NORTON ROSE FULBRIGHT

July 6, 2021

Sent By Registered Mail

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Norton Rose Fulbright Canada LLP
1 Place Ville Marie, Suite 2500
Montréal, Quebec H3B 1R1 Canada

F: +1 514.286.5474
nortonrosefulbright.com

RECEIVED
JUL 12 2021
CONSUMER PROTECTION

Julie Himo
+1 514.971.2497
julie.himo@nortonrosefulbright.com

Dear Sir/Madam:

Re: Legal Notice of Cybersecurity Incident

We write on behalf of our client, Financière des Professionnels ("**Fdp**"), to notify you of two security incidents which resulted in the unauthorized access and exfiltration of the personal information of three (3) New Hampshire residents.

Fdp was the victim of two cyber security incidents. There is no indication that the incidents are related to one another.

The first incident was discovered on February 11, 2021 ("**February Breach**"). Fdp had a business email compromise where an unauthorized third party sent emails from Fdp's corporate email address to some of its customers. The customers were immediately informed about the incident.

Upon discovering this incident, Fdp engaged cyber forensic experts to conduct a comprehensive investigation. The investigation concluded that eight (8) Microsoft Office 365 accounts were compromised, and phishing emails were sent from a Fdp corporate email address to some clients. These clients were immediately notified of the incident. There was no indication that the Fdp servers had been accessed. The investigation as to whether data had been exfiltrated was still ongoing when the second incident occurred.

The second incident was discovered on April 6, 2021 ("**April Breach**"). Fdp was the victim of a ransomware-type intrusion directed towards some of its servers. An unauthorized third party gained access to Fdp's IT system. Fdp immediately undertook additional investigation and discovered on April 13, 2021 that certain personal information may have been exfiltrated. Despite the forensic investigation, Fdp has not been able to determine the cause of the incident.

From the investigation, Fdp has determined that the February Breach occurred from January 19, 2021 to February 12, 2021 and the April Breach occurred from April 2, 2021 to April 7, 2021.

The following personal information of clients has been compromised: name, email address, Social Insurance Number, drivers' license, and information about their Fdp account (including the customer account number).

Fdp is taking a number of additional measures to strengthen its systems such as: implementing multi-factor authentication, implementing an audit logs retention policy; enhancing remote monitoring, and consolidating event logs to increase correlation of anomalous events.

NORTON ROSE FULBRIGHT

In addition, to help protect the identity of impacted individuals, Fdp offered a complimentary credit monitoring and identity theft protection services for five years through Equifax. This product provides superior identity detection and resolution of identity theft.

All potentially affected individuals will be notified of the incident on July 8, 2021. A copy of the notification letter is enclosed.

If you have any questions or need further information regarding this incident, please contact me at (514) 971 2497 or julie.himo@nortonrosefulbright.com.

Yours truly,

Julie Himo

Enclosure

<Date>

<Suffix> <First Name> <Last Name>
<Address 1>
<City>
<Country>
<Postal Code>

Hello <Suffix> <Last Name>,

You are surely aware of the increase in cyber attacks targeting the systems of organizations of all sizes, especially in recent months, and even weeks.

We are communicating with you today to inform you that fdp has identified two recent intrusions against its systems.

What happened?

We were first informed on February 11th, 2021 of a phishing email campaign in which an unauthorized third party had sent emails from a fdp corporate email address to some of our customers. We immediately informed the impacted customers of the situation.

While an initial investigation indicated that the incident appeared to be limited in scope, we nonetheless retained leading cyber security experts, KPMG-EGYDE, to conduct a thorough investigation to determine the source of the incident and the extent to which personal information may have been accessed. This investigation has recently been completed.

In the meantime, a few weeks after the intrusion in our email system, a second attack was perpetrated against fdp. On April 6th, 2021 a ransomware-type intrusion was directed towards some of our servers. It should be noted that this second incident is independent from the first one.

Fortunately, the monitoring systems we have in place allowed us to identify early signs of suspicious activity and our teams immediately blocked access to our servers, limiting the scope of the intrusion.

In response to this incident, we once again mobilized cybersecurity experts to conduct a comprehensive investigation to confirm the extent of personal information potentially affected. This investigation required considerable work by the experts.

The investigations into these two incidents now allow us to provide you with more information on the potential impact of the incidents. We can confirm that in both incidents, some of your personal information may have been exfiltrated.

What types of information were impacted?

Based on our investigations, personal information that may have been exfiltrated and accessed by unauthorized third parties includes:

- **Personal information such as**: your name, social insurance number, address, email address, date of birth, passport number, etc.
- **Banking information**: identification of your banking institution (branch number, transit), checking account number, credit card number, etc.
- **Information from your fdp account**: customer account number, etc.

Based on the results of our investigation, **we have no evidence that your personal information has been misused** as a result of these incidents.

Protecting your data is our priority!

We are aware that this situation may cause some concern and we are sincerely sorry for this. Please be assured that we take this situation very seriously.

The protection of the personal information entrusted to us is a top priority and that is why we ensure the continuous modernization of our security infrastructure and processes and constantly monitor our systems.

Privileged access to Equifax credit monitoring and identity theft protection service

In addition to our internal measures to help protect your personal information, we offer you a **free five-year subscription** for Equifax's credit monitoring services. Equifax identity theft protection and credit monitoring services allow you to:

- Receive alerts on key changes to your Equifax credit reports based on your personal alert preferences.
- Access your Equifax credit scores for your educational use.
- Be alerted if your personal information is found on websites suspected of being fraudulent.
- Work with an identity restoration specialist if, for any reason, you become a victim of identity theft.
- Claim certain expenses in the event that you become a victim of identity theft.

To activate your Equifax subscription, we invite you to visit [Equifax US URL] and enter the following activation code: <CODE>. Please note that this code is valid until [Expiration Date].

If you have any questions, please feel free to contact fdp at info@fprofessionnels.com.

Again, we sincerely regret any concerns these incidents may cause.

Sincerely,

André Sirard, M. Sc., CFA, ASC, Adm. A.
President and CEO