FAIRPORT WEALTH

After Identity Theft: Next Steps to Secure your Information

1. File a police report.

2. Notify banks/credit card companies/custodians.

3. Add a freeze and/or alert with the Credit agencies. **For alerts, you only need to do this for one agency, and you'll be covered by all three.**

- https://www.equifax.com 1-888-766-0008
- https://www.experian.com 1-888-397-3742
- http://www.transunion.com 1-800-680-7289

4. Change your username and passwords (social media, email, banks, custodians, etc.).
    - set up Two-Factor ID

5. If you have clicked on a website that is malicious, the scammers may gain your future keystrokes for the next few sites which will include all your accounts and new passwords – make sure to delete all browsing history.

6. Contact phone provider to secure your phone number (set up Two-Factor ID).

7. Remove personal information on social media/email and check your privacy settings.

8. Consider a credit monitoring/protection service such as Lifelock or AllClear.

9. Add alerts to your credit cards/bank checking accounts so that you will receive notification if there are any changes to your accounts and/or new activity.

10. Add Two-factor ID to your bank accounts, Streaming services (like Amazon), etc.

Here is a link to the FTC regarding Identity theft protection services:

- https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services
- Report identity theft with the Federal Trade commission https://www.identitytheft.gov

BEST PRACTICES:

- Remember to sign out of each website once you are done browsing and turn off your computer.
- Don't clink on unsolicited email attachments or a legitimate-looking download.
- Let unknown callers go to voicemail.
- Use strong passwords.
- Avoid using unsecure WiFi networks in public places.
- When in doubt about a link, email etc., call your Advisor.