[Masterfeeds Letterhead]

[First Name] [Last Name]
[Full Address]

Re: Notice of Data Breach

Dear [First Name],

Masterfeeds, Inc. ("**Masterfeeds**") writes to inform you of a recent incident that may have affected the security of some of your personal information. While we are unaware of any actual misuse of your information and we have no direct evidence that personal information was actually accessed, impacted or misused, we are providing you this notification 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.

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. 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 you was contained on the affected servers and devices: SIN, bank account information, driver's license, passport number and PPSA information.

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.

As an additional precaution, Masterfeeds is offering you access to 12 months of complimentary credit monitoring services through Equifax. Details of this offer and instructions on how to enroll in these services are enclosed with this letter. To activate your account visit http://myservices.equifax.com/efx1_bresngis and use your unique activation code **<XXXXXXXX>** before **September 30, 2020**.

Steps You Can Take

Please review the enclosed "Steps You Can Take to Protect Your Personal Information," which contains information on what you can do to help protect against possible misuse of your information. 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 Plan for complimentary credit monitoring services.

Contacting Us

If you have additional questions or concerns, please contact me at 519-685-4300, ext. 231 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.

Sincerely,

MASTERFEEDS, INC.

Sylvia MacLure
Director of Human Resources

Steps You Can Take to Protect Your Personal Information

Protect Yourself

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. 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.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.

Credit Monitoring

See the below details on the Equifax Plan.

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. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;

4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Enter your Activation Code: <INSERT ACTIVATION CODE>

Enrollment Deadline: September 30, 2020

Product Information

Equifax® Credit Watch™ Gold with WebDetect Features

- Equifax® credit file monitoring and alerts to key changes to your Equifax credit report
- Wireless alerts (available online only) Data charges may apply.
- Access to your Equifax credit report
- Internet Scanning[1] Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Automatic Fraud Alerts[2] with a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Up to $25,000 Identity Theft Insurance[3]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to http://myservices.equifax.com/efx1_bresngis

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.

2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.

4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

1 Internet scanning, will scan for your Social Security number (if you choose to), up to 5 bank account numbers, up to 6 credit/debit card numbers you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to 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 Internet scanning is able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

2 The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

3 Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

EPC_CWA_227871_01