



faegredrinker.com

Kenneth K. Dort
Partner
kenneth.dort@faegredrinker.com
+1 312 569 1458 direct

Faegre Drinker Biddle & Reath LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606
+1 312 569 1000 main
+1 312 569 3000 fax

March 25, 2020

VIA FEDEX

Attorney General Gordon MacDonald
Office of the New Hampshire Attorney General
Attn: Security Incident Notification
33 Capitol Street
Concord, NH 03301

RE: Data Incident Notification

Dear Attorney General MacDonald:

Our firm represents VMS Fund Administration, LLC (“VMS”), a New Jersey corporation. VMS recently experienced a data incident and we are hereby formally notifying you of this event pursuant to N.H. Rev. Stat. Ann. § 359-C:20. By providing this notice, VMS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire notification security breach statute, or all/any other applicable laws (including those pertaining to personal jurisdiction).

On January 21, 2020, an employee of VMS fell victim to a phishing scam. VMS noticed suspicious activity on January 23, 2020 on that employee’s account and quickly shut off potential avenues of access to that email account. VMS then promptly notified counsel and engaged a nationally recognized third-party forensics firm to investigate the phishing incident. The forensics firm also reviewed the contents of the affected email account to determine if any personally identifiable information (“PII”) was in the account. On February 15, 2020, the forensics firm concluded its investigation and notified VMS that there were certain documents attached to emails within the account, which documents contained names, addresses and social security numbers.

While we have no evidence that any PII of any New Hampshire residents was accessed or acquired, we decided to notify the potentially affected individuals out of an abundance of caution. VMS sent written notification to the potentially affected individuals during the week of March 16, 2020 via United States mail. The notice contains a description of what happened and the PII that could have potentially been accessed. For your reference, we have attached a sample letter of the individual notice, attached hereto as Exhibit A. VMS sent this notice to the four (4) New Hampshire residents identified by the forensics firm.

RECEIVED
MAR 26 2020
CONSUMER PROTECTION

VMS is providing the affected individuals with two years of free Experian credit monitoring service and a toll-free number to call with any questions. Additionally, VMS is reviewing its security procedures to identify areas where further actions can be taken to mitigate the risk of falling victim to incidents like this in the future.

If you have any questions regarding this matter, please do not hesitate to contact me at 312-569-1458 or Kenneth.dort@faegredrinker.com.

Very truly yours,

/s/ Kenneth K. Dort

Kenneth Dort
Partner

EXHIBIT A

Sample Customer Notice



faegredrinker.com

Kenneth K. Dort
Partner
kenneth.dort@faegredrinker.com
+1 312 569 1458 direct

Faegre Drinker Biddle & Reath LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606
+1 312 569 1000 main
+1 312 569 3000 fax

March __, 2020

NAME
ADDRESS 1
ADDRESS 2
CSZ

Re: Notice of Data Breach

Dear [Insert Name]:

We are sending this notice to you on behalf of VMS Fund Administration, LLC (“VMS”) to notify you of a recent incident that may have resulted in unauthorized access to your personal information maintained by VMS, which it received as part of its administrative functions on behalf of investment funds where you are a limited partner or owner. This letter also provides you with information on the steps VMS has taken to further protect your data going forward and steps you can take to remain vigilant in monitoring your data.

What Happened?

On January 21, 2020, one VMS employee’s company email account was targeted by an unauthorized third party through a phishing scheme. Once VMS became aware of this situation on January 23, 2020, it promptly shut off all potential avenues for access to the account. Shortly thereafter, VMS engaged outside counsel and a nationally recognized third-party forensics firm to investigate the incident.

What Information Was Involved?

The investigation reviewed the circumstances of the incident and the email account in question (including all contents of emails in that account and attachments thereto) that was the subject of the incident. This detailed and careful investigation, which concluded on February 15, 2020, also searched for evidence that your data was in fact accessed. Based on the investigation, we found no evidence that your personal information was copied, stolen, exfiltrated or otherwise distributed out of the email account, and thus believe the risk that your data was accessed or compromised is low. However, because certain personal information such as your name, address and social security number could have been accessible for a short period of time, we are providing this notice to you.

What We Are Doing

We take the security of your personal information very seriously and we are now reviewing our security procedures to determine what additional steps we can take to limit these types of incidents in the future. The mailing of this notice was not delayed by law enforcement.

What You Can Do

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: June 30, 2020 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: **XXXXXXXXXX**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by June 30, 2020. Be prepared to provide engagement number **XXXXXXXX** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site. Finally, please review the enclosed attachment called *Preventing Identity Theft and Fraud* for more information on ways to protect against the potential misuse of your information.

March __, 2020

Page 3

For More Information

Again, we take the security of your information in our care very seriously and we regret any concern or inconvenience this incident may cause you. If you have additional questions, please call our dedicated assistance line at 1-XXX-XXX-XXXX Monday through Friday, 9:00 am – 6:30 pm ET.

Sincerely,

A handwritten signature in black ink, appearing to read 'K. Dort', with a horizontal line extending to the right.

Kenneth K. Dort

PREVENTING IDENTITY THEFT AND FRAUD

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. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and also to access some services that are free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this document and at www.identitytheft.gov/Know-Your-Rights. For example, 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.

At no charge, you can have these credit bureaus place a short-term or an extended "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
800-349-5151	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

You have the right to request a credit freeze from a consumer reporting agency, free of charge. But unlike a fraud alert, you must separately place a security freeze on your credit file at **each** bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

Equifax Security Freeze. 1-800-685-1111. P.O. Box 1057881, Atlanta, GA 30348-0241.
www.equifax.com/personal/credit-report-services;

Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013.
www.experian.com; or

TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000. www.transunion.com/credit-help

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means, and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement or your state Attorney General as well.

The Federal Trade Commission can be reached at:

Federal Trade Commission
Consumer Resource Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov or www.ftc.gov

OTHER IMPORTANT INFORMATION

You may also file a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report filed in this matter.

For Rhode Island residents:

You may obtain information about preventing and avoiding identity theft from Rhode Island's Attorney General Office: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, Phone: (401) 274-4400 <http://www.riag.ri.gov>.

For Maryland Residents:

You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.marylandattorneygeneral.gov

For North Carolina Residents:

You may obtain information about avoiding identity theft at: North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 919-716-6400 www.ncdoj.gov

For New Mexico Residents:

The Fair Credit Reporting Act provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, and seek damages from violators. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For California Residents:

You can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Iowa Residents:

You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico and Vermont 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).