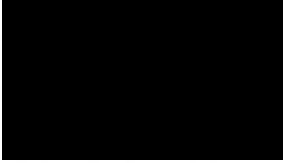




June 8, 2023



Dear [REDACTED],

We are writing to notify you of a recent incident that may affect the security of some of your personal information. Below we have provided you with information about the incident, our response thus far, and steps you can take to protect your information, should you wish to do so. The confidentiality, privacy, and security of our employees' information is one of our highest priorities. And while we do not currently have evidence that your information has been or will be misused, we nonetheless want to keep you informed.

**What Happened?** On February 27, 2023 we became aware that an employee had inadvertently been granted access to a document located on our network that contained sensitive information about our employees, and had accessed the document on one occasion that day. That same day, the employee reported to us that they had accessed the document. We immediately took steps to end the employee's access to the document and ensure that no other unauthorized individuals could access it. We also conducted a forensic investigation to determine if the document had been exported from our systems, and found no evidence that it had. However, in May of 2023 we received reports that the employee was reaching out to other employees to inform them that the employee had accessed their information. Consequently, we continued our investigation in order to determine if the employee had retained a copy of the document or any of the information in it. To date, although we have found no evidence that the document was exported from our systems, no evidence that the employee shared the document or any of the information in it with anyone else, and no evidence that the information in the document has been or will be misused, we have not been able to definitively confirm that the employee (who no longer works for the company) did not retain a copy of some or all of the information in the document. We have also contacted law enforcement to make them aware of the situation. In late May, we concluded our investigation, and we are notifying you because our review determined that your personal information was included in the document at issue.

**What Information Was Involved?** The following information about you was present in the document that the former employee accessed: your name, social security number, phone number, date of birth, mailing address, gender, hire date, earnings rate and federal filing status.



**What We Are Doing?** We take this incident and the security of our employees' information in our care very seriously. In addition to the steps described above, we are undertaking a review of existing practices to make sure that a similar incident does not happen again and reminding staff to notify us immediately if they become aware that they or anyone else has obtained access to sensitive documents or information to which they should not have access.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your accounts and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find more information about how to place a fraud alert and/or credit freeze on your accounts with the three primary credit reporting bureaus, should you wish to do so.

We, in conjunction with our legal counsel, will continue to work hard to address this matter and strengthen the security of our systems to help prevent further incidents. We sincerely apologize for any inconvenience this incident causes you, and we will keep you informed if any new information impacting you comes to light.

If you have any questions, please contact myself or [REDACTED] at [REDACTED] or via email at [REDACTED] and/or [REDACTED]

Sincerely,

A handwritten signature in blue ink that reads "Kim Veilleux".

Kim Veilleux  
Controller/HR Manager



## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
1. Social Security number;
2. Date of birth;
3. Addresses for the prior two to five years;
4. Proof of current address, such as a current utility bill or telephone bill;
5. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
6. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.



Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

**Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.