankMI.com.