SevOne

800 Boylston Street, Suite 500, Boston, MA 02199

March 14, 2016

Office of the Attorney General
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Dear Attorney General Joseph Foster:

I am writing to inform you that on March 7, 2016, SevOne was the victim of an email phishing incident that resulted in an unauthorized disclosure of 2015 W-2 forms of current and former employees. The personal information involved included name, address, Social Security number, income information and other information found on a 2015 W-2 form. At this time, SevOne believes that only ten New Hampshire residents were affected and we have no reason to believe that any other New Hampshire residents or non-W-2 data were affected.

We learned of the incident immediately after it happened and quickly began taking steps designed to prevent further unauthorized disclosure, including alerting current and former employees the day after we found out about the incident. In addition, SevOne is offering affected individuals two years of complimentary credit monitoring and identity repair services through AllClear ID and has provided affected individuals with information on how to help protect themselves from identity fraud, such as how to place a fraud alert. We enclose a copy of the initial notice and formal notices that we sent to affected individuals, which we sent on March 8, 2016 and March 14, 2016, respectively.

SevOne has notified the Federal Bureau of Investigation (FBI) and Internal Revenue Service (IRS) and is actively working with the IRS to help protect those affected by this incident. This notification has not been delayed because of a law enforcement investigation.

The protection of the personal information of our employees, current and former, is very important to SevOne. We are aggressively analyzing where process changes are needed and we are implementing those changes as quickly as we can.

If you have any questions or require additional information, please feel free to contact me at 617-982-7705 or dpyron@sevone.com.

Sincerely,

Diane Pyron

Diane Pyron
Chief Legal Officer

Encl.

All,

SevOne has been the victim of an email phishing incident that resulted in an unauthorized disclosure of your 2015 W-2 form. We are alerting you because cybercriminals can use W-2 data to file false tax returns in someone else's name – and we want to help you avoid that.

The phishing incident happened yesterday, March 7, 2016, and we learned of it immediately after it occurred. We are actively working to understand the incident and at this time we have no reason to believe any other SevOne data was affected.

We sincerely apologize to anyone who may have been affected and will send additional communications as further information is learned. To help protect you, at no cost to you, we will be providing 2 years of credit monitoring services, with details to follow. However, while the investigation is ongoing, we want to provide you with the following resources to educate you about tax identity theft and the steps you can take to thwart it:

1. **File your taxes as soon as possible**, if you have not done so already. We understand that the best way to avoid becoming a victim of tax identity theft is to file your taxes before any fraudsters can.

2. **Report suspected tax identity theft** with the Internal Revenue Service (IRS), Federal Trade Commission (FTC), major credit bureaus, and your financial or payment card institutions. For more information on how to file these reports, please see the IRS Taxpayer Guide to Identity Theft and the FTC's Tax-Related Identity Theft webpage. As noted in the IRS Taxpayer Guide to Identity Theft, IRS Form 14039, Identity Theft Affidavit, can be filed to report even a potential concern over suspect tax-related identity theft.

3. **Practice good data security** by:

    a. Making sure that any passwords that you use related to tax filings are unique, hard-to-guess, and have not been used previously for tax purposes.

    b. Ensuring that your computer has anti-virus protection and that it is up-to-date.

    c. Not giving out your Social Security number or other personal information to unknown sources. You should pay particular attention to any emails asking for personal information, financial information, or SSNs. You should also carefully inspect the sender of messages asking for this information (for example, if your tax preparer's email address is john.smith@taxpreparer.com you should not provide your information to john.smIth@taxpreparer.com).

4. **Understand your tax preparer's data protection.** If you use a tax preparer, ask them about how they protect your tax information – and you may want to consider changing tax preparers if you do not feel comfortable with the measures they take to protect your data.

Again, we apologize to anyone potentially affected and will keep you posted on the status of our investigation. If you have any questions, please contact us at 2015-questions@sevone.com.

Sincerely,
Diane Pyron
Chief Legal Officer

800 Boylston Street, Suite 500, Boston, MA 02199

March 14, 2016

To Current and Former SevOne Employees:

We are writing to inform you that on March 7, 2016, SevOne was the victim of an email phishing incident that resulted in an unauthorized disclosure of your 2015 W-2 form. We learned of the incident immediately after it happened and quickly began taking steps designed to prevent further unauthorized disclosure of your personal information, including alerting you the day after we found out and notifying the Federal Bureau of Investigation (FBI) and Internal Revenue Service (IRS). We are also aggressively analyzing where process changes are needed and we are implementing those changes as quickly as we can.

The personal information involved in this incident includes your name, address, Social Security number, income information and the other information found on your 2015 W-2 form. At this time, we have no reason to believe any other SevOne data was affected.

We take the security of your personal information seriously and sincerely apologize to anyone who may have been affected. To assist you in protecting your identity, we are offering **complimentary** credit monitoring and identity repair services through AllClear ID. Membership runs from the date of this letter. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. Sign-up information is below.

AllClear Services Information

The team at AllClear ID is ready and standing by if you need identity repair assistance. You may take advantage of this service at any time during the twenty-four month period. You are automatically enrolled in this service, and there is no enrollment requirement. If a problem arises, simply call **1-877-676-0379** and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

In addition, you may sign up for the PRO service, at no cost to you, which includes three bureau credit monitoring and a $1 million identity theft insurance policy, among other features. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling **1-877-676-0379** using the Redemption Code in the cover letter you received with this document. This service is valid for twenty-four months from the date of this letter, regardless of when you sign-up for the service.

Please note: Additional steps may be required to activate your phone alerts and monitoring options.

Additional Steps You Can Take to Protect Yourself

In addition to registering for the credit monitoring and identity repair services, we recommend that you:

1. **Remain vigilant** by checking your financial statements and reviewing your credit reports. You can also order free copies of your credit reports through www.annualcreditreport.com. For more information from the Federal Trade Commission (FTC) about steps you can take to reduce the likelihood of identity theft or fraud, you can:
   - Visit http://www.ftc.gov/bcp/edu/microsites/idtheft/
   - Call 1-877-ID-THEFT (1-877-438-4338)
   - Write to Federal Trade Commission
     600 Pennsylvania Avenue, NW
     Washington, D.C. 20580

2. **File your taxes as soon as possible**, if you have not done so already. We understand that the best way to avoid becoming a victim of tax identity theft is to file your taxes before any fraudsters can.

3. **Respond promptly to any inquiries from the Internal Revenue Service (IRS)**. Please note, however, that as a general rule the IRS does *not* initiate contact with taxpayers by email (or other electronic channels) to request personal or financial information. If you receive an electronic communication from the IRS requesting personal or financial information, you should contact the IRS at 1-800-366-4484 to confirm the validity of the communication.

4. **Report suspected tax identity theft** to the FTC, IRS, state regulators, major credit reporting agencies, your local law enforcement, and your financial or payment card institutions. For more information on how to file these reports, please see the IRS Taxpayer Guide to Identity Theft and the FTC's Tax-Related Identity Theft webpage. As noted in the IRS Taxpayer Guide to Identity Theft, IRS Form 14039, Identity Theft Affidavit, can be filed to report even a potential concern over suspect tax-related identity theft. If you have been the victim of an IRS impersonation scam, you can report that to the IRS through its Online Impersonation Scam Reporting Online Form. The contact information for the major credit reporting agencies, from which you can obtain information about fraud alerts and security freezes, is below.

5. **Practice good data security** by:
   - Making sure that any passwords that you use related to tax filings are unique, hard-to-guess, and have not been used previously for tax purposes.
   - Ensuring that your computer has anti-virus protection and that it is up-to-date.
   - Not giving out your Social Security number or other personal information to unknown sources. You should pay particular attention to any emails asking for personal information, financial information, or SSNs. You should also carefully inspect the sender of messages asking for this information (for example, if your tax preparer's email address is john.smith@taxpreparer.com you should not provide your information to john.sm!th@taxpreparer.com).

6. **Understand your tax preparer's data protection.** If you use a tax preparer, ask them about how they protect your tax information – and you may want to consider changing tax preparers if you do not feel comfortable with the measures they take to protect your data.

Information on Credit Report Fraud Alerts

You may also place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You can call any one of the three major credit bureaus at the contact information below or place fraud alerts online at the websites below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

	Equifax	Experian	TransUnion
Phone	1-800-525-6285 or 1-888-766-0008	1-888-397-3742	1-800-680-7289
Address	Equifax Consumer Fraud Division PO Box 740256 Atlanta, GA 30374	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp	https://www.experian.com/consumer/cac/InvalidateSession.do?code=SECURITYALERT	http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/fraudAlert.page

Information on Security Freezes

In addition to a fraud alert, you may also have a security freeze placed on your credit file. A security freeze will block a credit bureau from releasing information from your credit report without your prior written authorization. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. The fees for placing a security freeze vary by state, and a consumer reporting agency may charge a fee of up to $10.00 to place a freeze or lift or remove a freeze.

To place a security freeze on your credit report, you may send a written request to **each** of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting **each** consumer reporting agency online.

	Equifax	Experian	TransUnion
Address	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp	https://www.experian.com/freeze/center.html	https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp

Questions?

If you have any questions, please feel free to contact us at:

- **Email:** 2015-questions@sevone.com
- **Phone:** 1 (888) 970-0567 (SevOne's Main Number)
- **Address:** ATTN: Diane Pyron
800 Boylston Street, Suite 500
Boston, MA 02199

State-Specific Information

For residents of **Maryland**, **North Carolina**, and **Rhode Island:** For more information on identity theft and how to prevent it, you can contact your state's attorney general.

	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
Phone	1-410-576-6491	1-877-566-7226 (within North Carolina) or 1-919-716-6000 (if outside North Carolina)	1-401-274-4400
Email	Idtheft@oag.state.md.us	consumer@ncdoj.gov	consumers@riag.ri.gov
Address	Identity Theft Unit Attorney General of Maryland 200 St. Paul Place 16th Floor Baltimore, MD 21202	Consumer Protection Division Attorney General's Office Mail Service Center 9001 Raleigh, NC 27699-9001	Rhode Island Office of the Attorney General 150 South Main Street Providence, RI 02903
Website	https://www.oag.state.md.us/	http://www.ncdoj.gov	http://www.riag.ri.gov/

For residents of Rhode Island: Under Rhode Island law, you have the 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.

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Twenty-four (24) months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for twenty-four (24) months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements

To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.877.676.0379 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
    - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
    - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1-877-676-0379