

JONES DAY

2727 NORTH HARWOOD STREET • DALLAS, TEXAS 75201.1515
TELEPHONE: +1.214.220.3939 • FACSIMILE: +1.214.969.5100

March 4, 2016

DIRECT NUMBER: (214) 969-3788
JJOHNSON@JONESDAY.COM

Via First Class Mail

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

STATE OF NH
DEPT OF JUSTICE
2016 MAR -8 AM 11:28

Re: Recent Acronis, Inc. Security Incident

Dear General Foster:

I am writing to give you notice of a security incident affecting employees of our client, Acronis, Inc. (“Acronis”). This breach involves an estimated 17 individuals residing in your State.

On or about February 28, 2016, a sophisticated hacker was able to “spoof” our CEO’s email address, meaning that the hacker was able to send an email to one of our employees that looked like it came from our CEO. The hacker’s email asked for copies of employee W-2 forms. Notably, this hacker did not actually hack into our client’s systems, and our systems were never compromised. But believing the email request to be legitimate, one of our employees sent W-2 forms to this unknown individual on February 29, 2016.

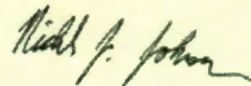
The employee W-2 forms included the name, postal address, social security number, marital status, employer information, salary details, employee benefit information, and certain tax return data, such as withholding information, exemptions and allowances of employees.

Acronis sent an email notification of this incident to current employees and will notify all affected individuals promptly by formal notification letter. An exemplar copy of the notice letter is enclosed for your information. As the enclosed letter explains, Acronis has strengthened internal controls, notified law enforcement, and provided credit protection services for two years, free-of-charge.

The Honorable Joseph Foster
March 4, 2016
Page 2

Should any significant new information arise, we will promptly inform you. In the meantime, please do not hesitate to contact me if I can provide you with any additional information.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard J. Johnson". The signature is written in a cursive style with a prominent flourish at the end.

Richard J. Johnson

Enclosure

Cc: Todd McClelland, Jones Day

NOTICE OF DATA BREACH

[DATE]

<title> <first name> <last name>
<address>
<city>, <state> <postal code>

Dear <title> <last name>:

As a conscientious member of the technology industry, we take very seriously our responsibility to safeguard all sensitive and confidential information provided to us. For this reason, we are writing to inform you of an incident involving your personal information that occurred at Acronis, Inc.

What Happened

We deeply regret that we are contacting you today to inform you of an incident that has resulted in unauthorized access by an unknown individual to your personal information.

On or about February 28, 2016, a sophisticated hacker was able to “spoof” our CEO’s email address, meaning that the hacker was able to send an email to one of our employees that looked like it came from our CEO. The hacker’s email asked for copies of employee W-2 forms. Notably, this hacker did not actually hack into our systems, and our systems were never compromised. But believing the email request to be legitimate, one of our employees sent W-2 forms, including yours, to this unknown individual on February 29, 2016. Upon discovery of the incident, we immediately notified law enforcement and have taken additional steps to prevent future incidents.

What Information Was Involved

The employee W-2 forms included your name, postal address, social security number, marital status, employer information, salary details, employee benefit information, and certain tax return data, such as withholding information, exemptions, and allowances.

What We Are Doing To Protect You

We have taken measures to minimize future risks to your privacy by strengthening internal controls, notifying law enforcement, and providing you a full package of credit protection services for two years, free-of-charge. This notification has not been delayed as a result of notifying law enforcement of the incident. For information on activating the credit protection services, please see the “Activate ProtectMyID Now in Three Easy Steps” on the first page of the attached document.

What You Can Do To Protect Yourself

We encourage you to remain vigilant by reviewing account statements and monitoring free credit reports. Enclosed you will find the steps you will need to take to enroll in the services we are making available to you. Also enclosed are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). We hope you will take full advantage of the resources we have provided at no cost to you.

Tax-Related Identity Theft

The IRS is warning taxpayers of tax-related identity theft, which is an incident where someone uses your stolen Social Security Number and other tax information to file a tax return claiming a fraudulent refund. If you e-file your tax return and discover that a return has already been filed using your Social Security Number, or if the IRS sends you a letter saying it has identified a suspicious return using your Social Security Number, you should visit the IRS's identity theft web page at <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> and follow the IRS's instructions. You can also visit that website in advance of any e-filing of your returns to explore possibly identity theft protections offered by the IRS.

For More Information

Should you wish to contact our Company directly about this matter and/or the protections available to you, please call _____ or write to Acronis Inc., _____.

The three major credit reporting agencies can provide information and assist you should you wish to have a "fraud alert" or "security freeze" placed on your credit file. The following table provides contact information for these organizations.

Company	Website	Telephone No.	Mail
Equifax	www.equifax.com	1-800-525-6285	P.O. Box 740241, Atlanta, GA 30374-0241
Experian	www.experian.com	1-888- 397-3742	P.O. Box 2104, Allen, TX 75013-0949
Trans Union	www.transunion.com	1-800-680-7289	P.O. Box 1000, Chester, PA 19022

The Federal Trade Commission (FTC) also can provide information about identity theft, fraud alerts, and security freezes. The FTC may be contacted through its website (<http://www.ftc.gov/>), by calling its toll-free telephone number (1-877-438-4338), or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Maryland and Oregon Residents

The Maryland Attorney General can be contacted through his website (<http://www.oag.state.md.us/>), by calling his toll-free telephone number (1-888-743-0023), or by mail at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202.

The Oregon Attorney General can be contacted through her website (<http://www.doj.state.or.us/about/pages/agoffice.aspx>), by calling her toll-free telephone number (1-877-877-9392), or by email at help@oregonconsumer.gov.

Please be assured that we are fully committed to protecting the information that you have entrusted to us and are extremely disappointed that this incident occurred. We value your service to our company and will diligently work to maintain the trust you have placed in us.

Sincerely,

Identify Theft Protection

To help protect your identity, we are offering a **complimentary two-year** membership of Experian's[®] ProtectMyID[®] Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. **ENSURE That You Enroll By: June 30, 2016** (Your code will not work after this date.)
2. **VISIT the ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. **PROVIDE Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement #: **PC99705**.

ADDITIONAL DETAILS REGARDING YOUR TWO-YEAR PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

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

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax[®] and TransUnion[®] credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** 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.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE[™], which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

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 877-371-7902.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (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.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➤ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax
1-800-525-6285
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-680-7289
www.transunion.com

➤ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with new credit application, which will prevent them from extending credit. A security freeze generally 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. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies. For more information on placing a security freeze on your credit file, please see the following page of this letter.

➤ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➤ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

➤ USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➤ OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

PLACING A SECURITY FREEZE ON YOUR CREDIT FILE

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 \$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: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance
Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.)
7. 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;
8. 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). Do not send cash through the mail.

The credit reporting agencies have three (3) 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 (5) 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 security freeze in order 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 proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as 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 (3) 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, 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 (3) business days after receiving your request to remove the security freeze.