

# Holland & Knight

800 17<sup>th</sup> Street, NW, Suite 1100 | Washington, DC 20006 | T 202-955-3000 | F 202-955-5564  
Holland & Knight LLP | www.hklaw.com

Christopher G. Cwalina  
Partner  
202-469-5230  
chris.cwalina@hklaw.com

RECEIVED  
SEP 05 2017  
CONSUMER PROTECTION

September 1, 2017

*VIA UPS NEXT DAY AIR*

Attorney General Gordon MacDonald  
Consumer Protection and Antitrust Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301  
Phone: (603) 271-3643

## **Re: Notice Pursuant to New Hampshire Statute § 359-C:19**

Dear Attorney General MacDonald:

Pursuant to New Hampshire Statute § 359-C:19, we are writing on behalf of Infinite Computer Solutions, Inc. (“Infinite”), to notify you of an unauthorized acquisition of personal information involving approximately seventeen (17) New Hampshire residents.

On July 27, 2017, Infinite confirmed that one of its test servers, which contained information of a limited number of employees for testing purposes, was compromised on or around May 26, 2017 by an unauthorized party. The test server was brought online for the purpose of auditing certain Infinite records; however, the server was inadvertently left online for a limited period of time after the auditing process was completed. During this period, an unauthorized actor obtained certain information on the server. Upon learning that this test server had been inadvertently left online, Infinite immediately took it offline, initiated an internal investigation to determine what occurred, and retained third-party experts to assist with its investigation. Infinite also notified law enforcement regarding this matter.

As soon as Infinite confirmed that an unauthorized actor obtained certain information on the server, Infinite immediately engaged the third-party forensic firm to conduct a manual review and analysis of the approximate 8,800 files at issue, to determine what personal information was potentially at issue, and who was impacted. While this analysis was ongoing, Infinite consulted with potential identity protection and mailing vendors. The third-party firm completed its manual review of the approximate 8,800 files on August 17, 2017. Upon receiving the third-party’s analysis, Infinite immediately began to review the third-party’s analysis to identify and verify the names and addresses, including states of

residence, of the individuals listed in the file. Infinite completed this review and matching process and determined New Hampshire residents were impacted on or around August 25, 2017. As soon as Infinite identified the addresses for impacted individuals, Infinite retained AllClear to provide notification, call center, and identity protection services. On or around August 28, 2017, Holland & Knight, on behalf of Infinite, provided copies of the notification letters and the address file to AllClear to complete the mailing process.

At this time, we believe the files at issue may have included human resources and employment related information, such as your name, date of birth, social security number, driver's license number, passport number, financial account information, Alien Registration number, and other employment-related documentation, including, if applicable, I-9 forms, W4 forms, direct deposit forms, life insurance forms, beneficiary forms, background investigation forms, drug testing forms, personnel action forms, emergency contact forms, and/or offer letters.

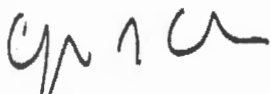
Infinite is notifying affected individuals and providing them with information on how they can protect their information. Infinite is offering two (2) years of identity protection services, at no cost, to potentially affected individuals. The details of these identity protection services and instructions for how to enroll, as well as information regarding additional steps individuals can take to help protect their information, is provided in the notice letter that will be mailed on or around September 5, 2017. Enclosed please find copies of this correspondence.

Infinite takes the protection of personal information very seriously and is making changes to existing policies and procedures designed to help prevent a similar occurrence from happening in the future. Below is the contact information for Niti Prothi, Vice President of Human Resources at Infinite:

Niti Prothi  
Vice President, Human Resources  
Infinite Computer Solutions Inc.  
15201 Diamondback Drive  
Suite 125  
(301) 355-7766  
[Niti.prothi@infinite.com](mailto:Niti.prothi@infinite.com)

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,



Christopher G. Cwalina



Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

September 5, 2017

## RE: NOTICE OF DATA BREACH

Dear John Sample:

Infinite Computer Solutions Inc. ("Infinite") is writing to let you know about a data security incident and to recommend steps that you can take to help protect yourself.

### What Happened

Infinite recently discovered that one of our test servers, which contained information of some of our employees for testing purposes, was compromised on or around May 26, 2017 by an unauthorized party. The test server was brought online for the purpose of auditing certain Infinite records; however, the server was inadvertently left online for a limited period of time after the auditing process was completed. During this period, an unauthorized actor obtained certain information on the server. Upon learning that this server was still online, Infinite immediately took it offline.

You have been identified as one of the individuals whose information was contained in the files that were compromised during this incident. We are notifying you of the incident in order to provide you with information and steps you can take to help protect your information.

### What Information Was Involved

At this time, we believe the files at issue may have included human resources and employment related information, such as your name, date of birth, social security number, driver's license number, passport number, financial account information, Alien Registration number, and other employment-related documentation, including, if applicable, I-9 forms, W4 forms, direct deposit forms, life insurance forms, beneficiary forms, background investigation forms, drug testing forms, personnel action forms, emergency contact forms, and/or offer letters.

### What We Are Doing

We take the protection of your information very seriously, and we sincerely apologize that this incident occurred. We are taking several steps to help protect your information, including providing **free identity protection services for two years**, as described further in this letter. Upon learning that this server was online, we initiated an internal investigation to determine what occurred and retained third-party experts to assist with our investigation. We have also notified law enforcement regarding this matter. In addition, we have made and continue to make changes to processes and procedures to help prevent a similar occurrence from happening again.



01-03-1-00

## What You Can Do

There are steps you can take to protect yourself in this situation, including enrolling in the free identity protection service we are offering. Details regarding the service and how to enroll are provided below.

### AllClear ID Protection Services

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

- AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-904-5755 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.
- AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](http://enroll.allclearid.com) or by phone by calling 1-855-904-5755 using the following redemption code:  
Redemption Code

If you would like to enroll your spouse or dependents in monitoring services, please contact AllClear ID at 1-855-904-5755 Monday through Saturday, 8 am to 8 pm Central Time.

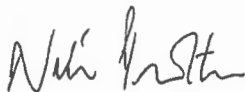
## For More Information

We also recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). We have attached information regarding additional actions you may consider to help reduce the chances of identity theft or fraud on your account as well as resources to obtain additional information about identity theft and ways to protect yourself.

## Questions and Concerns

We sincerely apologize that this incident occurred, regret any inconvenience it may cause you, and encourage you to take advantage of the AllClear ID services. Should you have additional questions or concerns regarding this matter, please do not hesitate to contact 1-855-904-5755.

Sincerely,



Niti Prothi  
Vice President, Human Resources  
Infinite Computer Solutions Inc.  
15201 Diamondback Drive  
Suite 125  
Rockville, MD 20850



## ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

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

A Fraud Alert is a consumer statement added to your credit report that alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. Once the fraud alert is added to your credit report, 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**  
PO Box 740241  
Atlanta, GA 30374  
1-800-525-6285  
www.equifax.com

**Experian**  
PO Box 4500  
Allen, TX 75013  
1-888-397-3742  
www.experian.com

**TransUnion**  
PO Box 2000  
Chester, PA 19016  
1-800-680-7289  
www.transunion.com

### ➤ **PLACE AN EXTENDED FRAUD ALERT ON YOUR CREDIT FILE**

You may also want to consider contacting the credit reporting companies and asking them to place an extended fraud alert. If you are a victim of identity theft and have created an Identity Theft Report, you can place an extended fraud alert on your credit file. It stays in effect for 7 years. When you place an extended alert, you can get 2 free credit reports within 12 months from each of the 3 nationwide credit reporting companies, and the credit reporting companies must take your name off marketing lists for prescreened credit offers for 5 years, unless you ask them to put your name back on the list.

### ➤ **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 entirely, which will prevent them from extending credit. 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 completed through each of the credit reporting companies. To obtain a security freeze from all credit reporting agencies, impacted individuals must contact each credit reporting agency separately and complete their respective security freeze request process. Fees may be required to be paid to the consumer reporting agencies in order to institute a security freeze on your credit file. To obtain a security freeze each credit reporting agency will require you to provide certain information to prove your identity, which may include your Full Name, Current and Prior Addresses, Social Security Number, Date of Birth, and/or Identification Card. With respect to minors, it is important to note that special state-by-state rules may apply regarding the availability of security freezes for minors.

- For information regarding Experian's security freeze process, see:  
<https://www.experian.com/freeze/center.html>
- For information regarding TransUnion's security freeze process, see:  
<https://www.transunion.com/credit-freeze/place-credit-freeze>
- For information regarding Equifax's security freeze process, see  
[https://www.freeze.equifax.com/Freeze/jsp/SFF\\_PersonalIDInfo.jsp](https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp)

### ➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit [www.annualcreditreport.com](http://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.



We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

➤ **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.

➤ **BE ON THE LOOKOUT FOR PHISHING SCHEMES**

We recommend that you be on the lookout for suspicious emails. Specifically, be on the lookout for phishing schemes, which are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator.

Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (look for misspellings in the email address). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate.

➤ **POLICE REPORT**

You may also have the right to file or obtain a police report.

➤ **SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT:**

The Federal Trade Commission ("FTC") has created the following summary of consumer rights under the Fair Credit Reporting Act, available at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>. Notably, the FTC states that: "The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under the FCRA. For more information, including information about additional rights, go to [www.ftc.gov/credit](http://www.ftc.gov/credit) or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580." As outlined in the FTC's summary, these rights include, but are not limited to the following:

- "You must be told if information in your file has been used against you."
- "You have the right to know what is in your file."
- "You have the right to ask for a credit score."
- "You have the right to dispute incomplete or inaccurate information."
- "Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information."
- "Consumer reporting agencies may not report outdated negative information."
- "Access to your file is limited."
- "You must give your consent for reports to be provided to employers."
- "You may limit "prescreened" offers of credit and insurance you get based on information in your credit report."
- "You may seek damages from violators."
- "Identity theft victims and active duty military personnel have additional rights."

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

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

**Federal Trade Commission**, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**For residents of Iowa:** You may also obtain information about preventing and avoiding identity theft from the Iowa Office of the Attorney General:

Iowa Office of the Attorney General, Consumer Protection Division  
1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-515-281-5926,  
<https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/>

**For residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division  
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us)

**For residents of Massachusetts:** You also have the right to obtain a police report.

**For residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division  
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov)

**For residents of Oregon:** You may also obtain information about preventing and avoiding identity theft from the Oregon Department of Justice:

Oregon Department of Justice, Consumer Protection  
1162 Court Street NE, Salem, OR 97301-4096  
1-877-877-9392, <https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/>

**For residents of Rhode Island:** You also have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General, Consumer Protection Unit  
150 South Main Street, Providence, RI 02903, 1-401-274-4400,  
<http://www.riag.ri.gov/ConsumerProtection/About.php>

**For residents of West Virginia:** You also 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 may also obtain information about preventing and avoiding identity theft from the West Virginia Attorney General's Office:

West Virginia Attorney General's Office, Consumer Protection Division  
P.O. Box 1789, Charleston, WV 25326, Toll-Free: 1-800-368-8808, Phone: 304-558-8986  
<http://www.ago.wv.gov/consumerprotection/pages/identity-theft-prevention.aspx>

