MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

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

October 28, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent JM Bullion, Inc. and Provident Metals Corp, a wholly owned subsidiary of JM Bullion, Inc., (hereinafter "JM Bullion") located at 11700 Preston Road Ste 660153 Dallas, Texas 75230, and are writing to notify your office of an incident that may affect the security of some personal information relating to one hundred seventy (170) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, JM Bullion does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 6, 2020, JM Bullion was alerted to suspicious activity on its website. JM Bullion immediately began an investigation, with the assistance of a third-party forensic specialist, to assess the nature and scope of the incident. Through an investigation, it was determined that malicious code was present on www.jmbullion.com from February 18, 2020 to July 17, 2020 and on www.providentmetals.com from January 1, 2020 to July 17, 2020 which had the ability to capture customer information entered into the websites in limited scenarios while making a purchase. These scenarios represented a small portion of the transactions processed on the websites during the impacted time frame. The malicious code found was permanently removed from the websites on July 17, 2020. JM Bullion provided notice to anyone who made a purchase on the websites during this time frame. The information that could have been subject to unauthorized

access includes name, address, and payment card information (account number, card expiration date and security code).

Notice to New Hampshire Residents

On or about October 28, 2020, JM Bullion provided written notice of this incident to all affected individuals, which includes one hundred seventy (170) New Hampshire residents. 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, JM Bullion moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially affected individuals. JM Bullion immediately reported this to its payment card processor and the major credit card brands and has been working with them since July. JM Bullion is also working to implement additional safeguards and training to its employees.

Additionally, JM Bullion is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. JM Bullion 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. JM Bullion is also reporting this matter to regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD:pls
Enclosure

EXHIBIT A

JM BULLION
www.jmbullion.com
8350 North Central Expressway, Suite 250, Dallas, Texas 75206

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

RE: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

JM Bullion, Inc. ("JM Bullion") is writing to inform you of an incident that may affect the security of some of your personal information. Through an investigation, we recently determined that malicious code was present on our website which had the ability to capture customer information entered into the website in limited scenarios while making a purchase. JM Bullion is advising you of our investigation and the steps we have taken in response to this incident. We also are providing you with information regarding steps you may take to help protect your personal information should you feel it is appropriate to do so.

What Happened? On July 6, 2020, JM Bullion was alerted to suspicious activity on its website. JM Bullion immediately began an investigation, with the assistance of a third-party forensic specialist, to assess the nature and scope of the incident. Through an investigation, it was determined that malicious code was present on the website from February 18, 2020 to July 17, 2020, which had the ability to capture customer information entered into the website in limited scenarios while making a purchase. These scenarios represented a small portion of the transactions processed on JM Bullion's website during the impacted time frame. You are receiving a notice because you made a purchase on the website during this time frame and your payment card information could be at risk. The malicious code found was permanently removed from the website on July 17, 2020.

What Information Was Involved? JM Bullion determined the type of information potentially impacted by this incident includes your name, address, and payment card information (account number, card expiration date and security code).

What We Are Doing. JM Bullion takes the security of personal information in its care very seriously. In response to this incident, JM Bullion notified law enforcement, our card processor, and the credit card brands, and continues to work with them as needed. We also reviewed our internal procedures and implemented additional safeguards on our website to protect customer information in our possession.

What Can You Do? You may review the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud* for additional information on how to better protect your personal information.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-???-???-????, Monday through Friday from 8:00 am to 5:30 pm Central Time.

We sincerely apologize for this incident and regret any concern or inconvenience this has caused you.

Sincerely,

Michael Wittmeyer
Chief Executive Officer
JM Bullion, Inc.

Steps You Can Take to Help Protect Against Identity Theft and Fraud

The confidentiality, privacy and security of your personal information is one of our highest priorities. That is why we are sharing these steps you may take to protect your identity and uncover any fraudulent activity on your accounts.

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, as set forth below, 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 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	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. 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, 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.); and
7. If you are a victim of identity theft, 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 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You may 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 may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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 their information has been misused to file a complaint with them. You may 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 in order to file a report with law enforcement for identity theft, you likely will need to provide some proof that you have been a victim. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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 North Carolina residents, the Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Rhode Island residents, the Attorney General may be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 65 Rhode Island residents may be impacted by this incident.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.

PROVIDENT
METALS

6125 Luther Lane, #465 Dallas, TX 75225

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

RE: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Provident Metals Corp ("Provident Metals") is writing to inform you of an incident that may affect the security of some of your personal information. Through an investigation, we recently determined that malicious code was present on our website which had the ability to capture customer information entered into the website in limited scenarios while making a purchase. Provident Metals is advising you of our investigation and the steps we have taken in response to this incident. We also are providing you with information regarding steps you may take to help protect your personal information should you feel it is appropriate to do so.

What Happened? On July 6, 2020, Provident Metals was alerted to suspicious activity on its website. Provident Metals immediately began an investigation, with the assistance of a third-party forensic specialist, to assess the nature and scope of the incident. Through an investigation, it was determined that malicious code was present on the website from January 1, 2020 to July 17, 2020, which had the ability to capture customer information entered into the website in limited scenarios while making a purchase. These scenarios represented a small portion of the transactions processed on Provident Metals' website during the impacted time frame. You are receiving a notice because you made a purchase on the website during this time frame and your payment card information could be at risk. The malicious code found was permanently removed from the website on July 17, 2020.

What Information Was Involved? Provident Metals determined the type of information potentially impacted by this incident includes your name, address, and payment card information (account number, card expiration date, and security code).

What We Are Doing. Provident Metals takes the security of personal information in its care very seriously. In response to this incident, Provident Metals notified law enforcement, our card processor, and the credit card brands, and continues to work with them as needed. We also reviewed our internal procedures and implemented additional safeguards on our website to protect customer information in our possession.

What Can You Do? You may review the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud* for additional information on how to better protect your personal information.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-???-???-????, Monday through Friday from 8:00 am to 5:30 pm Central Time.

We sincerely apologize for this incident and regret any concern or inconvenience this has caused you.

Sincerely,

Michael Wittmeyer
Chief Executive Officer
Provident Metals Corp

Steps You Can Take to Help Protect Against Identity Theft and Fraud

The confidentiality, privacy, and security of your personal information is one of our highest priorities. That is why we are sharing these steps you may take to protect your identity and uncover any fraudulent activity on your accounts.

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, as set forth below, 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 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	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. 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, 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.); and
7. If you are a victim of identity theft, 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 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You may 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 may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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 their information has been misused to file a complaint with them. You may 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 in order to file a report with law enforcement for identity theft, you likely will need to provide some proof that you have been a victim. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your 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 North Carolina residents, the Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Rhode Island residents, the Attorney General may be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 8 Rhode Island residents may be impacted by this incident.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.