NTT DATA, Inc.
100 City Square
Boston, MA 02129
Tel: +1 617 241 9200 Fax: +1 617 241 8032
Email: info@nttdata.com

STATE OF NH
DEPT OF JUSTICE
2016 MAY -9 AM 11:55

NTT DATA
Global IT Innovator

May 4, 2016

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

RE: Notification of Data Security Breach Incident

Dear Sir/Madame:

This letter is being sent in accordance with state 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 (1) state resident on about April 22, 2016 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 individuals on May 4, 2016.

We are offering two (2) years of credit monitoring and identity theft services for the affected individuals through Experian. 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 does not recur. This includes access and storage restrictions as well as enhanced transmission procedures.

We have notified the three Consumer Reporting Agencies of this incident. Should you have any additional questions, you may contact me directly at 617-517-1379.

Sincerely,

Katrina I. Kropa
Sr. Vice President, Employment & Litigation Counsel

/crd
Enclosure

Return mail will be processed by: IBC
PO Box 1122
Charlotte, NC 28201-1122
PO #122004A

1 00000001

NTT DATA
Global IT Innovator

May 4, 2016

Dear Colleague,

As you know by now, on April 22, 2016, NTT DATA was targeted by a criminal "phishing" scam resulting in the unauthorized disclosure of W-2 tax reporting information for a number of employees, including yours. This is a crime that we are taking very seriously. You can find more details about this incident in the enclosed FAQ document.

I'd like to apologize on behalf of the company for what's happened. This has been a very upsetting event for all of us who were impacted. We continue to work closely with the FBI and US Internal Revenue Service to address the cause of this event and identify the criminals responsible. Be assured that the privacy and protection of your personal information is very important to the company. An intensive internal audit and remediation plan is underway to prevent this type of data security breach from happening again.

Enclosed you will also find details for the credit monitoring services NTT DATA has arranged for all impacted employees. Please take advantage of these services to help further protect your personal information. If you haven't already done so, we also recommend that you complete and submit Form 14039 to the IRS, which will give permission to block your account and prevent fraudulently filed returns.

Again, we are deeply sorry that this happened and are committed to the safeguarding of company and employee information. We will keep you updated on any further developments related to this incident. In the interim, if you have any questions about what has happened or the content of this package, you can contact 877-690-7014.

Sincerely,

Steve Chapman
President, Financial Services

On behalf of NTT DATA, I am writing to inform you about a recent incident and to provide information to help you navigate the IRS process and enroll in a credit monitoring service described below. On Friday, April 22, 2016, we learned that Personal Identifiable Information (PII) data of certain current and former employees of NTT DATA had been stolen. The affected employees were those who received income from the Carlisle & Gallagher Consulting Group business unit between January 1 and December 31, 2015. We take security very seriously and deeply regret that this incident occurred.

NTT DATA was a victim of an emerging "phishing" scheme that purports to be from company executives requesting personal information on employees. On Friday, April 22, 2016, an employee received an email that appeared to be from an NTT DATA executive asking the employee to send a file containing 2015 W2 tax documents. The email was in fact not from an NTT DATA executive, but was a phishing email masked to imitate an email from that executive. The employee responded by transmitting the data, which then went to an unknown person outside the company.

The W2 data that were released include names, addresses, social security numbers and earnings information. NTT DATA takes this matter as a serious violation and breach of procedures, and has taken immediate steps to minimize the risk to each of us and to help prevent incidents of this kind in the future. We have contacted the FBI Internet Criminal Complaint Center and filed a case with them. We have also contacted the Internal Revenue Service civil and criminal divisions to alert them to the theft and are actively supporting each organization's respective investigations.

We have engaged Experian to provide each of you with credit monitoring services for 24 months. In order to obtain these services you will need to enroll in ProtectMyID through the following steps:

1. ENSURE **That You Enroll By: July 31, 2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/enroll**
3. PROVIDE **Your Activation Code: PE3YSACG3**

If you have questions or need an alternative to enrolling online, please call 877-441-6943 and provide engagement #: **PC101188.**

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH PROTECTMYID MEMBERSHIP:

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**.
- **Surveillance Alerts for**:
  - **Daily 3-Bureau Credit Monitoring**: Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
  - **Internet Scan**: Alerts if your personal information is located on sites where compromised data is found, traded or sold.
  - **Change of Address**: Alerts of any changes in your mailing address.
- **Identity Theft Resolution**: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
- **$1 Million Identity Theft Insurance**[1]: Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
- **Lost Wallet Protection**: If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-441-6943.

[1]Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additionally, there are a number of steps the Internal Revenue Service recommends each of us take as soon as possible to protect ourselves from identity theft following this incident.

- Please read the attached brochure from the Internal Revenue Service. It contains information on ways you can protect yourself.
- If you have not already done so, immediately file IRS Form 14039, which is attached to this letter. We have pre-filled in the brief description of the identity theft violation. You can complete the form, attach a copy of your identification, and fax it to the IRS. It will be kept on file for three years as an alert to the IRS to watch for suspicious tax filings.
- File your 2015 tax returns as soon as possible. A recent scam is for a thief to steal W2 forms and then quickly file tax returns using that information and receive your tax refund.
- 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 Washington DC, Florida or Georgia, 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.

In addition, you should 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 also 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. You may contact the nationwide credit reporting agencies at:

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

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 AN INDIANA RESIDENT: For additional steps you may want to take to protect yourself please read the Indiana Identity Theft Prevention section online at www.IndianaConsumer.com for more information about situation-specific actions and responses.

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

Please know that we sincerely regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact us at 877-690-7014 if you have any questions or concerns.

Sincerely,

Dean M. Williams
Executive Vice President, Human Resources

Form **14039** (April 2016)	Department of the Treasury - Internal Revenue Service **Identity Theft Affidavit**	OMB Number 1545-2139

Complete this form if you need the IRS to mark an account to identify questionable activity.

Section A - Check the following boxes in this section that apply to the specific situation you are reporting *(Required for all filers)*

☐ 1. I am submitting this Form 14039 for myself

☐ 2. I am submitting this Form 14039 in response to a mailed 'Notice' or 'Letter' received from the IRS. If person in **Section C** received IRS 'Notice CP 2000', or other IRS Notice questioning income, follow the instructions on that IRS 'Notice' or 'Letter'.
- Please provide 'Notice' or 'Letter' number(s) on the **line to the right** _____

☐ 3. I am submitting this Form 14039 on behalf of my dependent.
Please complete **Section F** on reverse side of this form.
Caution: If you are filing this on behalf of a Minor or Dependent, filing this form will protect his or her tax account but it will **not** prevent the dependent in **Section C** below from being claimed as a dependent by another person.

☐ 4. I am submitting this Form 14039 on behalf of another person *(other than my dependent)*.
- Please complete **Section F** on reverse side of this form.

Section B – Reason For Filing This Form *(Required)*

Check only **ONE** of the following boxes that apply to the person listed in **Section C** below.

☐ 1. **Federal tax records affected** and I am a victim of identity theft

☐ 2. **Federal tax records not affected** and I am a victim of identity theft, or an event has affected/compromised my personal information placing me at-risk to be a future victim of identity theft.

Please provide an explanation of the identity theft issue, how you became aware of it and provide relevant dates.
A company that issued me a paycheck during calender year 2015 was the victim of an emerging "phishing" scheme that purports to be from company executives requesting personal information on employees. On Friday, April 22, 2016, an employee transmitted 2015 W2 tax documents, including mine, in response to an email that appeared to be from a company executive asking for 2015 W2 tax documents. The email was in fact not from a company executive, but was a phishing email masked to imitate an email from him. The company notified me of the incident on April 22, 2015. The company also notified the IRS and the FBI of the incident on April 22, 2015.

Section C – Name and Contact Information of Identity Theft Victim or Potential Victim *(Required)*

Taxpayer's last name	First name	Middle initial	**Taxpayer Identification Number** *(Please provide your 9-digit SSN or ITIN)*

Current mailing address *(apartment or suite number and street, or P.O. Box)* If deceased, please provide last known address.

City	State	ZIP code

Tax Year(s) in which you experienced identity theft *(If not known, enter 'Unknown' in one of the boxes below)*

								Last tax year a return was filed

Address used on last filed tax return *(If different than 'Current')*	**Names used on last filed tax return** *(If different than 'Current')*

City (on last tax return filed)	State	ZIP code

Telephone number with area code *(Optional) If deceased, please indicate 'Deceased'*

Home telephone number Cell phone number

Best time(s) to call

Language in which you would like to be contacted ☐ English ☐ Spanish

Section D – State or Federal Issued Identification *(Required)*

Submit this completed form and a **clear and legible** photocopy of **at least one of the following** documents to verify the identity of the person listed in **Section C** above. **If necessary, enlarge photocopies so all information is clearly visible.**

Check the box next to the document(s) you are submitting:

☐ Driver's license ☐ Social Security Card ☐ Passport ☐ Valid U.S. Federal or State government issued identification**

** Federal employees should not copy his or her employee identification cards as 18 U.S.C. prohibits doing so.

Section E – Penalty of Perjury Statement and Signature *(Required)*

Under penalty of perjury, I declare that, to the best of my knowledge and belief, the information entered on this Form 14039 is true, correct, complete, and made in good faith.

Signature of taxpayer, or representative, conservator, parent or guardian	Date signed

Section F – Representative, conservator, parent or guardian information *(Required if completing Form 14039 on someone else's behalf)*

Check only **ONE** of the following five boxes next to the reason you are submitting this form

☐ **1. The taxpayer is deceased and I am the surviving spouse.** *(No attachments are required, including death certificate)*

☐ **2. The taxpayer is deceased and I am the court-appointed or certified personal representative.**
Attach a copy of the court certificate showing your appointment.

☐ **3. The taxpayer is deceased and a court-appointed or certified personal representative has not been appointed.**
- o Attach copy of death certificate or formal notification from a government office informing next of kin of the decedent's death.
- o Indicate your relationship to decedent: ☐ Spouse ☐ Child ☐ Parent/Legal Guardian ☐ Other _____

☐ **4. The taxpayer is unable to complete this form and I am the appointed conservator or have Power of Attorney/Declaration of Representative authorization per IRS Form 2848.**
- o Attach a **copy** of documentation showing your appointment as conservator or POA authorization.
- o If you have an IRS issued **Centralized Authorization File (CAF) number, enter the nine-digit number:**

☐☐☐☐☐☐☐☐☐

☐ **5. The victim or potential victim is a 'minor'. 'Minor' as defined per the state in which 'minor' resides.**
By checking this box and signing below you are indicating that you are an authorized representative, as parent, guardian or legal guardian, to file a legal document on the child's behalf.
- o Indicate your relationship to minor: ☐ Parent/Legal Guardian ☐ Fiduciary Relationship per IRS Form 56 ☐ Power of Attorney ☐ Other _____

Representative's name		
Last name	First name	Middle initial
Last four digits of Representative's Taxpayer ID number	Representative's telephone number *(include area code)*	

Representative's current mailing address *(apt., suite no. and street, or P.O. Box)*

City	State	ZIP code

Instructions for Submitting this Form

Submit this to the IRS via **Mail** or **FAX** to specialized IRS processing areas dedicated to assist you. In **Section C** of this form, be sure to include your Social Security Number or Individual Taxpayer Identification Number in the 'Taxpayer Identification Number' field.

Help us avoid delays:
Choose one method of submitting this form either by Mail or by FAX, not both. Please provide clear and readable photocopies. Note that 'tax returns' may not be submitted to either the mailing address or FAX number provided below.

Submitting by Mail	Submitting by FAX
• **If you checked Box 1 in Section B of Form 14039, are unable to file your tax return electronically because the primary and/or secondary SSN was misused, attach Form 14039 and documentation to your paper tax return** and submit to the IRS location where you normally file your tax return. **If you have already filed your paper return,** submit this Form 14039 and documentation to the IRS location where you normally file. Refer to the 'Where Do You File' section of your return instructions or visit IRS.gov and input the search term 'Where to File'. • **If you checked Box 1 in Section B and are submitting this Form 14039 in response to a notice or letter received from the IRS,** return this form and documentation **with a copy of the notice or letter** to the address contained in the notice or letter. • **If you checked Box 2 in Section B of Form 14039 (no current tax-related issue),** mail this form and documentation to: **Internal Revenue Service** Fresno, CA 93888-0025	• **If you checked Box 1 in Section B of Form 14039 and are submitting this form in response to a notice or letter received from the IRS that shows a reply FAX number,** FAX completed Form 14039 and documentation with a copy of the notice or letter to that number. • **Include a cover sheet marked 'Confidential'.** If no FAX number is shown on the notice or letter, follow the mailing instructions on the notice or letter. • **If you checked Box 2 in Section B of Form 14039 (no current tax-related issue),** FAX this form and documentation toll-free to: **855-807-5720**

Privacy Act and Paperwork Reduction Notice

Our legal authority to request the information is 26 U.S.C. 6001. The primary purpose of the form is to provide a method of reporting identity theft issues to the IRS so that the IRS may document situations where individuals are or may be victims of identity theft. Additional purposes include the use in the determination of proper tax liability and to relieve taxpayer burden. The information may be disclosed only as provided by 26 U.S.C. 6103. Providing the information on this form is voluntary. However, if you do not provide the information it may be more difficult to assist you in resolving your identity theft issue. If you are a potential victim of identity theft and do not provide the required substantiation information, we may not be able to place a marker on your account to assist with future protection. If you are a victim of identity theft and do not provide the required information, it may be difficult for IRS to determine your correct tax liability. If you intentionally provide false information, you may be subject to criminal penalties. You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by section 6103. Public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. If you have comments concerning the accuracy of these time estimates or suggestions for making this form simpler, we would be happy to hear from you. You can write to the Internal Revenue Service, Tax Products Coordinating Committee, SE:W:CAR:MP:T:T:SP, 1111 Constitution Ave. NW, IR-6526, Washington, DC 20224. Do not send this form to this address. Instead, see the form for filing instructions. Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Identity Theft Prevention and Victim Assistance

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, victim assistance and outreach.

What is tax-related identity theft?

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

Know the warning signs

You may be unaware you are a victim of tax-related identity theft until you file your tax return and discover a return was already filed using your SSN.

Be alert to possible tax-related identity theft if you receive an IRS notice or letter that states:

- You filed more than one tax return, and/or
- You owe additional tax, have a refund offset or you have IRS collection actions taken for a year you didn't file a return, or
- IRS records indicate you received wages from an employer unknown to you.

How to reduce your risk

- Don't routinely carry your Social Security card or any document with your SSN on it.
- Don't give a business your SSN just because they ask – only provide it when absolutely necessary.
- Don't give your personal information over the Internet, phone or mail unless you initiated the contact and/or know the person or business you are dealing with.
- Protect personal information at home on your computers and devices by using
  - firewalls,
  - anti-spam/virus software,
  - update security patches often and
  - change passwords for online Internet accounts on a regular basis.
- Review your credit report annually.
- Review your Social Security Administration earnings statement annually.

Steps for victims of identity theft

1. Call companies where you know fraud occurred.
2. Contact one of the three major credit bureaus to place a 'fraud alert' immediately on your credit record and request a copy of your credit report.
   - Equifax.com - 1-800-525-6285
   - Experian.com - 1-888-397-3742
   - TransUnion.com - 1-800-680-7289
3. Use the Federal Trade Commission's online complaint form at ftc.gov/complaint, or call the FTC at 1-877-438-4338, or TTY 1-866-653-4261.
4. Follow FTC's guidance at identitytheft.gov. Identitytheft.gov is the federal government's one-stop resource to help you report and recover from identity theft.

Additional steps for victims of tax-related identity theft

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

1. Respond immediately to any IRS issued notice; call the number provided on the IRS notice and verify you are talking to an IRS employee.
2. Complete IRS Form 14039, Identity Theft Affidavit, irs.gov/pub/irs-pdf/f14039.pdf. Mail or fax the form according to instructions. If you are responding to an IRS notice, be sure to include a copy of the notice.
   - You only need to file Form 14039 one time.
   - If you are an Identity Protection PIN recipient, you don't need to file a Form 14039 to tell us you are a victim of tax-related identity theft.
3. Continue to pay your taxes and file your tax return, even if you must do so by paper.
4. If you previously contacted the IRS and don't have a resolution to your identity theft issue, you may call the IRS for specialized assistance at 1-800-908-4490. Hours of operation: Monday - Friday, 7 a.m. - 7 p.m. your local time (Alaska & Hawaii follow Pacific Time).

Remember

The IRS doesn't 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. Neither does the IRS call with threats of lawsuits or arrests

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 guidance above, *"Steps for victims of identity theft"*.

Publication 4535 (EN-SP) (Rev. 11-2015) Catalog Number 48656M Department of the Treasury **Internal Revenue Service** www.irs.gov

Prevención de Robo de Identidad y Asistencia a las Víctimas

El robo de identidad constituye una carga para sus víctimas y presenta un desafío para muchas empresas, organizaciones y gobiernos, incluyendo el IRS.

El IRS combate este delito con una estrategia agresiva de prevención, detección, asistencia a las victimas e información.

¿Qué es el robo de identidad relacionado con los impuestos?

El robo de identidad relacionado con los impuestos ocurre cuando alguien utiliza indebidamente su número de Seguro Social para presentar una declaración de impuestos falsa y reclamar un reembolso fraudulento. Si usted se convierte en una víctima, estamos comprometidos a resolver su caso rápidamente.

Conozca las señales de advertencia

Puede que usted no esté consciente que es una víctima de robo de identidad relacionado con los impuestos, hasta que presente su declaración de impuestos y descubra que ya se ha presentado una declaración utilizando su SSN.

Esté alerta por posible robo de identidad si recibe un aviso o carta del IRS que dice que:

- Usted presentó más de una declaración de impuestos y/o
- Usted adeuda impuesto adicional, tiene compensado un reembolso o se han tomado acciones de cobro en su contra por un año que no presentó la declaración de impuestos o
- Los registros del IRS indican que usted recibió salarios de un empleador que desconoce.

Cómo reducir su riesgo

- No cargue constantemente su tarjeta de Seguro Social o cualquier documento con su SSN en él.
- No dé a un negocio su SSN sólo porque lo pidan — solamente proporciónelo cuando sea absolutamente necesario.
- No dé su información personal por Internet, teléfono o correo, a menos que usted haya iniciado el contacto y/o conozca la persona o el negocio con quién trata.
- Proteja su información personal en la casa, en sus computadoras y dispositivos por medio de:
  - firewalls,
  - Software contra spam y virus
  - Actualización frecuente de los parches de seguridad y
  - Cambio regular de las contraseñas para las cuentas en Internet.
- Revise anualmente su informe de crédito.
- Revise anualmente su información de ingresos de la Administración del Seguro Social

Pasos para las víctimas de robo de identidad

1. Comuníquese con las compañías donde usted sabe que el fraude ocurrió.
2. Comuníquese con una de las tres principales agencias de crédito para colocar una "alerta de fraude" inmediatamente en su registro de crédito y solicite una copia de su informe de crédito.
   - Equifax.com - **1-800-525-6285**
   - Experian.com - **1-888-397-3742**
   - TransUnion.com - **1-800-680-7289**
3. Utilice el formulario de querellas en línea de la Comisión Federal de Comercio (FTC, por sus siglas en inglés), en ftc.gov/complaint, o llame al FTC al 1-877-438-4338 o si utiliza el sistema TYY al 1-866-653-4261.
4. Siga las guías de la FTC en identitytheft.gov. Identitytheft.gov es el recurso centralizado del gobierno federal para ayudarle a informar y recuperarse del robo de identidad.

Pasos adicionales para las víctimas de robo de identidad relacionado con los impuestos

Si su SSN está en riesgo y usted conoce o sospecha que es una víctima de robo de identidad "relacionado con los impuestos", por favor, tome estos pasos adicionales:

1. Responda inmediatamente a cualquier aviso emitido por el IRS; llame al número en el Aviso del IRS y verifique que está hablando con un empleado del IRS.
2. Complete el Formulario 14039(SP), Declaración Jurada sobre el Robo de Identidad, en irs.gov/pub/irs-pdf/f14039sp.pdf. Envíe el formulario por correo o fax según las instrucciones. Si está respondiendo a un Aviso del IRS, asegúrese de incluir una copia del aviso.
   - Usted sólo necesita presentar el Formulario 14039(SP) una vez.
   - Si usted recibe un PIN de Protección de la Identidad, no necesita presentar el Formulario 14039(SP) para comunicarnos que es una víctima de robo de identidad relacionado con los impuestos.
3. Continúe con el pago de sus impuestos y presente su declaración de impuestos, incluso si tiene que hacerlo en un formulario impreso.
4. Si anteriormente se comunicó con el IRS y no tienen una resolución a su problema de robo de identidad, usted puede llamar al IRS para la asistencia especializada, al 1-800-908-4490. Horas de operación: lunes a viernes de 7 am. a 7 pm., hora local. (Alaska y Hawái siguen el horario del Pacífico).

Sobre las filtraciones de información de datos y sus Impuestos

No todas las filtraciones de información o accesos ilegales a la computadora causan el robo de identidad relacionado con los impuestos. Es importante saber qué tipo de información personal fue robada.

Si usted es víctima de una filtración de datos, manténgase en comunicación con la compañía para conocer lo que están haciendo para protegerle a usted y siga lo indicado anteriormente bajo "Pasos para las víctimas de robo de identidad".

Recuerde

EL IRS nunca inicia el contacto con contribuyentes por email, ni solicita por email sus datos personales ni información financiera. Esto aplica a cualquier vía de comunicación electrónica, tal como mensajes de texto y los medios sociales. El IRS tampoco llama con amenazas de demandas o arrestos

NTT DATA
Global IT Innovator

Frequently Asked Questions

Q1: What happened?

A1: On Friday, April 22, 2016, NTT DATA learned that Personal Identifiable Information (PII) data of certain current and former employees of NTT DATA who received a paycheck between January 1 and December 31, 2015, had been stolen earlier in the day.

Q2: How did this happen?

A2: NTT DATA was a victim of an emerging "phishing" scheme that purports to be from company executives requesting personal information on employees (Reference: https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s). On Friday, April 22, 2016, an employee received an email that appeared to be from an NTT DATA executive asking the employee to send a file containing 2015 W2 tax documents. The email was in fact not from an NTT DATA executive, but was a phishing email masked to imitate an email from him. The employee responded by transmitting the data which went to an unknown person outside the company.

Q3: When did this happen?

A3: The crime occurred Friday, April 22, 2016.

Q4: Who was affected?

A4: Certain current and former employees of NTT DATA who received income from the Carlisle & Gallagher Consulting Group unit between January 1 and December 31, 2015.

Q5: What actions has NTT DATA taken?

A5: The company has notified all individuals whose information was exposed so that they can take appropriate action to protect themselves. We take this matter as a serious violation and breach of procedures and have taken immediate steps to minimize the risk to each person impacted and to help prevent incidents of this kind in the future.

We have contacted the FBI Internet Criminal Complaint Center and filed a case with them. We have also contacted the Internal Revenue Service civil and criminal divisions to alert them to the theft and are actively supporting each organization's respective investigations.

We have provided each person impacted with information from the IRS, including directions on how to notify the IRS to alert them to possible fraud.

Additionally, we are in the process of establishing credit monitoring services for each person indicated and will communicate those details as soon as they are available. Details will be sent to your home address with instructions on how to enroll.

Q6: What personal information was exposed?

A6: The information theft included a copy of impacted individual's W2 form, which includes the individual's name, address, social security number and earnings information.

Q7: Were Social Security Numbers exposed?

A7: Yes.

Q8: Were credit card numbers exposed?

A8: No.

Q9: Were bank account numbers exposed?

A9: No.

Q10: Were driver's license numbers exposed?

A10: No.

Q11: How do I know if my personal information was exposed? And if so, what should I do?

A11: NTT DATA notified each impacted individual by email on Friday, April 22. If you received an email then your W2 information was exposed.

There are a number of steps you can take:

1. You should complete the IRS form 14039 that was provided. Fax it to the IRS along with the identification required by the form. The fax number is (855) 807-5720.

2. File your tax returns as soon as possible to prevent any thief from stealing your refund.

3. Contact the IRS Identity Theft Hotline at (800) 908-4490. When you call, they will ask you a series of questions to prove your identity, and will 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.

4. If you live in Washington, D.C., Florida, or Georgia, 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.

5. You can contact one of the three credit reporting bureaus and place a 90-day Initial Fraud Alert on your credit file (further directions below). That bureau will notify the other two bureaus and will send you confirmation that the alert has been placed along with a free copy of your credit report. Review your credit report carefully to see if there has been

any new credit requested. Mark on your calendar to call back and renew this Alert again every 90 days.

6. Enroll in the credit monitoring service NTT DATA will announce shortly. This service will actively look for unusual activity on your credit report and notify you of activity on your file. Further information will be provided in the near future to your home address. Please look for the letter in the coming days.

While no credit card or bank account information was impacted, you should always review your account statements carefully to see if there have been any charges that you have not authorized. If there are, contact your bank or credit card issuer immediately at the number on your monthly statement.

Q12: How will I know if my information was used by someone else?

A12: The best way to find out if someone has used your personal information to file a false tax return is to call 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 will 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.

You should also get a copy of your credit report from one of the three credit reporting bureaus. The credit report will show if there has been any new credit requested using your information. You can get a copy of your credit report from www.annualcreditreport.com.

Q13: Should I close my bank account or change my account or credit card number?

A13: No bank account or credit card information was disclosed. However, you should always review your account activity carefully.

Q14: How do I put an Initial Fraud Alert on my credit report?

A14: US law allows you to put a "fraud alert" on your credit report. This is a free service. A 90-day Initial Fraud Alert puts a statement on your credit file that you may have been or are about to become the victim of identity theft or other fraud. If you specify a telephone number, anyone using your credit report must call that number or take reasonable steps to verify your identity to confirm that a credit application is not the result of identity theft.

After you put a fraud alert on your credit report, you will be asked to provide proof of your identification when you apply for credit. This may limit your ability to apply for instant credit for in-store purchases but it should not interfere with your daily use of existing credit cards or banking accounts.

You can put a 90-day Initial Alert on your credit report by contacting one of the three major credit bureaus. The one you contact will notify the others. This will entitle you to a free credit report. You will receive confirmation of the alert from the bureau you contact. At the end of the 90 day period you may call back and place an additional Initial Fraud Alert on your credit file. We suggest that you do this every 90 days for at least one year.

Q15: How can I get in touch with the credit bureaus?

A15: There are three major credit bureaus. They are:

Experian:

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

Equifax:

800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241

Trans Union:

800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

Q16: Do I have to pay for a credit report?

A16: You are entitled to one free credit report a year from each of the three credit reporting bureaus. For example, this means that you can receive one today from Experian, you can then receive another in four months from Equifax, and you can receive another in eight months from TransUnion. By spacing out your requests for your free credit reports you can monitor your credit over the course of a year. If you want to receive more than one credit report form any of the credit reporting bureaus during the same year, you may have to pay a small charge.

Q17: How long will it take to get my credit report?

A17: You can access your credit report online at www.annualcreditreport.com. You can download or print the report from that site. You may also request the report by telephone (by calling 1-877-322-8228 and answering some questions to verify who you are) or by mail (by downloading the request form from www.annualcreditreport.com and mailing it to **Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281).**

If you request your report by phone or by mail it will take approximately two weeks to process the request, so you should allow two to three weeks for delivery to you.

Q18: What is a fraud alert?

A18: A fraud alert is a message added to your credit report that tells anyone who pulls a copy of your credit report that there is possible fraud associated with your account. It gives them a telephone number to call you before issuing any new credit.

An Initial Fraud Alert expires after 90 days. If you have been the victim of identity theft you may be able to place a 7-year fraud alert on your account. You can obtain more information online at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html.

Q19: How long does a fraud alert last?

A19: The Initial Fraud Alert lasts 90 days after it is placed on your report. You can remove the alert by calling the credit bureaus before the 90 days expires. You can place an additional alert every 90 days by calling one of the credit bureaus.

Q20: Will a fraud alert stop me from using my credit cards?

A20: No. A fraud alert requires the credit bureau to verify that you have asked to open a credit account. So a fraud alert may interfere with your ability to get immediate credit, for instance if you apply for instant credit at a department store. This is because the department store credit office will have to call you to verify your identity before issuing you credit. It will not stop you from using your credit cards.

Q21: Can I still apply for credit if I put a fraud alert on my credit report?

A21: Yes. The fraud alert may slow down the process of getting approval for credit because the fraud alert will require that the creditor verify your identity before approving new credit.

Q22: What should I watch out for on my credit report?

A22: Look for any accounts that you don't recognize especially new accounts. Look in the personal information section to see if the residence and employment information is correct or has changed. These things could be indications of fraud. If you see information you do not understand or that is wrong, call the credit bureau at the number on the report. If the information cannot be explained, contact your local police or sheriff's office.

Q23: If someone has used my information, what should I do?

A23: You should immediately notify your local police or sheriff's office and file a report of identity theft. Get a copy of the police report, because you may need to give a copy to the credit bureaus or creditors. Also contact one of the three credit bureaus and place a long term fraud alert on your account. For more information you can visit the website: www.consumer.gov/idtheft

Q24: Do I have to call all three credit bureaus?

A24: When you call one bureau, it will pass the report on to the other two. You should receive a confirming letter from each of the three bureaus. If you do not receive confirmations from all three credit bureaus, call the bureau which did not confirm the alert.

Q25: Will NTT DATA contact me to ask for my personal information because of this event?

A25: No. We already have your tax information. We do not ask for bank account information or personal identification numbers (PINs) or for your full credit card number unless you request an automatic deposit of your paycheck or you make a purchase or donation. If you are contacted directly by someone who claims to be with NTT DATA and who ASKS YOU FOR YOUR PERSONAL INFORMATION, contact us and your local sheriff's office **immediately** to report the suspicious contact.

Q26: I have already been contacted directly by someone claiming to be from NTT DATA or a law enforcement agency asking for my personal information (e.g., social security number, etc.). Did you contact me?

A26: No. We did not contact you. We already have your tax information and do not ask for bank account information or personal identification numbers (PINs) or for your full credit card number unless you request an automatic deposit of your paycheck or you make a purchase or donation. If you were contacted directly by someone who claimed to be with NTT DATA or law enforcement and who ASKS YOU FOR YOUR PERSONAL INFORMATION, please contact us and your local sheriff's office **immediately** to report the suspicious contact.

Q27: Will you contact me by email to sign up for credit monitoring/identity protection services?

A27: No. You should be aware of scam email campaigns targeting individuals of a recent data breech. These scams, designed to capture personal information (known as "phishing"), appear as if they are from NTT DATA and include a "click here" link for credit monitoring. These emails are NOT from us. Do not reply to the email or reach out to the senders in any way. Do not supply any information on the website that may open, if you have clicked on a link in email. Do not open any attachments that arrive with email.

The company will not call individuals regarding this incident and NTT DATA is not asking for any information over the phone or via email. For more guidance on recognizing scam email, please visit the FTC Website: http://www.consumer.ftc.gov/articles/0003-phishing

REFERENCE SHEET FOR WEBSITES:

Credit Reporting Bureaus:

Annual Credit Reports:
http://www.annualcreditreport.com

Experian:
888-397-3742
P.O. Box 2002
Allen, TX 75013
http://www.experian.com

Equifax:
800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
http://www.equifax.com

Trans Union:
800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
http://www.transunion.com

Internal Revenue Service: www.irs.gov

Identity Theft and Fraudulently Obtained Tax Refunds
https://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/IRS-Identity-Theft-and-Fraudulently-Obtained-Tax-Refund-Checks

Report Suspected Tax Fraud
https://www.irs.gov/Individuals/How-Do-You-Report-Suspected-Tax-Fraud-Activity%3F

Request Copy of Fraudulent Tax Returns
https://www.irs.gov/Individuals/Instructions-for-Requesting-Copy-of-Fraudulent-Returns

Federal Trade Commission: www.ftc.gov

Identity Theft
Hotline: 877-ID-THEFT (877-438-4338)
https://www.identitytheft.gov/

Phishing Emails

http://www.consumer.ftc.gov/articles/0003-phishing

https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s

Tax Related Identity Theft

https://www.consumer.ftc.gov/articles/0008-tax-related-identity-theft

Filing a Complaint with the FTC

https://www.ftccomplaintassistant.gov
1-877-FTC-HELP (1-877-382-4357) (TTY: 1-866-653-4261)

Social Security Administration

Fraud Hotline: 800-269-0271
Benefits Statement: 800-772-1213
http://www.ssa.gov

Privacy Rights Clearing House Identity Theft Resources

http://www.privacyrights.org/identity.htm
This not-for-profit organization provides statistics, fact sheets and government records about identity theft.

Identity Theft Resource Center

http://www.idtheftcenter.org
This not-for-profit organization is dedicated exclusively to identity theft. It provides consumer and victim support about identity theft and includes resources, consumer alerts and instructions for victims.