



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 18, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Grafton Apparel Ltd. ("Grafton") located at 115 Applewood Crescent, Vaughan, ON L4K 5C1, Canada, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) Maryland resident. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Grafton does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

Grafton learned on December 13, 2021 that its IT systems were accessed by an unauthorized individual in November and December 2021. When this was discovered, Grafton immediately took steps to secure its systems and launched an investigation with the assistance of leading outside cybersecurity experts. The investigation identified that the cause of the incident was a third-party software vulnerability, which has since been addressed. Grafton has identified that some personal information, almost exclusively about employees and former employees, was taken from its systems without authorization during the incident. The categories of information potentially involved in the incident vary by individual.

The information that could have been subject to unauthorized access for the Maryland resident include name and taxpayer identification number.

Notice to Maryland Resident

On January 19, 2022, Grafton will provide written notice of this incident to all potentially affected individuals which includes approximately one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Grafton moved quickly to investigate and respond to the incident, assess the security of its systems, and identify and notify potentially affected individuals. Grafton is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for 2 years through Equifax at no cost to the individuals.

Additionally, Grafton is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Grafton is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

A handwritten signature in black ink, appearing to read "Rebecca Jones", is written over a light gray rectangular background.

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/jlm
Enclosure

EXHIBIT A

[Grafton Letterhead]

January [●], 2022

Dear <<First Name>> <<Last Name>>:

We recently experienced a cybersecurity incident at Grafton. As described below, we have identified that some of the information that we hold was involved in this incident and that this may have included information that we hold about you. We are writing to inform you about this incident and steps you can take to protect your information.

What happened?

We have learned that some of our IT systems were accessed by an unauthorized individual in November and December 2021. When we learned of this incident, we immediately took steps to secure our systems and we launched an investigation with the assistance of leading outside cybersecurity experts. We also immediately notified the appropriate authorities.

We have identified that some information was taken from our systems without authorization during the incident. We have taken steps to secure the deletion of the information that was taken. While we have no evidence of any misuse of the information, as the information may have included some of your personal information, we are writing to notify you about this incident.

What information was potentially involved?

The categories of information potentially involved vary by individual and may include the following types of information which Grafton held in connection with your employment at Grafton: name and taxpayer identification number.

What are we doing?

We are taking this matter seriously and have reported it to law enforcement and relevant privacy commissioners. We are also contacting you to notify you about this incident and to provide the enclosed information about steps you can take to protect yourself, including credit monitoring as described below.

We are offering you a premier credit monitoring and identity theft product, the Equifax Complete Premier Plan, for two years at no charge to you, including:

- Annual access to your 3-bureau credit report and VantageScore credit scores in the US;
- Daily access to your US Equifax credit report and 1-bureau VantageScore credit score;
- 3-bureau credit monitoring with email notifications of key changes to your US credit reports;

- WebScan notifications 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, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock;
- 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 US\$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft; and
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.¹

Signing up for the free credit monitoring and identity protection services will take about five minutes. To activate your account, visit <https://www.equifax.com/activate> and use your unique activation code [XXXXXX] before [date].

Enter your unique activation code, then click “Submit”

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 Summary information only. For the full details of the elements of the Equifax Complete Premier Plan (United States), please contact Equifax as indicated.

No credit card is required. We encourage you to activate the services as soon as possible. For more information on this plan, please contact Equifax at (866) 243-0734 from 8 a.m. to 3 a.m. (ET) Monday to Sunday.

We deeply regret that this incident occurred and are committed to working to prevent these types of events from occurring in the future. If you have any questions about this incident, please contact me at michelle.carter@griftonapparel.com. You may also write to Grafton at 115 Applewood Crescent, Concord, Ontario L4K 5C1 or call (416) 780-2144.

Yours truly,

Michelle Carter
Director, Human Resources

STEPS YOU CAN TAKE TO FURTHER 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 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 1-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.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. 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:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	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, DC 20580; 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. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.