Potential Fraud Tips

Here are some practical tips for individuals whose information may be compromised by a breach:

- Personal credit reports should be monitored for new applications that were filed on your behalf.
- Monitor all monthly statements for any unauthorized payments.
- Monitor your existing credit card and Credit Union/ bank accounts closely for charges you don't recognize; such as address or phone number changes.
- Consider placing a credit freeze on your files. A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts.
- If you decide against a credit freeze, consider placing a fraud alert on your files. A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you.
- File your taxes early — as soon as you have the tax information you need, before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS. The IRS will only contact you through the mail.

Phishing and Ransomware

Criminals will use an email, telephone messages (vishing) or text messages on cell phones (Short Message Service or SMShing) to trick recipients into disclosing personal and financial data. Some phishing attempts ask e-mail or text recipients to respond with personal information; and others include links to what appear to be familiar Web sites but are really spoofed copies. Once the user clicks on the link to the spoofed site, all future online activity gets funneled through the phisher's system, giving him or her access to any account numbers and passwords the user enters online.

To protect yourself from phishing:

- NEVER respond to an e-mail asking you to verify or update your personal information
- Never click on links in unsolicited e-mail that you receive
- Delete any unsolicited e-mails in your e-mail accounts – don't even open them!
- Protect your passwords. Never write them down or enter them online unless *you* initiated the transaction.
- Never give out your personal or financial information on the phone or online unless you initiated contact
- Check your credit report at least once annually or sign-up for weekly or monthly alerts through credit management agencies
- At home, use spam blockers, firewalls, virus protection, and adware & malware destroyers
- Update your Operating System whenever security patches are available

Ransomware attacks have relied on a user's clicking on a phishing e-mail or infected website or downloading malicious software. The ransomware would infect individual machines and shared resources to which the user had access rendering them useless until a fee is paid. These attacks can focus on individuals, businesses and industries.

The FBI recommends the following:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Enable automated patches for your operating system and web browser.

Visit https://www.identitytheft.gov/Info-Lost-or-Stolen to learn more about protecting yourself after a data breach.