10/1/2024

VIA Online Submission
Office of the Attorney General
1125 Washington Street SE
Olympia, WA 98504-0100

Re: Notification Pursuant to Wash. Rev. Code § 19.255.010 et seq.

Dear Attorney General Ferguson:

We are writing to notify you of recent security incidents experienced by FTV Employment Services and its affiliates ("FTV") that involved the personal information of approximately five hundred eighty-nine (589) Washington residents.

NATURE OF THE INCIDENT

In October and November 2023, FTV detected unusual activity within our network environment stemming from cybersecurity incidents involving two separate unauthorized third parties. Upon becoming aware of this issue, we immediately engaged leading external cybersecurity experts to assist us in thoroughly investigating the incidents. The investigation identified that the unauthorized third parties gained access to our network and viewed and acquired data between January 25, 2023 and November 6, 2023, at which point unauthorized access was terminated.

As part of our investigation, FTV initiated a detailed review of these files to determine whether personal information may have been present in the files affected during the incidents. Based on that review, which concluded on September 3, 2024, FTV determined that the files viewed and/or acquired contained personal information of Washington residents, including their full names and one or more of the following: date of birth, Social Security number, driver's license or state-issued identification card number, passport number, birth certificate number, financial account number, credit or debit card number, and/or health insurance information.

STEPS TAKEN IN RESPONSE TO THE INCIDENT

In November 2023, while its investigation was ongoing, FTV issued a precautionary notice about the incident and offered complimentary credit monitoring to all current employees. On October 3, 2024, FTV began notifying potentially affected Washington residents in accordance with applicable law. Enclosed is a template copy of the notification letter. FTV is providing the residents with 24 months of credit monitoring at no charge and has established a dedicated toll-free support line staffed to answer any questions individuals may have about the incidents or the services available to them. Within the notification, FTV also advises the affected residents on general best practices and safeguards to protect themselves from identity theft, including to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis, as well as the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports.

At FTV, protecting the privacy of personal information is a top priority. FTV remains fully committed to maintaining the privacy of personal information in our possession and has taken numerous

precautions to safeguard it. In response to the incidents, we worked closely with forensic consultants to investigate, contain, and eradicate the incidents, as well as to confirm the security of our network environment. FTV also notified federal law enforcement authorities of the incidents and enhanced our security monitoring capabilities and technical controls to further protect the privacy of personal information in the future.

If you have any questions concerning this notification, please contact our outside counsel Jennifer Urban at jurban@foley.com.

Sincerely,
FTV Employment Services

[redacted]
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
[redacted]

[redacted]

[redacted]

Dear [redacted]

At [redacted], we value and respect the privacy of your information, which is why we are writing to inform you about recent cybersecurity incidents that involved personal information. We want to provide you with further information about these incidents, the measures taken in response, and steps that you can take to help protect yourself.

WHAT HAPPENED?

In October and November 2023, we detected unusual activity within our network environment stemming from cybersecurity incidents involving two separate unauthorized third parties. Upon becoming aware of this issue, we immediately engaged leading external cybersecurity experts to assist us in thoroughly investigating the incidents. The investigation identified that the unauthorized third parties gained access to our network and viewed and acquired data between January 25, 2023 and November 6, 2023, at which point their access was terminated.

Based on our investigation and comprehensive review of potentially affected data, which concluded on September 3, 2024, we can confirm that certain personal information was involved in the incidents, and that your personal information [redacted] Once our comprehensive investigation was concluded, we worked to notify you as quickly as we could.

WHAT INFORMATION WAS INVOLVED?

Based on our subsequent investigation and comprehensive review of potentially affected data, we determined that the information involved in these incidents may have included your full name, and one or more of the following: date of birth, Social Security number, driver's license or state-issued identification card number, passport number, birth certificate number, financial account number, credit or debit card number, and/or health insurance information.

WHAT HAVE WE DONE IN RESPONSE?

In response to the incidents, we promptly implemented remedial and containment measures, working with leading external cybersecurity experts to assist with these efforts. In addition, we notified U.S. federal law enforcement and enhanced our security monitoring capabilities and technical controls. In addition to those efforts, we have arranged for you to enroll, at no cost to you, in a comprehensive 24-month credit monitoring and identity restoration service through Equifax. A description of this service and instructions on how to enroll can be found within the enclosed "Other Important Information" document included with this letter.

WHAT YOU CAN DO NOW?

Please review the enclosed "Other Important Information" document for further steps you can take to protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection, as well as details on how to place a fraud alert or a security freeze on your credit file. We recommend that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports for unauthorized activity. If you discover any suspicious or unusual activity on your accounts, promptly notify the financial institution or company with which your account is maintained.

FOR MORE INFORMATION.

For further information and assistance, please contact our dedicated incident response line at 833-251-9667 between 9 a.m. – 9 p.m. EST, Monday through Friday.

Sincerely,

[redacted]

OTHER IMPORTANT INFORMATION

Enroll in Credit Monitoring

Enter your Activation Code: [redacted]
Enrollment Deadline: [redacted]

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of [redacted] then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.
[2]Credit monitoring from Experian and TransUnion will take several days to begin. *[3]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.* *[4]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.* *[5]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.co* *[6]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the nationwide credit reporting agencies. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's (FTC) website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the national credit reporting agencies for the purpose of requesting a copy of your credit report and other general inquiries is provided below:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213
- **Innovis**, PO Box 1689, Pittsburgh, PA 15230-1689, www.innovis.com, 1-800-540-2505

Fraud Alert. You have the right to place an initial or extended "fraud alert" on your file at no cost by contacting any of the nationwide credit reporting agencies. Contact information for the national credit reporting agencies for the purposes of placing a fraud alert on your file is provided below. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For this reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

- **Equifax**, PO Box 105069, Atlanta, GA 30348-5069, www.equifax.com/personal/credit-report-services/credit-fraud-alerts, 1-800-525-6285
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts, 1-800-680-7289
- **Innovis Consumer Assistance**, PO Box 26, Pittsburgh, PA 15230-0026, hwww.innovis.com/personal/fraudActiveDutyAlerts, 1-800-540-2505

Security Freeze. You have the right to place, lift, or remove a "security freeze" on your credit report, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze separately with each of the consumer reporting agencies. To place a security freeze on your credit report, you may do so by contacting each of the consumer reporting agencies through the contact information below:

- **Equifax**, PO Box 105788, Atlanta, GA 30348-5788, www.equifax.com/personal/credit-report-services/credit-freeze, 1-800-298-0045
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html, 1-888-397-3742
- **TransUnion**, PO Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze, 1-888-909-8872
- **Innovis**, PO Box 26, Pittsburgh, PA 15230-0026, www.innovis.com/personal/securityFreeze, 1-800-540-2505

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and may provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338).

- ***For California residents***, you may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.
- ***For District of Columbia residents***, you may also obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.
- ***For Iowa Residents***, you are advised to report suspected incidents of identity theft to law enforcement or the Iowa Attorney General's Office at Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, telephone: 1-515-281-5926 or 1-888-777-4590.
- ***For Maryland residents***, you may obtain information about avoiding identity theft from the Maryland Office of the Attorney General at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.
- ***For New Mexico residents***, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
- ***For New York residents***, you may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General by calling 1-800-771-7755 or visiting https://ag.ny.gov; the New York State Police by calling 1-518-457-6721 or visiting https://troopers.ny.gov/; and/or the New York Department of State by calling 1-800-697-1220 or visiting https://www.dos.ny.gov.

- ***For North Carolina residents***, you may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.
- ***For Oregon Residents***, you are advised to report any suspected incidents of identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.
- ***For Rhode Island residents***, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to the incidents. There are approximately [redacted] Rhode Island residents that may be impacted by the incidents.