



April 21, 2020

Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED

APR 25 2020

CONSUMER PROTECTION

Re: Presidio, Inc.'s Notice of Data Security Breach

Dear Attorney General MacDonald,

We represent Presidio, Inc. (Presidio), an IT-solutions service provider, with headquarters located at One Penn Plaza, Suite 2832, New York, NY 10119. We write to notify you that Presidio has sustained a data security breach affecting the personally-identifiable information of 3,324 present and former Presidio employees, including 44 New Hampshire residents.

Specifically, Presidio discovered on March 13, 2020 that, on or about March 5, 2020, an unknown third-party gained unauthorized access to a software service containing personal information of present and former Presidio employees working for the company in 2019 and/or 2020.

Presidio's internal IT and cybersecurity teams took immediate action to investigate this reported irregularity. The teams uncovered the March 5, 2020 intrusion and traced its results. In particular, they ascertained that, by means of the unauthorized access to the software service, the culpable actor had, *first*, altered the direct deposit accounts of 13 Presidio employees; and, *second*, with respect to only two of those altered accounts, direct deposits were thereby wrongfully diverted. Presidio promptly corrected all the direct deposit accounts altered by the intruder, restored in full the funds that had been diverted from such two accounts, and contacted the banks to retrieve the misdirected deposits.

Having identified and contained the intrusion at the outset, Presidio's IT and cybersecurity teams proceeded to conduct a thorough investigation of the intrusion and all records affected by it. In addition to uncovering the thirteen altered direct deposit accounts and the two diverted deposits, on March 21, 2020 the internal forensic investigators found that the personal information accessed by the unauthorized party included (a) the name, Social Security number, and total compensation of each Presidio employee who received from the company a 2019 W-2 form (wage and tax statement); and (b) the names and wage/tax information of Presidio employees listed on a 2020 payroll register report.

To alert those whose personal information has been subject to such unauthorized access or use, and in compliance with applicable law, Presidio is providing written notice of the data breach to all affected individuals. A template copy of that notice accompanies this report to your office. Such notice was mailed to the affected New Hampshire residents on or about April 21, 2020.

The notice also informs the affected residents of your state that Presidio has arranged for TransUnion to provide them with credit monitoring and identity theft restoration services, at no charge to them, for the next twelve (12) months. More detailed information on those prepaid ameliorative services is included in the TransUnion attachment to each data breach notice. Together with those services, Presidio has made available a toll-free phone number, allowing the affected individuals to obtain further information and assistance.

Supplementing the investigative and remedial initiatives outlined above, Presidio has engaged the expert forensic services of an external cybersecurity firm to review the company's own investigation and assess its preliminary findings. Furthermore, Presidio has implemented proactive security measures designed to prevent a recurrence of last month's cyberattack. Presidio is also evaluating additional enhancements to its written protocols for the protection of the personal information, accounts, and privacy of its employees, including, without limitation, its personal data protection policy.

If you have any questions or seek further information, please contact the undersigned member of the firm directly at 516.262.3000 or rakmal@h-alaw.com

Respectfully submitted,



Rizwan Akmal, Esq.



Future. Built.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

One Penn Plaza
Suite 2832
New York, N.Y. 10119
www.presidio.com

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

We are writing to inform you about a recent data security incident affecting some of your personal information. We value our relationship with you, and we respect your privacy. In addition to providing you this notice, therefore, we want to outline certain steps you may consider taking under the circumstances to help safeguard your personal information and protect your credit.

WHAT HAPPENED?

We have determined that on or about March 5, 2020, an unknown third party gained unauthorized access to a software service containing personal information of present and former Presidio employees working for us in 2019 and/or 2020.

WHAT INFORMATION WAS INVOLVED?

The personal information accessed by the unauthorized party included (a) the name, Social Security number, and total annual compensation of each Presidio employee who received from Presidio a 2019 W-2 form (wage and tax statement), and (b) the names and wage/tax information of employees listed on a 2020 payroll register report.

WHAT WE ARE DOING

Presidio takes this data breach very seriously. Our internal IT and cybersecurity teams took immediate action to identify and contain the intrusion. They have also been conducting a thorough investigation of the intrusion and all records affected by it. Supplementing these initiatives, we have engaged the expert forensic services of an external cybersecurity firm to review our own investigation and assess its preliminary findings. We have implemented proactive security measures designed to prevent a recurrence of such an attack. Moreover, we are evaluating additional enhancements to our protocols for the protection of the personal information, accounts, and privacy of our employees.

WHAT YOU CAN DO

As always, we recommend you be on the alert for suspicious activity related to your financial accounts and credit reports. We encourage you to regularly and carefully check your statements and records to ensure there are no transactions or other activities that you did not initiate or authorize.

We strongly urge you to sign up to receive, at no charge to you, the credit monitoring and identity theft restoration services provided by TransUnion. We have arranged for TransUnion to make these prepaid services available to you for the next twelve (12) months. For more information about these services, please review TransUnion's attachment to this letter. For more information, please see the attached "Steps You Can Take to Further Protect Your Information."

FOR MORE INFORMATION

Please be assured that we are committed to helping you protect your credit and identity and ensuring that your personal information is safe and secure. We regret this incident and apologize for any concerns it may have caused you.

For further information and assistance, please contact 855-917-3461 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,

A handwritten signature in black ink, appearing to read "Elliot Brecher". The signature is fluid and cursive, with a long horizontal stroke at the end.

Elliot Brecher, Senior Vice President & General Counsel

Steps You Can Take to Further Protect Your 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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you 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 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 can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>, or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

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 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. 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>.

Credit Report Monitoring/Identity Theft Protection Services

In addition, Presidio has arranged with TransUnion to provide you with credit monitoring and identity theft restoration services for the next twelve (12) months, at no cost to you. **To take advantage of this offer, you must enroll between now and <<Enrollment Deadline>>.** To learn more about these services and how to enroll, please review TransUnion's attachment to this letter.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

OTHER IMPORTANT INFORMATION

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.

Complimentary One-Year *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

Article I. How to Enroll: You can sign up online or via U.S. Mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Article II. ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)