[redacted]

From: Dunn, Amy Grewal <amy.dunn@faegredrinker.com>
Sent: Friday, July 17, 2020 12:19 PM
To: DOJ: Consumer Protection Bureau
Cc: Weiss, Jason G.
Subject: Notice of Data Incident
Attachments: EXPERIAN_F6415_L01_Collabera All States.doc.pdf

Good morning,

I am writing on behalf of Collabera, Inc. ("Collabera") to inform you of a data incident that may have involved our employees' personal information. On June 8, 2020, Collabera identified malware in its network system consistent with a ransomware attack. We promptly restored access to our data from backup files without having to obtain a decryption key, and the malware has been removed from the system. We immediately launched an investigation to determine the nature and scope of this event. On June 10, we became aware that the unauthorized party obtained some data from our system. We are working with outside forensic experts and law enforcement to conduct a more detailed review of the incident. Based on our investigation to date, it appears the unauthorized party was first in Collabera's environment on May 24, 2020.

We believe the incident likely involved some employee personal information. The information potentially involved varied, but may have included first and last names, mailing addresses, telephone numbers, Social Security Numbers, dates of birth, employee benefits and employee verification information, passport/visa information, and e-mail addresses.

Though we have no reason to believe that our employees' personal information has been misused for the purpose of committing fraud or identity theft, we are providing individual notifications and taking protective measures out of an abundance of caution. Collabera cares about protecting the identity of its employees, and is therefore offering credit monitoring and identity theft protection for two years. Individual notifications detailing the incident and the enrollment process were mailed to New Hampshire residents on July 10, 2020. A template copy of the notice is attached. Based on our investigation, it appears that 129 residents from New Hampshire may have been impacted.

Remedial steps Collabera has taken in response to this incident include enhanced data security measures (data minimization, destruction and/or encryption), implementing new technical safeguards (additional firewalls, additional endpoint detection & response agents, additional multifactor authentication, additional logging and monitoring), changed passwords, and revised procedures.

Please contact me if you have any further questions about this incident.

Regards,

Amy Grewal Dunn
Associate
amy.dunn@faegredrinker.com
Connect: vCard

+1 317 237 1057 direct

Faegre Drinker Biddle & Reath LLP
300 N. Meridian Street, Suite 2500
Indianapolis, Indiana 46204, USA

Collabera
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 10, 2020

F6415-L01-0000001 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE - L01
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

RE: Notice of Data Breach

Dear Sample A Sample:

I am writing on behalf of Collabera, Inc. ("Collabera") to inform you of an incident that may have involved your personal information. Though we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft, we are reporting to you and taking protective measures out of an abundance of caution.

This letter provides you with information on the steps Collabera has taken to further guard against the unauthorized disclosure and misuse of your personal data and the resources we are making available to you, as well as guidance on additional steps you may wish to take.

What Happened? On June 8, 2020, Collabera identified malware in its network system consistent with a ransomware attack. We promptly restored access to our data from backup files, and immediately launched an investigation to determine the nature and scope of this event. On June 10, we became aware that the unauthorized party obtained some data from our system. We are working with outside experts and law enforcement to conduct a more detailed review of the incident.

What Information Was Involved? Based on our investigation to date, we believe the incident likely involved some employee personal information. The information potentially involved varied, but may have included first and last names, mailing addresses, telephone numbers, Social Security Numbers, dates of birth, employee benefits and employee verification information, passport/visa information, and e-mail addresses.

What We Are Doing: We take the security of your personal information very seriously, and we are enhancing our security measures. We have retained a network security and forensic firm to investigate the incident and help us develop additional security measures. Moreover, we are implementing enhanced training procedures to mitigate the risk of further incidents and unauthorized access to personal information.

In addition, we are offering you complimentary credit monitoring for two years through Experian, one of the world's leading experts in identity protection, as described below.

What You Can Do: Please review the enclosed attachment called *Preventing Identify Theft and Fraud* for more information on ways to protect against the potential misuse of your information and remain vigilant in monitoring your financial accounts.

Because we care about protecting your identity and your financial health, we are offering a complimentary two-year membership in Experian's® IdentityWorks℠.

This product provides you with superior detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: 10/31/2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your activation code: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (866) 274-5767 by 10/31/2020. Be prepared to provide engagement number DB21123 as proof of eligibility for the identity restoration services by Experian.

Fraud and Identity Restoration

In addition to the foregoing, we have arranged for free Identity Restoration support in the event of fraudulent use of your information. It is available to you for two years from the date of this letter regardless of whether or not you participate in IdentityWorks, and does not require any action on your part at this time.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (866) 274-5767. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and attempt to resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

The Terms and Conditions for this service are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

We strongly encourage you to carefully review your bank, credit card, and other financial statements regularly. If you see any transactions you don't recognize or which appear suspicious, notify your financial institution immediately, as well as Experian.

We sincerely regret any inconvenience this incident may cause you. If you have additional questions, please call the customer assistance line at (866) 274-5767 Monday through Friday from 8 a.m. to 10 p.m. CST, and Saturday and Sunday from 10 a.m. to 7 p.m. CST.

Sincerely,

Mike Chirico
Senior Director, Human Resources
Collabera, Inc.

Preventing Identity Theft and Fraud

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting http://www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact these national credit reporting agencies to request a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files. Contact information for these agencies is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies using the contact information above.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Other Important State Information

You may also file a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report filed in this matter.

For California Residents:
You can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Iowa Residents:
You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland Residents:
You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.marylandattorneygeneral.gov.

For New Mexico Residents:
The Fair Credit Reporting Act provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, and seek damages from violators. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For North Carolina Residents:
You may obtain information about avoiding identity theft at: North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 919-716-6400 www.ncdoj.gov.

For Rhode Island residents:
You may obtain information about preventing and avoiding identity theft from Rhode Island's Attorney General Office: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, Phone: (401) 274-4400 http://www.riag.ri.gov.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico and Vermont Residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional reports.