

15 March 2016

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

STATE OF NH
DEPT OF JUSTICE
2016 MAR 16 AM 10:20

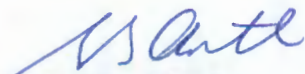
RE: Notification of Data Security Breach Incident

Dear Sir/Madame:

This letter is being sent in accordance with New Hampshire law to inform your office that our company recently suffered an email spoofing incident that resulted in an employee unwittingly sending an unknown outside third party W-2 information about one New Hampshire resident on about February 16, 2017 in response to an email request that appeared to be from a company executive. In fact the email was from an unknown outside third party. The information provided included name and Social Security Number. We have enclosed a copy of the notice letter that we will be sending to the affected individual on March 15, 2016.

We are offering two years of credit monitoring and identity theft services for the affected individual through Kroll Services. We have notified the IRS of this incident and are taking steps internally to improve our procedures for protecting data so that this type of incident doesn't recur. This includes access and storage restrictions as well as enhanced transmission procedures. Should you have any additional questions, you may contact me directly at (703) 891-8001.

Sincerely,



S. Bradford Antle
Chief Executive Officer



4000 Legato Rd, Suite 600
Fairfax, VA 22033

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

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

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On February 16th, several files containing W-2 data for some current and former employees was accidentally released via email to someone fraudulently posing as the company CFO. Email spoofing (sending an email that appears to be from someone else) has become more and more sophisticated and is being used by thieves to obtain information. We discovered this incident last week, when we heard from a few employees that they had seen suspicious activity related to the IRS. In two cases, employees were unable to file their tax returns due to fraudulent tax returns being filed ahead of their attempt. This was our first indication of the breach.

The IRS has been notified as well as the state taxing authorities. We are certainly going to cooperate with any investigations that ensue. However, it appears as though many companies have had the same breach of W-2 data this year already.

What information was involved?

W-2 information was accidentally released so it clearly contains your Social Security number, name, address, income, and deduction.

What we are doing.

First and foremost, to address those who have been impacted by this breach, to help relieve concerns and restore confidence following this incident, we have secured the services of a company named Kroll to provide identity monitoring at no cost to you for two years. 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 Theft Insurance, Identity Consultation, and Identity Restoration.

Visit kroll.idMonitoringService.com to enroll and take advantage of your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-877-309-0021. Additional information describing your services is included with this letter.

We are also taking steps internally to improve our procedures for protecting data so that this type of incident doesn't recur. This includes access and storage restrictions as well as enhanced transmission procedures.

In an effort to protect you from tax-related identity theft, we contacted the Internal Revenue Service and shared the details of the data theft. Criminals who steal personal data may try to monetize that information by filing fraudulent tax returns.

The IRS offered the following guidance:

- The IRS recommends that taxpayers who have had Social Security numbers stolen review information in Publication 5027, Identity Theft Information for Taxpayers, for additional steps they should take to protect themselves.

- We are also enclosing IRS Form 14039, Identity Theft Affidavit, you should submit to the IRS to flag your account for fraud. **We think it is advisable to file the form right away and do not wait.**
- File your 2015 tax returns as soon as possible.
- Contact the IRS Identity Theft Hotline at (800) 908-4490. If you call, they will ask you a series of questions to prove your identity and can discuss with you if they see any fraud on your account. They will also place a note on your file to help protect it from a fraudulent filing.
- If you live in DC, FL or GA, you can also request an additional PIN from the IRS to use when you file your taxes. This will further help reduce the risk of someone else filing a fraudulent claim.
- It is important to respond to any IRS letters or notices. The IRS also explains what victims of tax-related identity theft can expect and how its victim assistance process works.
- There is additional information at www.irs.gov/identitytheft. Generally, more than nine out of 10 refunds are issued in less than 21 days. However, when the IRS gives greater scrutiny to a suspect tax return or seeks to protect known victims from tax-related identity theft, it may take additional time to issue refunds to legitimate taxpayers.

What you can do.

You should always remain vigilant for incidents of fraud and identity theft including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain free credit reports from each nationwide credit reporting agency. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to keep an eye on the accuracy and completeness of the information in your reports. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. If you live in Colorado, Georgia, Maryland, New Jersey or Puerto Rico you may be entitled to additional copies of your report. Contact the credit reporting agencies to find out more. You may contact the nationwide credit reporting agencies at:

| | | |
|--|--|---|
| Equifax (800) 525-6285 P.O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com | Experian (888) 397-3742 P.O. Box 9532 Allen, TX 75013 www.experian.com | TransUnion (800) 680-7289 Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790 www.transunion.com |
|--|--|---|

If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

For more information.

If you have questions, please call 1-877-309-0021, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

IF YOU ARE A CALIFORNIA RESIDENT: Even if you do not find any signs of fraud on your credit reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. The law allows you to order a free credit report from each agency every 12 months. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to monitor the accuracy and completeness of the information in your reports. Just call one of the numbers above to order your report and keep the "fraud alert" in place. For more information on identity theft, you may visit the California Office of Privacy Protection website, www.oag.ca.gov/privacy.

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
<http://www.ftc.gov/idtheft/>

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: For more information on identity theft, we suggest that you visit the New York State Consumer Protection Board website at www.dos.ny.gov/consumerprotection.

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

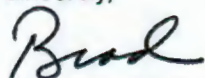
North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.com>

IF YOU ARE A WEST VIRGINIA RESIDENT: You have the right to obtain a security freeze. 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 have a right to place a security freeze on your credit report pursuant to West Virginia law. 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, within five business days you will be provided a unique personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer-reporting agency and provide all of the following: (1) The unique personal identification number or password provided by the consumer-reporting agency; (2) Proper identification to verify your identity; and (3) The period of time for which the report shall be available to users of the credit report.

A consumer-reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request. A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. If you are actively seeking credit, 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, a few days before actually applying for new credit. You have the right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer-reporting agency.

Sincerely,



Brad Antle, CEO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability 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 may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is \$5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Credit Monitoring through TransUnion

You'll 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 investigator, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals buy, sell, and trade personal information. You'll be promptly notified if evidence of your identity information being traded or sold is discovered.

Public Persona

Public Persona monitors public record databases for names, aliases, and addresses that are associated with your Social Security number. If information is found, an alert email is sent.

Quick Cash Scan

Quick Cash Scan monitors thousands of short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll investigator for more information.

\$1 Million Identity Theft Insurance

Reimburses you for out-of-pocket expenses totaling up to \$1 million in legal costs for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Identity Consultation

You have unlimited access to consultation with a dedicated licensed investigator at Kroll. 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 Restoration

If you become a victim of identity theft, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

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.