



Andrew B. Epstein
+1 720 566 4203
aepstein@cooley.com

RECEIVED
JAN 09 2019
CONSUMER PROTECTION

January 8, 2019

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

Re: Notice of a Potential Information Security Incident

Dear Attorney General MacDonald:

On behalf of my client, Enservio, Inc. ("Enservio" or "Company"), I write to inform you of a potential information security incident that may affect five (5) New Hampshire residents. Enservio will notify all potentially affected residents and outline steps that they make take to help protect themselves.

On or about December 10, 2018, Enservio learned that an unauthorized individual gained prohibited access to certain Enservio web-based e-mail accounts that contained limited personal information about a few New Hampshire residents with whom Enservio has a relationship. Although Enservio cannot be certain whether any particular individual's information within an e-mail account was accessed as a result, some e-mails and attachments maintained within the accounts contained limited personal information, such as names, addresses, and Social Security numbers. Accordingly, and out of an abundance of caution, Enservio is providing notice to all potentially affected individuals and to your office in the event that the unauthorized individual accessed such information.

Enservio takes the privacy of personal information seriously and deeply regrets that this potential incident occurred. Upon learning of the potential incident, Enservio promptly took steps to address it, including engaging an outside forensic firm to assist in investigating and remediating the situation. In addition, Enservio has taken steps to help prevent this type of potential incident from occurring in the future, including resetting all affected e-mail accounts' passwords as well as providing additional training to its employees on the maintenance of personal information and how to recognize e-mail phishing schemes. Enservio will provide periodic updates to its employees as new threats come to its attention.

On or about January 9, 2019, Enservio will provide all potentially affected individuals with written notification about the potential incident. Enservio will, at no cost to the notice recipient, offer twelve months of identity-protection services that includes credit monitoring. For your reference, I have included a template of the notice being sent to the potentially affected New Hampshire residents.

If you have any questions or need further information regarding this potential incident, please contact me at 720-566-4203 or aepstein@cooley.com.



Office of the Attorney General
January 8, 2019
Page Two

Sincerely,

A handwritten signature in blue ink, appearing to read "Andrew B. Epstein".

Andrew B. Epstein

Enclosure

196134470 v1



January 9, 2019

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

Notice of Data Breach

We are writing to inform you of a potential security incident involving certain personal information you provided to Enservio, Inc. ("Enservio" or "Company"). We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened

We recently learned that an unauthorized individual appears to have obtained and used a limited number of Enservio employees' login information to our web-based email system. The few accessed Enservio email accounts contained some personal information, which will be discussed in more detail below.

What Information Was Involved

The information stored in the impacted email accounts varied by individual but may have included first and last names, as well as <<ClientDef1(INSERT VARIABLE TEXT)>>. Based on our investigation, it appears your personal information was stored in one of the accessed accounts and, therefore, could be affected by this incident. Our investigation has not found any evidence that this incident involves any unauthorized access to or use of Enservio's internal computer systems or network. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

We take the privacy of personal information seriously and deeply regret that this potential incident occurred. We took steps to address this incident promptly after it was discovered. Our Information Technology personnel promptly initiated an internal investigation. We retained an independent forensic firm to assist our investigation of and response to this incident. To help prevent this type of incident from occurring in the future, we have taken steps to bolster our IT security, including resetting all affected user account passwords and conducting additional employee training.

To help protect your identity, we are offering one year of complimentary identity monitoring services through Kroll. These services help detect possible misuse of your personal information and provide you with superior identity monitoring support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions included with this letter.

What You Can Do

Although we are not aware of any identity theft arising out of this potential incident, we want to make you aware of steps that you can take as a precaution:

- **Activating the Complimentary Identity Monitoring Services.** As outlined above, we are offering one year of identity monitoring services at no charge to you. For more information about these services and instructions on

Enservio
117 Kendrick Street, Suite 250
Needham, MA 02494

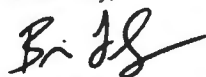
completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide. Note that you must complete the enrollment process by April 9, 2019.

- **Checking Credit Reports and Financial Accounts.** You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.
- **Consulting the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact our dedicated call center at 1-866-775-4209 between the hours of 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday. Again, we sincerely regret any concern this incident may cause you.

Sincerely,



Brian Filip
Managing Director

Information about Identity Theft Protection

To help protect your identity, we are offering complimentary identity monitoring services through Kroll.

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

You have until April 9, 2019 to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

You've been provided with access to the following services¹ from Kroll.

- **Single Bureau Credit Monitoring:** You will receive alerts when there are changes to your credit data — for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.
- **Web Watcher:** Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.
- **Public Persona:** Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.
- **Quick Cash Scan:** Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported and you can call a Kroll fraud specialist for more information.
- **\$1 Million Identity Fraud Loss Reimbursement:** Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

- **Fraud Consultation:** You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- **Identity Theft Restoration:** If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this reference guide.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protecting against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>.

Security Freezes and Fraud Alerts:

You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's

credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity;
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
- (4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies' Contact Information

Equifax (www.equifax.com)

General Contact:

P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:

P.O. Box 740256, Atlanta, GA 30374

Credit Freezes:

P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)

General Contact:

P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:

P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)

General Contact:

P.O. Box 105281
Atlanta, GA 30348
800-888-4213

Fraud Alerts and Security Freezes:

P.O. Box 2000, Chester, PA 19022
888-909-887