McDonald Hopkins
A business advisory and advocacy law firm®

RECEIVED
DEC 18 2020
CONSUMER PROTECTION

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Christine N. Czuprynski
Direct Dial: 248-220-1360
E-mail: cczuprynski@mcdonaldhopkins.com

December 11, 2020

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Direct Federal Credit Union – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Direct Federal Credit Union ("Direct Federal"). I am writing to provide notification of an incident at Direct Federal that may affect the security of personal information of 1,014 New Hampshire residents. Direct Federal's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Direct Federal does not waive any rights or defenses regarding the applicability of New Hampshire or personal jurisdiction.

On October 12, 2020, the Direct Federal cyber-security systems identified an unauthorized user accessing one server. Direct Federal's IT team was aware of the situation less than an hour after it began. The team was able to quickly take steps to ensure that no others could access the system. The unauthorized access was terminated, and any future threats of this unauthorized access were eliminated. While Direct Federal was able to quickly identify, address, and resolve the issue, a limited amount of member information may have been visible to the unauthorized party.

To understand what information may have been accessed during this situation, Direct Federal began a prompt and thorough investigation. After an extensive, multi-week forensic investigation and manual document review by external cyber-security experts, the investigation concluded that the files accessed without authorization contained member information. Specifically, on November 11, 2020 Direct Federal discovered that some of the accessed files contained the New Hampshire residents' names, addresses, and Direct Federal member numbers. Social Security numbers and dates of birth were not included in the files.

Direct Federal has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, Direct Federal wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Direct Federal is providing the affected residents with written notification of this incident commencing on or about December 10, 2020 in substantially the same form as the letter attached hereto. Direct Federal is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Direct Federal is advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Direct Federal, protecting the privacy of personal information is a top priority. Direct Federal is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Direct Federal continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions concerning this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Christine N. Czuprynski

Encl.

DIRECTFEDERAL
BANKING AT THE RATE OF LIFE

[redacted]

[redacted]

Dear [redacted],

Our members rely on Direct Federal to maintain the privacy and security of their personal information. This is a responsibility we take seriously — investing financial, staff, and other resources in creating and maintaining strong information technology. This letter will address a recent data security incident at Direct Federal.

What Happened?

On October 12, 2020, our cyber-security systems identified an unauthorized user accessing one of our servers. Direct Federal's IT team was aware of the situation less than an hour after it began. The team was able to quickly take steps to ensure that no others could access the system. The unauthorized access was terminated, and any future threats of this unauthorized access were eliminated. Once the immediate concern was addressed, our IT team worked collaboratively with external cyber-security experts to further secure our systems. Based on that work, we are confident that ongoing operations remain safe and secure. While Direct Federal was able to quickly identify, address, and resolve the issue, we do believe a limited amount of member information may have been visible to the unauthorized party.

What Information May Have Been Accessed?

To understand what information may have been accessed during this situation, Direct Federal began a prompt and thorough investigation. After an extensive, multi-week forensic investigation and manual document review by external cyber-security experts, the investigation concluded that the files accessed without authorization contained member information. Specifically, on November 11, 2020 we discovered that some of the accessed files contained your name, address, and Direct Federal member number. Social Security numbers and dates of birth were not included in the files.

What Can You Do?

At this time, we have no evidence that any of your information has been stolen or misused. However, we believe it is important that you be aware of this issue in case you want to take additional precautionary measures such as:

- Promptly reviewing your financial account statements for fraudulent or irregular activity
- Placing a fraud alert and/or security freeze on your credit files; you can do this for free with any of the major credit monitoring services (Experian, TransUnion, and Equifax)
- Obtaining a free credit report (available from any of the providers noted above)

See attached for more information on each of these steps.

What Steps Has Direct Federal Taken?

Direct Federal took a number of steps to ensure that no fundamental changes were made to our network. We also updated our manual security protocols and enhanced our technology driven security systems and services. We recognize that good data security requires ongoing vigilance and will continue to invest in the types of systems that allowed us to quickly identify and contain this issue. Direct Federal pledges to continue our longstanding and extensive effort to safeguard information.

Please note that no employee from Direct Federal Credit Union will ever call you and ask for your Social Security number. We remain fully committed to both maintaining the privacy of your personal financial information and to sharing information with you in a timely, transparent manner.

For More Information

If you have any further questions regarding this incident, please call our response line at [redacted]. The response line is available Monday through Friday, [redacted].

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

Placing a Fraud Alert on Your Credit File

You may place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

Placing a Security Freeze on Your Credit File

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.freeze.equifax.com	experian.com/freeze	www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Obtaining a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. 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.

Additional Helpful Resources

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.