IDC

140 Kendrick Street
Building B
Needham, MA 02494

Phone: +1 508 872 8200
Web: idc.com

April 15, 2022

BY U.S. MAIL

Office of the Attorney General
Consumer Protection Bureau
33 Capitol St.
Concord, NH 03301

To Whom It May Concern:

On behalf of IDC Research, Inc. ("IDC"), and pursuant to N.H. Rev. Stat. § 359-C:20(I)(B), this letter provides notice of a cybersecurity incident. IDC provides market intelligence and consulting services globally for the information technology, telecommunications, and consumer technology sectors. IDC's principal place of business is located at 140 Kendrick Street Building B, Needham, MA 02494.

On February 16, 2022, IDC experienced a network intrusion for the purpose of attempting to obtain a ransom payment. On February 15, 2022, IDC identified indications of potential unauthorized access to its IT systems that prompted further investigation. After confirming that there was an unauthorized access, IDC initiated its incident response effort with the assistance of outside cybersecurity experts. During its incident response effort, IDC identified file encryption appearing on a device it was actively viewing, allowing it and the outside cybersecurity experts to rapidly identify and greatly limit the spread of the attack by shutting down servers and VPNs. IDC proceeded with a thorough investigation, with the support of outside cybersecurity experts, and notified law enforcement. IDC has since restored the few affected systems from backup and never interacted with the threat actor. There has been no observed malicious activity in IDC's environment since February 17, 2022, and IDC has found no indication that the unauthorized third party remains in IDC's network or otherwise has access to it.

While IDC identified evidence of attempted data exfiltration by the unauthorized third party, IDC currently has no evidence confirming that the unauthorized third party's attempt was successful. Targeted online monitoring commissioned by IDC has not revealed any indications that IDC's data has been or is potentially going to be published, or has been acquired by another unauthorized third party. To date, IDC has identified five New Hampshire residents whose personal information may have been affected by the incident.

Depending on the individual, the categories of personal information that may have been affected included the following: name, date of birth, Social Security number, bank account information, address, email address, and phone number. IDC is not aware of any

cases of identity theft, fraud, or financial losses to individuals stemming from this incident.

IDC anticipates sending formal notice to these individuals on April 18, 2022 via U.S. mail. A sample of the notification letter is enclosed. As stated in the attached sample notice, IDC is offering to provide individuals 24 months of free identity theft and credit monitoring services through Equifax to individuals whose personal information may have been affected.

Efforts to further secure IDC's systems are ongoing. IDC promptly undertook measures to enhance its security and improve its capabilities to detect cyber threats and avoid unauthorized activity, including resetting privileged passwords and utilizing enhanced network monitoring software.

Given that its investigation and review is now complete, IDC does not anticipate making any further updates to your office. However, it will of course do so should any new material facts arise. IDC takes the protection of personal information seriously and is committed to answering any questions that your office may have. Please do not hesitate to contact me at 508-935-4076 or Renuka_Drummond@idg.com.

***

In accordance with N.H. Rev. Stat. § 91-A:5(IV), (XI), and/or other applicable laws and regulations, IDC requests that confidential treatment be provided to this letter and to any notes, memoranda, or other records created by or at the direction of the Office of the Attorney General, its officers, or staff members that reflect, refer to, or relate to this letter (the "Confidential Materials"). IDC also requests that Confidential Materials be kept in a non-public file and that only staff of your Office have access to them. Should your Office receive any request for the Confidential Materials pursuant to the New Hampshire Right to Know Law or otherwise, IDC requests that the undersigned be immediately notified of such request and be furnished a copy of all written materials pertaining to such request.

Respectfully yours,

Renuka Drummond
Corporate Secretary and Group General Counsel
IDC Research, Inc.

Enclosure

140 Kendrick Street
Building B
Needham, MA 02494
Phone: +1.508.872.8200
Web: idc.com

April 18, 2022

[redacted]

[redacted]

NOTICE OF SECURITY INCIDENT

Dear [redacted],

We are writing regarding a cybersecurity incident that occurred at IDC Research, Inc. ("IDC"). We want to make clear at the outset that keeping personal data safe and secure is very important to us, and we deeply regret that this incident occurred.

WHAT HAPPENED?

On February 16, 2022, we detected that an unauthorized third party gained remote access to certain portions of IDC's network in an effort to disrupt our operations. We promptly began to investigate the incident with the support of outside cybersecurity experts. We believe the unauthorized third party first gained remote access to our network on or about February 14, 2022. Based on our investigation, we identified an attempt by the unauthorized third party to acquire some of IDC's internal company data, which included personal information of certain individuals, including certain of your personal information, but we do not have evidence confirming that this attempt was successful.

WHAT INFORMATION WAS INVOLVED?

The types of personal information that the unauthorized third party may have accessed or obtained included your [redacted]. However, IDC currently has no evidence confirming that your information has actually been removed from its system or misused. Targeted online monitoring commissioned by IDC has not revealed any indications that IDC's data (including personal data belonging to you or other individuals) has been or is potentially going to be published, or has been acquired by another unauthorized third party.

WHAT WE ARE DOING

We took prompt steps to address this incident, including contacting law enforcement and engaging outside cybersecurity experts to help remediate and ensure the ongoing security of our systems. As part of our ongoing efforts to ensure the security of our systems, we have enhanced cybersecurity protections throughout our environment and will continue to improve our security based on what we learn.

In an abundance of caution, we have secured the services of Equifax to provide identity and credit monitoring services at no cost to you for two years. Below please find information on signing up for a complimentary two-year membership to Equifax Complete Premier which helps detect misuse of your personal information and provides you with identity protection focused on identification and resolution of identity theft.

April 18, 2022
Activation Code: [redacted]
Expiration Date: **July 31, 2022**

Equifax Complete Premier

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores.
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score.
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports.
- WebScan notifications[3] 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[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock.[5]
- 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.[6]
- 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 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Credit monitoring from Experian and TransUnion will take several days to begin.

3 WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of 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 we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

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

5 Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

6 The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Enrollment Instructions

To sign up online for online delivery, go to www.equifax.com/activate

Enter your unique Activation Code of [redacted] then click "Submit" and follow these 4 steps:

1. **Register:** Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:** Complete the form with your email address, create a password, and accept the Terms of Use.
3. **Verify Identity:** To enroll in your product, the system will ask you to complete an identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Please click the "View My Product" button to access the product features.

You need to activate your membership in order to receive your benefits, and must do so no later than **July 31, 2022. Your Activation Code will not work after this date.**

WHAT YOU CAN DO

We strongly encourage you to contact Equifax and take advantage of the credit monitoring and identity theft protection services we are providing to you free of charge. Remain vigilant and carefully review your accounts for any suspicious activity.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained and any relevant government agency, such as IRS, SSA, or state DMV, as applicable.

If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

We take our responsibility to protect your information extremely seriously, and are very sorry that this incident has occurred. If you have any questions regarding this incident or the services available to you, please contact us at privacy@idc.com.

Sincerely,

Renuka Drummond
General Counsel
International Data Group

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements 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 incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.ftc.gov/features/feature-0014-identity-theft
1-877-IDTHEFT (438-4338)
1-866-653-4261 (TTY)

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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian:**	**TransUnion:**
equifax.com	experian.com	transunion.com
www.equifax.com/CreditReportAssistance	www.experian.com/fraudalert	www.transunion.com/fraud
P.O. Box 740241	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
866-349-5191	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226.

For Georgia, Maine, Maryland, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: For more information on identity theft, you can contact the following:

New York Department of State Division of Consumer Protection at
http://www.dos.ny.gov/consumerprotection or (800) 697-1220

NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

***