



BROWN-FORMAN

August 25, 2020

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

To Whom It May Concern:

On behalf of Brown-Forman Corporation (“Brown-Forman”), I am writing to inform you about a recent cyberattack in which Brown-Forman was the victim. The attack impacted personal information relating to New Hampshire residents.

On July 28, 2020, we discovered suspicious activity in our environment, which we promptly began to investigate and contain. On August 4, 2020, we learned that the unauthorized actors carrying out this activity stole certain data from our internal network. We took immediate steps to contain the malicious activity and to safeguard our systems. On August 11, 2020, the attackers began releasing the stolen data publicly.

Through our investigation, to date it appears that the impacted records included certain payroll, benefits, and other information relating to some of our current and former employees, and, in more limited cases, their dependents and beneficiaries. This included information such as names and Social Security Numbers. Out of an abundance of caution, we will begin notifying all current and former employees who worked for Brown-Forman as of January 1, 2013 about this incident, including two (2) residents of New Hampshire. We will provide these individuals with a complimentary offer for Experian IdentityWorksSM identity protection services, which includes credit monitoring from all three nationwide bureaus, access to Experian credit reports, identity theft insurance and identity restoration services. Individuals can enroll by visiting <https://www.experianidworks.com/3bcredit> or calling toll-free to (833) 704-9391. In the event we notify a material additional number of individuals residing in New Hampshire, we will update your office.

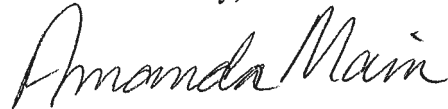
In response to this incident, we have implemented additional IT security measures to protect our data and to prevent further attacks on our systems. These measures included temporarily disabling certain systems, limiting system access, and deploying additional security software on computers. Additionally, we continue to monitor actively for signs of further activity or compromise. We are also partnering with third-party data security experts to respond to the incident. We also informed

the FBI, and are cooperating with them. Brown-Forman maintains a written information security program.

Attached is a sample of the letter we are providing to New Hampshire residents.

Please do not hesitate to contact me at (502) 774-7814 or Amanda_Main@b-f.com if you have any questions.

Sincerely,

A handwritten signature in black ink that reads "Amanda Main". The signature is written in a cursive, flowing style.

Amanda Main
Senior Attorney and Privacy Officer



BROWN-FORMAN

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

August 25, 2020

F7332-L01-0000001 P001 T00001 *****MIXED AADC 159



SAMPLE A SAMPLE - US INDIVIDUAL
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



Notice of Data Breach

On behalf of Brown-Forman, we are writing to inform you about a recent cyber attack that involved personal information housed on the Brown-Forman network. We want to be sure you are aware of the actions the company is taking, what actions you can take to keep your data as secure as possible, and recommendations on how to monitor your personal information. We sincerely regret any inconvenience this incident may cause you and know that it comes at an already difficult time.

WHAT HAPPENED. On July 28, 2020, we discovered suspicious activity in our internal network and promptly began to investigate and contain it. On August 4, 2020 we learned the cyber criminals stole certain records containing information about some of our current and former employees. In some cases, these records contained limited information about employee dependents or beneficiaries. Out of an abundance of caution, we are providing this letter to all current employees of Brown-Forman as well as former employees who worked at Brown-Forman as of 2013 to alert them of this incident. We will notify you separately if your beneficiaries or dependents were impacted.

WHAT INFORMATION WAS INVOLVED. We believe the incident involved information regarding current and former employees, as well as certain beneficiaries and dependents of those employees. This includes information such as: names, Social Security Numbers, work contact information (such as Brown-Forman email address), home address, position, business title, and salary-related information (such as base pay, hire date, and weekly hours worked).

WHAT WE ARE DOING. We began investigating the incident as soon as we became aware of suspicious activity on our network. We took several steps to limit access to our network to prevent further data from being compromised or stolen, engaged outside forensic experts to help us better understand the impact of this incident, and are cooperating with law enforcement.

0000001



F7332-L01

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 personal information.

As a precaution, we have arranged the option for you to enroll in a complimentary one-year credit monitoring service. We have engaged Experian to provide you with its IdentityWorksSM identity protection services, which includes credit monitoring from all three bureaus, access to your Experian credit report, \$1 million in identity theft insurance and identity restoration services. If you would like to proceed with this option, you have until November 30, 2020 to activate the free credit monitoring service by using this activation code: **ABCDEFGHI**. This code is unique to you and should not be shared. To enroll, please visit <https://www.experianidworks.com/3bcredit>, call toll-free to 833-704-9391, or toll call to 479-343-6227 using any applicable international dialing codes (if you happen to be outside of the U.S.). For telephone calls, the hours of operation are Monday-Friday 6am-6pm PST and Saturday-Sunday 8am-5pm PST.

Please 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.

Additionally, you may contact the Federal Trade Commission (“FTC”) or local 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, call the FTC at (877) IDTHEFT (438-4338), or write to FTC at 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 (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.

Lastly, you can obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. For example, 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.

FOR MORE INFORMATION. We regret any inconvenience this incident may cause you. If you have any questions or concerns, we hope that you will call toll-free to 833-704-9391, or toll call to 479-343-6227 using any applicable international dialing codes (if you happen to be outside of the U.S.).

Sincerely,

Tim Nall
SVP, Chief Information & Advanced Analytics Officer

Kirsten Hawley
SVP, Chief Human Resources & Corporate Communications Officer

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>

