COMMUNITY FIRST BANK | HFG TRUST

February 12, 2021

In January 2021, one of the Washington State Auditor's (SAO) software service providers, Accellion, issued a general announcement that it had experienced a security incident in December 2020. In mid-January, Accellion told SAO that the incident might have allowed unauthorized access to data temporarily stored in Accellion's servers. This incident might have exposed the sensitive data of Washingtonians to people who should not have had access to it.

SAO immediately took action to determine what information may have been affected. It includes:

- Personal information of people who filed for unemployment claims from Jan. 1 to Dec. 10, 2020. This group includes many state employees, as well as people whose identity was used to file for claims fraudulently in early 2020. SAO auditors were reviewing all claims data as part of an audit of that fraud incident. This affects about 1.6 million people. This information includes names, addresses, social security numbers, employer name and bank account numbers.
- Personal information of a smaller number of people, including data held by the Department of Children, Youth and Families
- Non-personal financial and other data from local governments and state agencies

The Washington State Department of Financial Institutions suggests you follow these steps to protect your account form fraud:

1. **Change your passwords**. Use the security branch as an opportunity to change and strengthen your passwords, especially those related to online financial institution accounts.
2. **Enable two-factor authentication**. Our online banking system already uses multi-factor authentication when logging in to your online banking account.
3. **Activate bank and credit card account alerts**. Community First Bank offers FREE products to help protect our clients from fraud. Notifi allows you to set up account alerts within the "Alert" tab in online banking. With **Card Valet®** you can manage your card from your mobile device.
4. **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.
5. **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

6. **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).
7. **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.

You can learn more about the security breach at the Washington State Auditor's website: www.sao.wa.gov/breach2021/.

As always, we are available should you have any questions.