
NOTICE OF DATA BREACH

June, 2020

There has been a recent incident at Masterfeeds, Inc. (“**Masterfeeds**”) that may have affected the security of some of your personal information. While we do not have evidence of actual access to your individual and we are unaware of any actual misuse of your information, we are providing this notice which contains information about the incident, our response to the incident, steps you can take and resources available to help protect your information from possible misuse, should you feel it appropriate to do so. We have also provided contact details for the person who you should contact if you would like to obtain further information about the breach.

We are providing notice of the incident via our website, as well as to certain privacy commissioners. We have also provided individual notifications to customers and employees whose contact details are available to us.

DETAILS OF INCIDENT

On March 13, 2020, Masterfeeds became aware of unusual activity on its systems. Masterfeeds detected malware on its devices and that some systems were unavailable. Masterfeeds immediately commenced an investigation, with the aid of forensic experts, to confirm the nature and scope of the activity. Masterfeeds determined that an unauthorized actor potentially had access to certain servers and devices, and through such potential access, may have accessed certain personal information that was stored on the servers and devices. We are unable to confirm whether the information was subject to unauthorized access or acquisition, but because the possibility exists, we are providing this notification to you. We are unaware of any actual misuse of the information and we have no direct evidence that personal information was actually accessed, impacted or misused. We believe the breach took place from approximately March 12, 2020 to March 14, 2020.

PERSONAL INFORMATION INVOLVED

While we have no evidence of actual access or acquisition, we have determined that the following information related to employees and former employees of Masterfeeds, Pharm Barn and Cowtown was contained on the affected servers and devices that may have been accessed: name, date of birth and SIN.

STEPS WE HAVE TAKEN

We take this incident and the security of personal information very seriously. Upon discovering unusual activity in our system, we immediately took steps to remediate our network and conducted an investigation to determine the nature and scope of the incident. Additionally, while

we have safeguards in place to protect data in our care, we are working to review and enhance these protections as part of our ongoing commitment to data security. To reduce the risk of harm in the future, Masterfeeds is taking steps to migrate servers to more secure applications and services with additional security controls in place.

Masterfeeds is offering you access to 12 months of complimentary credit monitoring and identity theft restoration services through the Equifax Complete™ Premier Plan. Please contact us for details on how to access this plan and enroll in these services. You must activate your account before September 30, 2020.

STEPS YOU CAN TAKE

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. As noted above, we encourage you to make use of the Equifax Complete™ Premier Plan for complimentary credit monitoring services.

We encourage that you take the following steps to minimize your risk:

- Contact your bank and credit card companies.
Ask that an alert be placed on your account.
- Pay attention to your credit card and bank statements.
Keep records of recent purchases, payments and financial transactions.
Watch your billing cycles closely and be suspicious of any missing account statements or suspicious transactions.
- Regularly (at least annually) check your credit report.
- Place a fraud warning or fraud alert on your credit report (as detailed below).
- Use new, unique, hard-to-guess passwords for your online accounts and change them often.

For resources and information on how to protect yourself, visit the following webpages:

- Royal Canadian Mounted Police's Identity Theft and Identity Fraud Victim Assistance Guide: <http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm>.
- Canadian Anti-Fraud Centre: <https://www.antifraudcentre-centreantifraude.ca/index-eng.htm>.

CONTACTING US

If you have additional questions or concerns, please contact our privacy officer at 519-685-4300, ext. 1231 or smaclure@masterfeeds.com

We sincerely regret any inconvenience this incident may cause you. We remain committed to safeguarding the information in our care and will continue to take steps to enhance the security of our systems and complying with applicable privacy legislation.