



Julie M. Hess, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, 36th Floor
Philadelphia, Pennsylvania 19103
JHess@constangy.com
Mobile: 610.416.9236

March 3, 2023

VIA ELECTRONIC SUBMISSION

Attorney General Anthony Brown
Maryland Attorney General's Office
Consumer Protection Division
200 St. Paul Place
Baltimore, Maryland 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown,

We represent Exponential Interactive, Inc. dba VDX.tv ("Exponential"), a global provider of advertising intelligence and digital media solutions, in connection with the data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland data breach notification law.

Nature of the Security Incident.

On September 12, 2022, Exponential discovered malware on its system. In response, Exponential took immediate steps to secure its network and promptly launched an investigation. In so doing, Exponential engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been impacted. The investigation revealed that some files may have been potentially accessed without authorization. On January 13, 2023, Exponential discovered that some of those files contained certain employee-related information. To effectuate notification, Exponential then took steps to identify those individuals and their current mailing addresses, which was completed on February 15, 2023. The data elements impacted by this incident include name and Social Security number.

Number of Maryland Residents Affected.

Exponential notified 12 Maryland residents of this incident via first-class U.S. Mail on March 3, 2023. A sample copy of the notification letter is attached hereto.

Steps Taken Relating to the Incident.

Exponential has taken steps to prevent similar incidents from occurring in the future. Those steps have included working with leading cybersecurity experts to enhance the security of its network. Exponential is also offering the potentially impacted individuals credit and identity monitoring at no cost through Kroll, to ensure their information is protected.

Contact Information.

Exponential remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me directly at JHess@constangy.com.

Best regards,

/s/ Julie M. Hess

Julie M. Hess
Constangy, Brooks, Smith & Prophete LLP

Enclosure: Sample Consumer Notification Letter



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

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

<<b2b_text_1(NOTICE OF DATA BREACH / NOTICE OF SECURITY INCIDENT)>>

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

Exponential Interactive d/b/a vdx.tv ("Exponential") is writing to inform you of a data security incident that may have involved your personal information. Exponential takes the privacy and security of your information very seriously. Therefore, we are writing to inform you about the incident and advise you of certain steps you can take to help protect your personal information, including activating the free identity monitoring services we are offering to you.

What Happened. On September 12, 2022, Exponential discovered malware on its system. We immediately launched an investigation and took steps to secure our network. We also engaged an independent digital forensics firm to assist with the investigation and determine what happened and whether sensitive information may have been accessed or acquired during the incident. Through the course of our investigation, Exponential learned that some files may have potentially been accessed without authorization. On January 13, 2023, we discovered some of those files contained certain employee-related information. A thorough review of the types of personal information potentially impacted, identification of potentially impacted individuals, and verification of current mailing addresses for those individuals, was completed on February 15, 2023.

Notably, we have no evidence of the misuse or attempted misuse of any potentially impacted personal information.

What Information Was Involved. The files that may have been accessed contained your <<b2b_text_2(name, data elements)>>.

What Are We Doing. As soon as Exponential discovered this incident, we took the steps described above. In addition, Exponential implemented enhanced safeguards to minimize the chance that an incident like this could occur in the future. Furthermore, out of an abundance of caution, we are providing you with information about steps that you can take to help protect your personal information and offering you complimentary identity monitoring services through Kroll, a data breach and recovery services expert. These services include 12 months of Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. With these services, Kroll will help to resolve issues if your identity is compromised.

What You Can Do: Please read the recommendations included with this letter which you can follow to help protect your personal information. Exponential also strongly encourages you to activate the complimentary identity monitoring services being offered to you through Kroll.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

Exponential Interactive, Inc. dba [VDX.tv](https://vdx.tv)
2340 Powell Street, #378
Emeryville, CA 94608

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

For More Information: If you have questions or need assistance, please call Kroll at (866) 674-4330 from 6:00 a.m. to 3:30 p.m. Pacific Time, Monday through Friday, excluding U.S. holidays. Please have your membership number ready.

Helping protect your information is important to us. Please know that we take this incident very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Tim Sleath', with a stylized flourish at the end.

Tim Sleath,
DPO and Head of Product Strategy and Enterprise IT

Steps You Can Take to HELP Protect Your PERSONAL Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft 1-877-438-4338

Maryland Attorney

General 200 St. Paul
Place Baltimore, MD
21202 oag.state.md.us 1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney

General 150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov> 1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and

your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.