



Ryan M. Cook
1020 Highland Colony Parkway, Suite 310
Ridgeland, Mississippi 39157
Ryan.Cook@lewisbrisbois.com

August 9, 2024

Via electronic-mail: *ldtheft@oag.state.md.us*

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

Re: Our Client: Linchpin-IT
Matter: Data Security Incident

Dear Attorney General Brown:

We represent Linchpin-IT located in Glendale, California, with respect to a data security incident described in more detail below.

This letter will serve to inform you of the nature of the security breach, the number of Maryland residents being notified, what information has been affected, and the steps that Linchpin-IT has taken to secure its systems. We have also enclosed hereto a sample of the notification letter sent to the affected individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On or around May 2, 2024, an unauthorized party gained access to Linchpin-IT's email environment. Linchpin-IT promptly engaged a specialized third-party forensic incident response firm to assist with securing the environment and investigating the incident. On July 19, 2024, Linchpin-IT determined that some personal information was contained in the affected files. Linchpin-IT has since been taking steps to send notification letters to the affected individuals.

Linchpin-IT found that the incident affected individuals' name, address, date of birth, driver's license number, bank account number, and social security number. The types of affected personal information varied by individual. As of this writing, Linchpin-IT has not received any reports of related identity theft in connection with the incident.

2. Maryland Residents Notified

A total of two (2) residents of Maryland were affected by this security incident. Notification letters to these individuals were mailed on August 2, 2024 via first class mail, and included an offer of free credit monitoring. Sample copies of the notifications are included with this letter.

3. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at Ryan.Cook@LewisBrisbois.com or 601.499.8128.

Sincerely,

A handwritten signature in black ink, appearing to read "Ryan Cook", is positioned above the typed name.

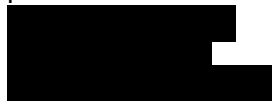
Ryan M. Cook for
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: *Sample notification letter*

RMC

Linchpin-IT
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P



August 2, 2024

Via First-Class Mail

Notice of Data Security Incident

Dear [REDACTED],

We are writing to inform you of a data security incident that may have resulted in unauthorized access to your personal information. This letter contains information about the incident and steps you can take to help protect your personal information.

What Happened:

On May 2, 2024, Linchpin-IT detected and stopped a network security incident that involved an unauthorized party gaining access to our email environment. The affected data contained personal information such as name, address, date of birth, driver's license number, financial account number and Social Security number. The types of affected personal information varied by individual.

What We Are Doing:

Upon becoming aware of the incident, we promptly took steps to investigate the issue and secure our systems. We worked with third-party forensic specialists to investigate the extent of unauthorized activity. In addition, we have implemented measures to further enhance the security of our network environment.

We are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for <<service length>> months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in credit monitoring services at no charge, please log on to **<https://bfs.cyberscout.com/activate>** and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

000010102G0500

P

Also, you will need to reference the enrollment code above when calling or enrolling online, so please do not discard this letter.

For More Information:

Enclosed you will find additional information regarding the resources available to you, and the steps you can take to further protect your personal information.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident. Please call 1-800-405-6108, Monday through Friday, 8:00 am to 8:00 pm ET, excluding holidays, for assistance or for any additional questions you may have.

We regret any inconvenience this may cause you.

Sincerely,

Linchpin-IT

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address and the date of issue. It is free to place, lift or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement, the FTC and the relevant state Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.



00001020280000

P

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General - Consumer Protection: 2005 North Central Avenue, Phoenix, AZ 85004; 602-542-5025

Colorado Office of the Attorney General - Consumer Protection: 1300 Broadway, 9th Floor, Denver, CO 80203; 720-508-6000; www.coag.gov

District of Columbia Office of the Attorney General - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois Office of the Attorney General - 115 S. LaSalle St., Chicago, IL 60603; 866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 888-743-0023; <https://www.marylandattorneygeneral.gov/>

New York Office of Attorney General - Consumer Frauds Bureau: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/> or to contact the Bureau of Internet and Technology (BIT); 212-416-8433; <https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 877-566-7226; <https://ncdoj.gov/protecting-consumers/>

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 401-274-4400; www.riag.ri.gov_