Steps To Take After a Data Breach to Protect Your Financial Accounts from Fraud

☐ **CHANGE YOUR PASSWORDS**
Use the security breach as an opportunity to change and strengthen your passwords, especially those related to online financial institution accounts.

☐ **TWO FACTOR AUTHENTICATION**
Enable two-factor authentication to log on to your bank account to prevent unauthorized access.

☐ **ACTIVATE BANK AND CREDIT CARD ACCOUNT ALERTS**
Most financial institutions offer a variety of text and e-mail alerts through online banking. You may also wish to ask your specific institution what they recommend to keep your accounts safe.

You can set up alerts for:

- When your profile or password is updated
- When an ATM withdrawal exceeds a certain amount
- When your account drops below a specific amount
- When purchases happen

☐ **MONITOR YOUR ACCOUNTS FOR UNUSUAL ACTIVITY**
Monitor your financial accounts for unusual activity and withdrawals. If you notice unauthorized activity, report it to your financial institution immediately.

☐ **CONSIDER PLACING A FRAUD ALERT OR FREEZE ON YOUR CREDIT REPORT**
A fraud alert informs creditors of possible identity theft or fraudulent activity within your credit file and requests that the credit grantor contact you prior to establishing any accounts in your name. A fraud alert lasts for one year, seven if requested and you meet specific requirements. A freeze locks your credit so that credit applications are denied until/unless you unfreeze your credit.

To place a fraud alert or freeze, contact any of the three credit reporting agencies:

- Equifax - 800.685.1111 or www.equifax.com
- Experian - 888.397.3742 or www.experian.com
- Transunion - 800.916.8800 or www.transunion.com

☐ **KEEP AN EYE OUT FOR UNUSUAL EMAILS, TEXT MESSAGES OR PHONE CALLS**
Keep an eye out for any unusual emails, text messages or phone calls, especially if they appear to come from the State of Washington or your financial institution. These could be social engineering attempts from hackers. Verify that the communication is legitimate by calling the organization back through an official phone number - one from the back of your credit or debit card or the agency's website directory.

☐ **CHECK YOUR CREDIT REPORT**
Obtain your free annual credit report from www.annualcreditreport.com. Check your credit report for errors or fraudulent activity. Report anything suspicious to the credit bureau and the organization that provided the information to the bureau. You can now check your report every week (through April 2021).

☐ **CONSIDER FILING YOUR TAXES EARLY**
Get a jump on your taxes to prevent a scammer from using your Social Security number to file a fraudulent return. If you've already filed, the IRS will flag the second return as suspicious. If you wait, yours could be the one that gets flagged.

Additional Resources

- State Auditor's Office Data Breach Website
- OFM Data Breach Website
- Recovering from Identity Theft
- How to Check Your Annual Credit Report
- How To Request A Security Freeze