

Kennedys

BY Certified Mail, Return Receipt Requested

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6706
Joshua.Mooney@kennedyslaw.com
March 8, 2022

Re: Notice of Cybersecurity Incident

Dear Sir/Madam:

We write on behalf of Absolute Results Productions Ltd. ("Absolute Results"), a Canadian company, and its affiliate Absolute Results Technologies USA Inc. about a cyber incident discovered on October 8, 2021. Absolute Results suffered the incident. Its investigation now has determined that the incident potentially impacted two Maryland residents, former employees/contractors of Absolute Results Technologies.

Upon discovering the attack, Absolute Results undertook immediate steps to re-secure its systems, including quarantining all of its servers and machines, restoring its servers and machines to pre-virus conditions, and by working with outside cybersecurity counsel and experts. Absolute Results also began a prompt investigation, which confirmed that an unauthorized actor had gained access to a portion of its network and through the use of malware (a virus), encrypted network files. The investigation also revealed that the actor accessed and copied some files, and that some or all of these copied files have been or may be posted on the dark web. The type of personal information potentially accessed includes names, dates of birth, addresses, driver's license numbers, passport numbers, bank account numbers, and social security numbers. It later determined that the personal information of two Maryland residents potentially was impacted.

Absolute Results is in the process of notifying impacted individuals - employees and contractors - by e-mail and (for US residents) by mail. Notice to Maryland residents will be provided in 7-10 business days.

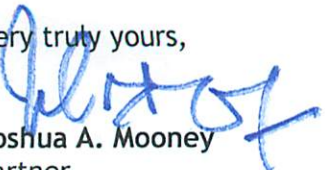
Kennedys is a trading name of Kennedys CMK LLP. Kennedys Law LLP, a UK Limited Liability Partnership, is a partner of Kennedys CMK LLP

Kennedys offices, associations and cooperations: Argentina, Australia, Belgium, Bermuda, Brazil, Canada, Chile, China, Colombia, Denmark, Dominican Republic, England and Wales, France, Guatemala, Hong Kong, India, Ireland, Israel, Italy, Mexico, New Zealand, Northern Ireland, Norway, Oman, Pakistan, Panama, Peru, Poland, Portugal, Puerto Rico, Russian Federation, Scotland, Singapore, Spain, Sweden, Thailand, United Arab Emirates, United States of America.

Office of the Maryland Attorney General

If your office has further questions, I may be reached at the email address or telephone number above. Thank you.

Very truly yours,



Joshua A. Mooney
Partner
For Kennedys

Enclosure



BY MAIL

March __, 2022

<<name>>

<<address>>

<<city>>, <<state>> <<ZIP Code>>

Re: Notice of Data Breach

Dear <<First Name>>,

As you may know, Absolute Results Productions Ltd. ("Absolute Results") recently experienced a cybersecurity incident involving data held by it of its affiliate, Absolute Results Technologies USA Inc. As soon as this was discovered, we acted quickly to secure the affected systems and commenced an investigation with the assistance of outside cybersecurity experts. This letter is to inform you that in our investigation, we learned that the incident may have impacted some personal information that you provided to us. This notice provides you with information about the incident, our response, and additional steps you may take to protect your information, should you determine it is appropriate to do so. This notice was not delayed by law enforcement.

What Happened?

On October 8, 2021, we discovered that our systems were accessed by an unauthorized party. When we discovered this incident, we took immediate steps to secure our systems by quarantining all servers and machines, restoring our servers and machines to pre-virus conditions, and working with outside cybersecurity counsel and experts to further address and contain the incident.

We also began a prompt investigation. To date, the investigation has confirmed that an unauthorized actor gained access to a portion of our network and through the use of malware (a virus), encrypted network files. The investigation also revealed that the actor accessed and copied some data files, and that some or all of these copied data files have been or may be posted on the dark web. The investigation has not found evidence of other misuse. While at this time we have been unable to identify exactly what data files have been copied and may be posted on the dark web, out of an abundance of caution, we are treating all of the data on our impacted servers and machines as potentially copied and acquired. That universe of data may contain personal information about you.



What Type of Information Was Involved

The Absolute Results systems impacted potentially contained the following types of personal information: name, date of birth, address, driver's license number, passport number, bank account information, social security numbers, and any other personal information that you provided to Absolute Results.

What We Are Doing

We are reaching out to notify you about the cybersecurity incident and to provide information below regarding steps you can take to remain vigilant and protect yourself, including offering a 24-month subscription to credit monitoring, as described below. We have also reported this incident to law enforcement, the Offices of various State Attorneys General, and other relevant authorities pursuant to applicable law.

Additionally, we are offering you a premier credit monitoring and identity theft product, the Equifax Complete Premier, for two years at no charge to you, which includes:

- Annual access to your 3-bureau credit report and VantageScore credit scores;
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score;
- 3-bureau credit monitoring with email notifications of key changes to your 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 \$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 www.equifax.com/activate and use your unique

¹ Summary information only. For the full details of the elements of the Equifax Complete Premier, please contact Equifax as indicated on the enclosed document entitled "Steps You Can Take To Further Protect Your Information".



activation code: <<activation code>> before May 31, 2022. We encourage you to activate the services as soon as possible.

What You Can Do

We also have enclosed an addendum to this letter ("**Addendum A - What You Can Do**") to provide you with further information as to what you may do to protect against fraud.

Further Information

We deeply regret that this incident occurred and are working to prevent these types of events from occurring in the future. If you have any questions about this incident, you may contact me by email at slopez@absoluteresults.com or by phone at (604) 774-3062.

Sincerely,

A handwritten signature in black ink, appearing to be 'SL' with a flourish.

Sheila Lopez

Data Privacy and Compliance Manager



Addendum A - What You Can Do

Absolute Results encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity. You may also review and consider the information and resources outlined in the below, which includes information regarding enrollment for the complimentary credit monitoring and identity restoration services. You have the right to file a report with local police and obtain a copy.

You are entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion (listed below). 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.

You also 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, you may 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. you cannot be charged to place or lift a credit freeze on your credit report.

The contact information for the three credit reporting agencies are:

Equifax (<https://www.equifax.com/personal/credit-report-services/>), tel.: 1-888-298-0045, addresses: Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069, Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788;

Experian (<https://www.experian.com/help/>), tel.: 1-888-397-3742, addresses: Experian Fraud Alert, P.O. Box 9554, Allen, TX



75013, Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013;
and

TransUnion (<https://www.transunion.com/credit-help>), tel.: 1-833-395-6938, addresses: TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016, TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094.

To request a security freeze, you will need to provide the following (1) your full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security number; (3) date of birth; (4) address(es) 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, 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.

In addition, you may further educate yourself regarding identity theft, fraud alerts, credit freezes, and steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission ("FTC"), or your state Attorney General. The contact information for the FTC is as follows:

FTC: (www.identitytheft.gov), tel.: 1-877-ID-THEFT (1-877-438-4338) & TTY: 1-866-653-4261, address: 600 Pennsylvania Avenue NW, Washington, DC 20580.

The Federal Trade Commission 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.

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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

If you believe you are the victim of identity theft or fraud, or have reason to believe your personal information has been misused, you should immediately:

1. **File a complaint with the police.** Ask for the case reference number and the officer's name and telephone number. If you choose, you may obtain a copy of the police report.



2. Inform your bank and creditors by phone and in writing about any irregularities.
3. Report any irregularities in your mail delivery, for example, opened envelopes, missing financial statements or documents.
4. Alert the government tax agency, where you may be able to place an alert.
5. Take any other appropriate steps to reduce or eliminate the impact of identity theft, fraud, or misuse.