SIDLEY AUSTIN LLP
SIDLEY

SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
+1 202 736 8000
+1 202 736 8711 FAX

emcnicholas@sidley.com
+1 202 736 8010

BEIJING
BOSTON
BRUSSELS
CENTURY CITY
CHICAGO
DALLAS
GENEVA
HONG KONG
HOUSTON
LONDON
LOS ANGELES
NEW YORK
PALO ALTO
SAN FRANCISCO
SHANGHAI
SINGAPORE
SYDNEY
TOKYO
WASHINGTON, D.C.

FOUNDED 1866

March 21, 2016

The Honorable Joseph Foster
Attorney General of New Hampshire
33 Capitol Street
Concord, NH 03301

Dear General Foster:

We write on behalf of our client CareCentrix, Inc. ("CareCentrix") to inform you of a data security incident involving the personal information of certain current and former CareCentrix employees, including approximately 2 New Hampshire residents.

On March 7, 2016, CareCentrix discovered that one of its employees emailed a copy of IRS Form W-2s for all current and former employees to an individual falsely purporting to be a CareCentrix employee on February 24, 2016. The forms contain individual's names, addresses, and social security numbers as well as income and withholding information. CareCentrix immediately investigated, contacted federal law enforcement at the FBI and IRS, and has determined that the incident was the apparent result of a spearphishing email where a likely criminal actor impersonated the CareCentrix employee. We have also asked the IRS to flag affected social security numbers to deter fraudulent tax returns claiming tax refunds.

CareCentrix internally notified employees of the incident on March 10, 2016 to inform potentially affected employees and outline preliminary steps they could take to protect themselves. CareCentrix is also notifying all potentially affected current and former employees in a formal letter on March 21, 2016, and a sample of that communication is enclosed as Exhibit A. In addition to alerting employees, the FBI and the IRS, CareCentrix is offering free credit monitoring services with identity repair and protection services from AllClearID for two years, and informed all affected employees about methods to monitor their accounts and protect themselves from identity theft.

If you have any questions about this incident, please do not hesitate to contact me at the number listed above.

Respectfully submitted,

Edward R. McNicholas

Edward R. McNicholas
Partner

carecentrix
It pays to care at home
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00038
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 21, 2016

NOTICE OF DATA BREACH

Dear John Sample:

We are writing to share with you important information about a security incident that involved your personal information, as well as steps we are taking in response, and the resources we are making available to you.

What Happened?

On March 7, 2016, we discovered that as the apparent result of a fake email from an individual impersonating a CareCentrix employee, a copy of your IRS Form W-2 was emailed to an unknown unauthorized individual on February 24, 2016. We immediately initiated an investigation and contacted federal law enforcement, the IRS, and arranged for 24 months of credit monitoring at no charge to you.

What Information Was Involved?

Your IRS Form W-2 is a Wage and Tax Statement that includes your name, address, and Social Security number along with income and withholding information.

What We Are Doing

We are fully cooperating with law enforcement in their investigation. We have also notified the IRS and asked them to flag affected Social Security numbers in order to help detect and deter filing of fake tax returns in order to claim fraudulent tax refunds.

Notices like this one are being sent to all individuals whose information was affected, and we have included here information about steps you can take to protect yourself.

What You Can Do

If you believe you are the victim of identity theft, including having someone else claim a tax refund in your name, please contact law enforcement immediately. You will likely need to file a police report about the incident.

To determine if a fraudulent claim has been filed under your name, you can call the IRS Identity Theft hotline at 1-800-908-4490. For the individuals that learn that a false claim has been filed, IRS Form 14039 Identity Theft Affidavit likely will need to be completed and filed.

Even if no fraudulent tax refund is claimed, as a result of our notification to the IRS, you may receive a letter from the IRS to verify that your tax return is valid when you file your taxes this year. It is important that you respond to that letter with regard to your actual tax return.

We encourage you to regularly review your financial accounts and credit reports, and report any suspicious or unrecognized activity immediately. You should be particularly vigilant for the next 12 to 24 months and report any suspected incidents of fraud to us and your financial institution. Please also read the important information included on ways to obtain your free credit report and protect yourself from identity theft.

As your Social Security number was affected, you may wish to consider placing a fraud alert or security freeze on your accounts. More information about these options is detailed below. And you also should consider taking advantage of our offer of free credit monitoring, as detailed below.

Other Important Information

As a precaution, CareCentrix has arranged with AllClear ID to help you protect your identity at no cost to you for a period of 24 months. You are pre-qualified for identity repair and protection services and have additional credit monitoring options available, also at no cost to you.

You can call AllClear ID with any concerns about your identity at 1-866-979-2595. This hotline is available from Monday to Saturday, 8 am to 8 pm Central Standard Time.

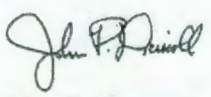
We have also included additional steps you could consider at any time if you ever suspect you've been the victim of identity theft, as well as a publication with information and tips to protect yourself from tax-related identity theft from the IRS. We offer this out of an abundance of caution so that you have the information you need to protect yourself.

For More Information

For more information about this incident, call toll-free 888-571-7348.

We take the security of your information very seriously, and regret any uncertainty or inconvenience that this incident may have caused you.

Sincerely,



John P. Driscoll
Chief Executive Officer
CareCentrix, Inc.

AllClear Identity Theft Protection

We have arranged to have AllClear ID help you protect your identity for 24 months at no cost to you, effective on the date of this notice. You are pre-qualified for identity repair and protection services and have additional credit monitoring options available, also at no cost to you.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-866-979-2595 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. 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 1-866-979-2595 using the following redemption code: Redemption Code.

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

Important Identity Theft Information: Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

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 below.

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com
- TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.800.525.6285
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00, (or in certain states such as Massachusetts, no more than $5.00), each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

Suggestions if You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1- 877-IDTHEFT (438-4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.
- Keep complete records of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: http://www.ftc.gov/idtheft; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

Identity Theft Information for Taxpayers

Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

You may be unaware that this has happened until you e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying it has identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS about:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages or other income from an employer for whom you did not work.

Steps for victims of identity theft

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at identitytheft.gov.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
  - www.Equifax.com 1-888-766-0008
  - www.Experian.com 1-888-397-3742
  - www.TransUnion.com 1-800-680-7289
- Close any financial or credit accounts opened by identity thieves

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.
- Complete IRS Form 14039, *Identity Theft Affidavit*, if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach form to your paper return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

More information is available at: IRS.gov/identitytheft or FTC's identitytheft.gov.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, *Identity Theft Affidavit*, only if your Social Security number has been compromised and IRS has informed you that you may be a victim of tax-related identity theft or your e-file return was rejected as a duplicate.

How you can reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. Taxes. Security. Together. We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal data. Don't routinely carry your Social Security card, and make sure your tax records are secure.

See Publication 4524, *Security Awareness for Taxpayers* to learn more.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Publication 5027 (Rev. 12-2015) Catalog Number 67495R Department of the Treasury **Internal Revenue Service** www.irs.gov

04-04-2