Was your personal information stolen or compromised?

Monitoring Your Identity – steps you can take when you are at a high risk of identity theft.

A. Place a fraud alert with the Credit Reporting Agencies (CRA).

a. Once you place the alert with 1 agency they will alert the other 2.
    i. Transunion
        1. Online: http://www.transunion.com/fraud-victim-resource/place-fraud-alert
        2. Phone: 800-680-7289
    ii. Experian
        1. Online: https://www.experian.com/fraud/center.html
        2. Phone: 888-397-3742
    iii. Equifax
        1. Online: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
        2. Phone: 800-525-6285
b. Fraud Alerts last for 90 days. At the 90 days, you may have the option to place an extended 7-year fraud alert. See the CRA policy for placing an extended alert.

B. Get free copies of your credit reports.

a. You are entitled to 1 free credit report every 12 months from each CRA.
    i. Online: https://www.annualcreditreport.com/index.action
    ii. Phone: 1-877-322-8228
        1. Order from each agency every 4 months to see your report frequently.
b. When you place a fraud alert you are entitled to 1 free credit report from each CRA when you place the initial fraud alert.
    i. Request these right away and diligently review your report. You are looking for anything you don't recognize or remember doing. I.E. requests for credit, addresses you have never resided at, etc.

C. Alert & Close any/all bank, credit card, library accounts that may be compromised.

a. If you choose to keep your accounts open it is important to monitor all your accounts closely for fraudulent transactions.
    i. The amount of time between the fraudulent charges occurring and when you notify the bank will determine your financial liability.

D. Create an online social security account

a. https://www.ssa.gove/myaccount/
    i. Monitor your yearly earnings statements for reported income that exceeds the amount you know you made.
        1. If your social security number is stolen, the thief could use your information to fraudulently create your online social security account. Which would give them the ability to direct your SSD or retirement to an account of their choosing.

E. Police report

a. If you become an identity theft victim, update the police report with all new information

F. Monitor all current accounts for transaction you did not make

G. Child Identity Theft

a. Call all 3 Credit Reporting Agencies to find out if your children, under 18, have a credit report. Unless your child has taken out credit in their own name, there should not be a credit report for them. If there is a credit report, they are a victim of identity theft.
    i. You can find resources to begin the recovery process online at https://www.ftc.gov/, or call the Spokane COPS Crime Victim Advocate at 509-625-3328.

Documentation Essentials:

- Phone
    - Who you spoke with and when. What you spoke about and agreed upon. What you need to follow-up on. How to reach this person again.
- Snail Mail
    - Send all correspondence via certified mail with delivered receipt required.
    - Send only copies; never send the originals.
- Email
    - Not recommended – if you choose to use this form of communication ask for a message received confirmation.
    - Print out all email correspondence

Safeguard your personal information

At Home	Online

➢ Purchase a locking mail box
➢ Purchase a home safe – keep social security card, passport, etc. locked-up.
➢ Shred documents containing personal information
➢ Decrease unsolicited snail mail – opt-out
➢ Decrease telemarketer calls – National Do-Not-Call registry
	➢ Avoid phishing scams
	  ○ Links in emails
	  ○ Pop-up ads
	➢ Unique & strong passwords
	  ○ Use characters
	  ○ Use random words
	➢ https:// Use only websites that contain the lock symbol and https at the *beginning* of their web address
	➢ Think first, post second

On the Go	Computers, phones, IoT's**

➢ Use public wi-fi cautiously
  ○ Avoid going to bank, social media, & email sites
  ○ Turn off public sharing
➢ Skimmers at gas pumps or ATMs
  ○ Look for an unbroken seal on pump
  ○ Pay inside
  ○ Use ATMs inside the bank
	➢ Use anti-virus & firewalls & anti-malware
	➢ Multi-factor authentication
	  ○ Something you know, something you have, and something you are
	➢ Password protect *every* device you own; use multi-factor authentication when available

Tools	Scams
➢ Banking alerts ➢ Multi-factor authentication ➢ Security Keys/Tokens ➢ Password managers ➢ Biomentrics	➢ IRS/Tax – phone, email, or snail mail ➢ Jury Duty – phone ➢ Lottery – phone, email, or snail mail ➢ Job – craigslist ➢ Phishing – email, links, or ads ➢ Skimmers – gas stations, ATMs ➢ Hacking – any device or IoT

Report

Resources	Reporting Scams	Reporting Internet Scams
Decrease unsolicited snail mail 1-888-5-OPT-OUT **Decrease Telemarketer Calls** 1-888-382-1222	**Report IRS Email Scams** phishing@IRS.gov **Report IRS Impersonators** You don't owe money: 1-800-366-4484 You do owe money: 1-800-829-1040 **Report ALL Scams** FTCcomplaintassistant.gov	**Report Internet Scams** www.ic3.gov FTCcomplaintassistant.gov **Report All scams** Ftccomplainassistant.gov **Also**, report scams directly to companies – e.g. google, amazon, craigslist, yahoo.