Cognizant

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
doj-cpb@doj.nh.gov

June 17, 2020

To Whom It May Concern:

I write on behalf of Cognizant Technology Solutions Corporation ("Cognizant"), to inform you about a recent incident in which Cognizant was the victim of a ransomware attack through which personal information relating to New Hampshire residents was accessed by an unauthorized third party.

On April 20, 2020, Cognizant learned that the attackers staged and likely exfiltrated a limited amount of data from Cognizant's systems, primarily relating to internal tax and finance documents. Based on our investigation, we understand that this exfiltration occurred between April 9 and 11.

Through our investigation, we have determined that the impacted data included instances of the following categories of personal information mostly relating to current and former employees, and also a limited number of contractors and employees of or other individuals related to previously or potential acquired companies: name and Social Security number and/or financial account information. While we have not seen any public disclosure of the data and have no reason to believe it has been misused, we will begin providing notice to approximately 10 individuals residing in New Hampshire about this incident.

As part of our investigation, we also found documentation used to manage our internal corporate credit card program that contained instances of employee corporate cardholder name and card number, and expiration date in some instances. We provided notice to the issuer of the cards about these accounts and we have been informed that they have not seen an increase in fraudulent activity on these accounts. While we do not believe that this will create a risk of harm to our employees relating to this information, out of an abundance of caution we are notifying all of our employees who have active corporate credit card accounts. We will begin providing notice to approximately 125 employees with active corporate credit card accounts residing in New Hampshire.

We are providing these individuals with an offer for complimentary credit monitoring, dark web monitoring, and identity theft insurance and recovery services provided by ID Experts. An individual can enroll in these services online at https://ide.myidcare.com/cognizant or by calling +1-833-579-1114.

Please find attached samples of the letters we will be sending to these individuals. In the event we notify a material additional number of individuals residing in New Hampshire, we will update your office.

Cognizant is taking this security incident very seriously. We have been cooperating with the FBI in connection with their own investigation of the cyber criminals responsible for the attack. In addition to quickly containing the incident, we are also taking steps to further enhance Cognizant's overall security posture. Cognizant maintains a written information security program.

Please do not hesitate to contact me at +1-480-267-6552 or Ellen.Geller@Cognizant.com if you have any questions.

Sincerely,

Ellen Geller
Data Privacy Lead Americas

Cognizant

C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

<<FirstName>> <<LastName>>
<<Address1>><<Address2>>
<<City>>, <<State>> <<Zip Code>>

June 17, 2020

Notice of Data Breach

Name,

On behalf of Cognizant Technology Solutions, I am writing to inform you about a recent incident that may have involved your Cognizant corporate credit card. We regret that this incident occurred and take the security of your personal information seriously.

WHAT HAPPENED. We recently discovered that Cognizant was the victim of a ransomware attack carried out by international cyber criminals. On April 20, 2020, Cognizant learned that the attackers staged and likely exfiltrated a limited amount of data from Cognizant's systems. Based on our investigation, we understand that this activity occurred between April 9 and 11.

WHAT INFORMATION WAS INVOLVED. The majority of the personal information that was impacted was information relating to our corporate credit cards. Out of an abundance of caution, we are giving notice to all associates who have an active corporate credit card. All associates who have an active corporate credit card will be offered credit and identity theft monitoring services from ID Experts, as detailed below.

WHAT WE ARE DOING. We notified the issuer of the cards of impacted accounts. They continue to monitor the account for any fraudulent activity and we have been informed that they have not seen an increase in fraud for our accounts. Cognizant is taking this security incident very seriously. We have been cooperating with the Federal Bureau of Investigation in connection with their investigation of the cyber criminals responsible for the attack. In addition to quickly containing the incident, we are also taking various steps to further improve Cognizant's overall security posture.

WHAT YOU CAN DO. While we have no reason to believe that any fraudulent activity has been carried out on the accounts, to assist you and consistent with law, we are providing you with the following information about general steps you can take to protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary 12-month credit and dark web monitoring service provided by ID Experts, which also includes identity theft insurance coverage and managed identity restoration services. You have until September 18, 2020 to activate this complimentary service by using the following activation code: [Enrollment Code]. This code is unique for your use and should not be shared. To enroll, go to https://ide.myidcare.com/cognizant or call 833- 579-1114.

FOR MORE INFORMATION. Please know that we are truly sorry for inconvenience or concern this incident may cause you. Please do not hesitate to contact us at 833-579-1114 if you have any questions or concerns. We have also prepared a list of frequently asked questions which you may find helpful and which can be accessed online at https://ide.myidcare.com/cognizant.

Sincerely,

Becky Schmitt

Becky Schmitt
Chief People Officer

ADDITIONAL INFORMATION

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your Attorney General, 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 website, at www.consumer.gov/idtheft, or 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 credit reports from each nationwide credit reporting agency. 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, under the federal Fair Credit Reporting Act ("FCRA"), 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 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) 685-1111	(888) 397-3742	(888) 909-8872
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
Equifax.com/personal/ credit-report-services	Experian.com/help	Chester, PA 19022 TransUnion.com/credit-help

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

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 at the following numbers to place a security freeze to restrict access to your credit report:

(1) Equifax – (800) 685-1111
(2) Experian – (888) 397-3742
(3) TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

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: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

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

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

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

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

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

IF YOU ARE A RHODE ISLAND RESIDENT: We are notifying approximately 34 individuals residing in Rhode Island in connection with this incident. You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov/