CITRIX®

New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

April 29, 2019

To Whom It May Concern:

On behalf of Citrix Systems, Inc., I am writing to inform you about a recent incident in which Citrix was the victim of a cyberattack through which personal information relating to New Hampshire residents may have been impacted.

On March 6, 2019, the FBI informed Citrix that the FBI had reason to believe that international cyber criminals gained access to Citrix's internal network. Following receipt of this information, we launched an investigation, which remains ongoing. We currently believe that the cyber criminals had intermittent access to our network between October 13, 2018 and March 8, 2019. We also believe that they removed files from our internal systems during that time period. On April 8, 2019, we determined that the removed files contained information about our current and former employees, and, in limited cases, information about beneficiaries and/or dependents. This information may have included, for example, names, Social Security numbers, and financial information. Out of an abundance of caution, we are providing notice to current and former employees of Citrix.

We have engaged leading cyber security firms to assist our internal team with our forensic investigation. We are also cooperating with the FBI in connection with their investigation of the incident. We have taken measures that we believe are designed to remove the cyber criminals' access to our systems, including a system wide password reset, tightened the rules related to password complexity and enhanced multifactor authentication on our systems. Additionally, we continue to actively monitor for signs of further activity or compromise.

We will begin notifying the approximately 90 current or former employees who are New Hampshire residents of this incident on April 29, 2019. We will provide these individuals with an offer for complimentary credit monitoring services. An individual can enroll by following the instructions in the letter we are providing them. Attached is a sample of the letter that we are providing to these New Hampshire residents.

Please do not hesitate to contact me at +1 (781) 203-4522 if you have any questions. I can also be reached at 15 Network Drive, Burlington, MA 01803, and by email at peter.lefkowitz@citrix.com.

Sincerely,

Peter Lefkowitz
Chief Privacy and Digital Risk Officer

Attachment

CITRIX®

Return Mail Processing Center
PO Box 9349
Dublin, Ohio 43017

<<Name1>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

April 29, 2019

Notice of Data Breach

I am writing to inform you that personal information about you may have been involved in the recent cyberattack on Citrix. This notice contains information about the incident that occurred, as well as services Citrix is providing and additional steps you can take to protect yourself against any potential misuse of your personal information. We deeply regret that this incident occurred and take the security of employee information seriously.

WHAT HAPPENED. On March 6, 2019, the FBI informed Citrix that the FBI had reason to believe that international cyber criminals gained access to Citrix's internal network. Following receipt of this information, we immediately launched an investigation, which remains ongoing. We currently believe that the cyber criminals had intermittent access to our network between October 13, 2018 and March 8, 2019 and that they removed files from our systems, which may have included files containing information about our current and former employees and, in limited cases, information about beneficiaries and/or dependents. Out of an abundance of caution, we are providing this letter to current and former employees of Citrix to alert them of this incident. We will notify you if your beneficiaries or dependents were impacted.

WHAT INFORMATION WAS INVOLVED. We believe that the cyber criminals may have accessed and or removed information relating to certain individuals who are current and former employees, as well as certain beneficiaries and dependents. This information may have included, for example, names, Social Security numbers, and financial information.

WHAT WE ARE DOING. We have engaged leading cyber security firms to assist our internal team with its forensic investigation, and we are cooperating with the FBI in connection with their investigation of the cyber criminals. We have taken measures that we believe are designed to remove the cyber criminals' access to our systems, and we are monitoring for signs of further activity or compromise. We are also providing resources, explained in this letter, to help protect against potential misuse of your information.

WHAT YOU CAN DO. We are providing you with the following information about general steps that you can take to protect against potential misuse of your personal information.

Additionally, and as a precaution, we have arranged for you, at your option, to enroll in Equifax ID Patrol, a complimentary one-year credit monitoring, dark web monitoring, and identity restoration service. You have until August 31, 2019 to activate the free, optional service by using the following activation code: [***]. This code is unique for your use and should not be shared. Please go to **http:/myservices.equifax.com/patrol** to enroll.

You should always remain vigilant for incidents of fraud and identity theft by, for example, 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 state's 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. Under the federal Fair Credit Reporting Act (FCRA), you are entitled to one free copy of your credit report every twelve 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 (800) 685-1111 P.O. Box 740241 Atlanta, GA 30374-0241 Equifax.com/personal/ credit-report-services	Experian (888) 397-3742 P.O. Box 9701 Allen, TX 75013 Experian.com/help	TransUnion (888) 909-8872 Fraud Victim Assistance Division P.O. Box 2000 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 also 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.

FOR MORE INFORMATION. Please know that we regret any inconvenience or concern this incident may cause you. We have included an FAQ in this letter that we hope will answer any questions you may have. Please do not hesitate to contact us by calling at (855) 424-0786 if you have any questions or concerns.

Please visit **www.citrix.com/validateletter** if you would like to validate that this is a legitimate communication originating from Citrix.

Sincerely,

Peter Lefkowitz

Peter Lefkowitz
Chief Privacy and Digital Risk Officer

Enclosures: Employee FAQ

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 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 AN OREGON RESIDENT: You may contact local law enforcement, the Oregon Attorney General's Office or the FTC to report suspected identity theft. 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

Oregon Department of Justice
Attorney General Ellen F. Rosenblum
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392
https://doj.state.or.us

IF YOU ARE A RHODE ISLAND RESIDENT: We are giving notice to 11 Citrix employees and former employees who are residents of Rhode Island. 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/

Employee Frequently Asked Questions (FAQs)

1. What happened?

On March 6, 2019, the FBI informed Citrix that the FBI had reason to believe that international cyber criminals gained access to Citrix's internal network. Our forensic security experts confirmed that the cyber criminals removed files from our internal systems that included information about our current and former employees and, in limited cases, beneficiaries and/or dependents.

Our investigation into this incident is still ongoing; but out of an abundance of caution, we are alerting current and former employees of Citrix about this incident and providing them with Equifax monitoring services in countries where they are available.

2. What personal information about me do the cyber criminals have?

Our investigation remains ongoing; however, the personal information that was accessed or removed may have included, for example, names, Social Security numbers, certain financial information, or other personal information relating to your employment.

3. How will I know if I was impacted?

Our investigation has not yet concluded; but out of an abundance of caution, we have sent a notice to the most recent home address on file for current and former employees who were employed by Citrix.

4. Are my spouse, children or other dependents impacted?

Citrix's investigation is ongoing, but we believe that in limited cases information about beneficiaries and/or dependents may have been impacted. We will be contacting employees whose beneficiaries' and/or dependents' information may have been impacted, and we will make Equifax benefits available to these individuals, where possible.

5. What is Citrix doing about this cyber incident?

Following receipt of the information from the FBI, we immediately launched a thorough investigation and engaged leading cyber security firms to assist our internal team. We also have been cooperating with law enforcement in connection with their own investigation into the cyber criminals.

Additionally, in the weeks following the discovery of the incident, Citrix and its outside security experts introduced measures to expel the cyber criminals from its systems. We are monitoring for signs of further activity, but importantly have found no indication that the security of any Citrix product or service was compromised.

We have taken steps to address issues that could have contributed to this situation, and we are investing in resources and technology to improve our internal security going forward.

6. Is the incident contained and resolved?

We currently believe that the cyber criminals had intermittent access to our network between October 13, 2018 and March 8, 2019. There is no evidence that the cyber criminals remain in the system.

Citrix took decisive action intended to prevent cyber criminals from entering the network through a similar mechanism. In the weeks following the discovery of the incident, Citrix and its outside security experts introduced measures to expel the bad actors from its systems.

7. How do I sign up for credit monitoring / identify theft protection?

As a precaution, we have arranged for you to enroll in complimentary credit monitoring, dark web monitoring, and/or identity restoration services in the countries where such services are available. If these services are available in your country, you can use the unique activation code included in this letter to activate the service. You have until 8/31/19 to do so.

To enroll, please follow the instructions included within the letter.

8. What can I do to further protect myself?

You should always remain vigilant for incidents of fraud and identity theft by, for example, regularly reviewing your account statements and regularly monitoring your 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.

If you believe you have been the victim of identity theft or fraud, immediately contact your financial institutions and law enforcement. If you are in the United States, you may also contact the Federal Trade Commission (FTC).

9. What's next?

We are conducting a comprehensive review of our security and evaluating next steps.

10. How can I be sure this letter from Equifax is legitimate?

Please visit **www.citrix.com/validateletter** if you would like to validate that this is a legitimate communication originating from Citrix.

11. Can I receive a copy of this communication in my native language?

Please email **AskHR@citrix.com** to receive a copy of this letter and FAQ in French, German, Japanese, Chinese (simplified), or Spanish.