CMC CATHOLIC MEDICAL CENTER | Information Security

Identity Theft Protection Checklist

Prepare for it

- Keep a list of all account numbers with customer service telephone numbers in a **secure** place for easy access if you need them (photocopies of both sides of credit cards is a good start).

Monitor Your Accounts

- Check the status of your bank accounts at least every few weeks (or use automated monitoring).

Watch Your Credit

- Check each of your 3 credit reports from AnnualCreditReport.com (877) 322-8228 annually.
- Some organizations including AAA AAA.com/experianidtheft/ (choose Essential) and Discover https://www.discover.com/credit-cards/resources/protect-your-social-security-number/ offer FREE credit monitoring.
- Unless you plan to apply for a loan, consider freezing your credit (within the credit bureaus) to prevent someone from opening a new account in your name (typically costs between $0 and $30 per freeze/unfreeze)
- Consider setting lower credit limits to reduce your liability.

Guard Your Papers and information sources

- When traveling, have your mail: ▫held, ▫sent to a post office or ▫put in a locked mailbox.
- Ensure your purse, wallet, laptop and mobile devices (smart phones, tablets, etc.) are never left unattended, even for a minute.
- Shred (with a cross-cut shredder) old or unwanted documents with personal information including:
  - Banking & credit card statements, Drivers license info, Medical info (including prescription labels) and Insurance info

Keep It Private

- Be **very** careful of, times, locations and other personal information you post to social media sites.
- Consider the benefit of sharing your information for catalogs, mailing lists, email coupons, loyalty programs.
- **Never** share financial information including credit card numbers, account numbers, PIN numbers, CVCs, passwords, or personal info with anyone in a conversation you did not initiate.
- Don't let anyone watch your keyboard (or an ATM) as you input a PIN, password, or credit card number.
- Opt out of mailing lists: 888-5-OPTOUT (888) 567-8688 and the FTC: (888) 382-1222 DoNotCall.gov

Protect Yourself Online

- Use strong passwords. Don't use the same password for different accounts where money or identity is involved.
- Carefully read Email.
  - Don't click on embedded **links** or **attachments** from people you don't know.
  - Be suspicious of anything that sounds "too good to be true" and verify claims independently.
- Browse carefully.
  - Bookmark sites that you visit often.
  - Type addresses by hand if it's a new site that you may not trust.
  - Don't perform transactions online unless the sites are secured (via HTTPS).
- Keep software, anti-virus protection, firewalls and operating system patches updated.
  - If you don't have anti-virus protection, get it, configure it properly and use it.
  - Turn on the firewall that comes with Windows if you haven't already. This may require some tuning to ensure your applications work through the firewall, but it's worth the effort.
- Any popup window from your computer or the WWW that tells you to call a number or click a link to protect your computer is a **scam**.

Act quickly

- If you think your identity has been stolen, take the following actions immediately:
  - Call your financial institutions.
  - Alert the credit bureaus: Equifax.com (888) 298-0045, Experian.com (888) 397-3742 and TransUnion.com (855) 681-3196
  - Contact the FTC via Consumer.FTC.gov/articles/0277-create-identity-theft-report
  - If it involves mail, contact the Postal Inspectors at USPIS.gov
  - If your SSN is involved, contact the IRS www.irs.gov. Tax Identity Fraud has become very popular.
  - File a police report.