



Blair L. Dawson
550 West Adams Street, Suite 300
Chicago, Illinois 60661
Blair.Dawson@lewisbrisbois.com
Direct: 312.463.3332

October 27, 2021

File No. 30841.1775

VIAWEB PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notification of Data Security Incident

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents Paladin Advisors (“Paladin”) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine’s data breach notification statute.

1. Nature of the Security Incident

Paladin is an independent, registered investment adviser based in Kensington, New Hampshire.

On August 22, 2021, Paladin discovered that its systems had been encrypted. Upon discovery, Paladin took immediate steps to secure its systems prior to restoration. Simultaneous with its remediation and restoration efforts, Paladin retained a digital forensics firm and incident response counsel to assist with its response efforts and conduct an investigation to determine the source and scope of the incident.

The investigation determined personal information may have been impacted as a result of the incident. Paladin then worked diligently to determine the individuals who were impacted and their address information in order to provide notification of this incident.

2. Type of Information and Number of Maine Residents Involved

The incident involved personal information for approximately **8** Maine residents. The information involved in the incident may differ depending on the individual but may include name, Social Security number, financial account number, and driver's license or other ID information.

Paladin notified 7 impacted Maine residents of this data security incident via first class U.S. mail on October 14, 2021. Due to a formatting error, 12-month enrollment codes for identity monitoring services were included in the letter instead of the intended 24-month codes. Paladin mailed updated notices on October 27, 2021, providing 24 months of credit monitoring.

Additionally, on October 25, 2021, Paladin identified address information for the remaining 1 individual. The notification letters will be sent to these individuals via USPS First Class Mail on October 27, 2021.

3. Measures Taken to Address the Incident

In response to the incident, Paladin retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Additionally, Paladin reported the incident to the Federal Bureau of Investigation ("FBI") and will cooperate fully and assist with any investigation. Paladin Advisors also implemented additional security measures to further harden our digital environment in an effort to prevent a similar event from occurring in the future.

Finally, Paladin is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

4. Contact Information

Paladin is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Blair Dawson at 312-463-3332 or Blair.Dawson@lewisbrisbois.com.

Attorney General Aaron Frey
October 27, 2021
Page 3

Sincerely,



Blair L. Dawson of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

BLD:vh:mj
Encl.: Sample Consumer Notification Letter



To Enroll online, please visit www.equifax.com/activate
Or call Equifax representatives at 1-866-243-0734
FULL NAME>: <ASSIGNED ACTIVATION CODE>

October 14, 2021

<FULL NAME>
<STREET ADDRESS>
<CITY>, <STATE> <ZIP CODE>

Dear <FIRST NAME>,

We are writing to let you know of a recent data security incident at Paladin that may have involved your personal information. While we have no reason to believe that your information was misused, we are providing this notice out of an abundance of caution. With the assistance of Paladin's cybersecurity advisory team, we have engaged with subject-matter experts to ensure the safety of your personal data, and to further intensify our technology security practices. Your peace of mind is our utmost concern and we are happy to address your questions and concerns at any time.

What Happened: On August 22, 2021, Paladin discovered that its systems had been encrypted. Upon discovery, we took immediate steps to secure our systems prior to restoration. In addition, we retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident.

What Information Was Involved: We determined that the affected systems may have contained some of your personal information. However, we have no reason to believe that any of your information has been misused as a result of this incident.

What We Are Doing: We are pleased to report minimal disruption to our client and investment operations, aided by prior business continuity planning and strong teamwork. Paladin's systems were back up and running quickly, with most elements fully restored as of this writing. We are working with our cybersecurity advisors to identify additional steps that we can take to "harden" our network. Along with their usual rigorous precautions, our custodians have additional steps available to secure your accounts – ranging from placing restrictive money movement coding to redesignating your brokerage account numbers. Please let us know if you wish to pursue these options.

In addition, we have reported the incident to the Federal Bureau of Investigation and are committed to providing the FBI and law enforcement whatever assistance is needed.



What You Can Do: Even though there is no evidence of misuse of information involved in this incident, we are offering identity theft protection through Equifax, the global data, analytics and technology company. Key features of the Equifax Credit Watch Gold package include 24 months of Credit Monitoring with daily access to your Equifax credit report, WebScan notifications, Automatic Fraud Alerts, Identity Restoration Services with an assigned Restoration Specialist, and up to \$1,000,000 Identity Theft Insurance Coverage. With this protection, Equifax will help you resolve issues if your identity is compromised. We encourage you to enroll in the identity protection service using your personally-assigned Activation Code, which is noted on this letter as well as on the enclosed instruction sheet. You may enroll online, or by calling a representative at 866-243-0734 during the hours of 9am-9pm Eastern Time, Monday through Friday. Please note that this enrollment offer will be available to you through January 31, 2022.

If you have not already done so, we recommend that you consider placing a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report without written authorization. You may also file an affidavit with the IRS in order to obtain additional verification when filing your tax returns.

There are other protective steps you may take to secure your personal information, which are contained in the attached materials. We are happy to discuss these with you by phone.

Again, at this time, there is no evidence that your information has been misused. If you have any questions concerning this incident, please reach out by phone so we can address your concerns or provide practical assistance. The security of your information is a top priority for Paladin Advisors and we are committed to safeguarding your data and privacy. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Yours sincerely,

Karen Parker Feld
Chief Executive

Steps You Can Take to 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
www.consumer.ftc.gov - and - www.ftc.gov/idtheft
1-877-438-4338

North Carolina Attorney General

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

New York Attorney General

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

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
www.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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



[Name]

[Address]

Re: Cyber Incident Update

Dear [name],

We write to provide an updated enrollment code for the 24-month identity protection services that is being provided to you at no charge. Due to a formatting error, 12-month codes were sent in the letter dated October 14, 2021.

The corrected, 24-month code is <<**enrollment code**>>. You may enroll at www.equifax.com/activate or by calling a representative at (866) 243-0734 during the hours of 9 AM – 9 PM Eastern Time, Monday through Friday. Please note that this enrollment offer will be available to you through January 31, 2022.

If you signed up using the code provided on October 14, 2021, you may still sign up using this corrected code. Your services will run concurrently for a total of 24 months of identity theft protection.

Yours sincerely,

Karen Parker Feld

Chief Executive



To Enroll online, please visit www.equifax.com/activate
Or call Equifax representatives at 1-866-243-0734
«First_Name» «Last_Name»: «Activation_Code»

October 27, 2021

«First_Name» «Last_Name»
«Add_1» «Add 2»
«City», «State» «Zip_Code»

Dear «First_Name»,

We are writing to let you know of a recent data security incident at Paladin that may have involved your personal information. While we have no reason to believe that your information was misused, we are providing this notice out of an abundance of caution. With the assistance of Paladin's cybersecurity advisory team, we have engaged with subject-matter experts to ensure the safety of your personal data, and to further intensify our technology security practices. Your peace of mind is our utmost concern and we are happy to address your questions and concerns at any time.

What Happened: On August 22, 2021, Paladin discovered that its systems had been encrypted. Upon discovery, we took immediate steps to secure our systems prior to restoration. In addition, we retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident.

What Information Was Involved: We determined that the affected systems may have contained some of your personal information. However, we have no reason to believe that any of your information has been misused as a result of this incident.

What We Are Doing: We are pleased to report minimal disruption to our client and investment operations, aided by prior business continuity planning and strong teamwork. Paladin's systems were back up and running quickly, with most elements fully restored as of this writing. We are working with our cybersecurity advisors to identify additional steps that we can take to "harden" our network. Along with their usual rigorous precautions, our custodians have additional steps available to secure your accounts – ranging from placing restrictive money movement coding to redesignating your brokerage account numbers. Please let us know if you wish to pursue these options.

In addition, we have reported the incident to the Federal Bureau of Investigation and are committed to providing the FBI and law enforcement whatever assistance is needed.



What You Can Do: Even though there is no evidence of misuse of information involved in this incident, we are offering identity theft protection through Equifax, the global data, analytics and technology company. Key features of the Equifax Credit Watch Gold package include «12_or_24» months of Credit Monitoring with daily access to your Equifax credit report, WebScan notifications, Automatic Fraud Alerts, Identity Restoration Services with an assigned Restoration Specialist, and up to \$1,000,000 Identity Theft Insurance Coverage. With this protection, Equifax will help you resolve issues if your identity is compromised. We encourage you to enroll in the identity protection service using your personally-assigned Activation Code, which is noted on this letter as well as on the enclosed instruction sheet. You may enroll online, or by calling a representative at 866-243-0734 during the hours of 9am-9pm Eastern Time, Monday through Friday. Please note that this enrollment offer will be available to you through January 31, 2022.

If you have not already done so, we recommend that you consider placing a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report without written authorization. You may also file an affidavit with the IRS in order to obtain additional verification when filing your tax returns.

There are other protective steps you may take to secure your personal information, which are contained in the attached materials. We are happy to discuss these with you by phone.

Again, at this time, there is no evidence that your information has been misused. If you have any questions concerning this incident, please reach out by phone so we can address your concerns or provide practical assistance. The security of your information is a top priority for Paladin Advisors and we are committed to safeguarding your data and privacy. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Yours sincerely,

Karen Parker Feld
Chief Executive

Steps You Can Take to 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
www.consumer.ftc.gov - and - www.ftc.gov/idtheft
1-877-438-4338

North Carolina Attorney General

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

New York Attorney General

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

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
www.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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.