Debevoise & Plimpton

Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
+1 212 909 6000

By First-Class Mail

September 18, 2020

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

Data Breach Notification

To Whom It May Concern:

On behalf of Payoneer Inc. ("Payoneer"), and consistent with N.H. Rev. stat. § 359-C:20, this letter provides notice of a computer data security incident potentially affecting approximately 3 New Hampshire residents. Payoneer is a financial services company that provides online money transfer and digital payment services.

On or about August 3, 2020, Payoneer learned that an unauthorized third party had gained remote access to an employee's business email mailbox with the apparent aim of sending phishing emails to individuals whose email addresses the mailbox contained (described further below).

We discovered the incident after receiving reports from the employee that these unauthorized email messages had been sent from their account. We then quickly took steps to terminate the unauthorized access and began a thorough investigation.

Based on the findings of our investigation to date, we believe that the incident was likely the result of a credential stuffing attack that first resulted in unauthorized access to the employee's email mailbox on or about July 26, 2020. There are also indications that on July 27, 2020, the unauthorized third party potentially obtained a copy of a portion of the employee's mailbox through an automated synchronization that can occur over some types of connections.

Furthermore, on August 3, 2020, the unauthorized third party sent, using an automated tool, what Payoneer believes to be identical phishing emails to 1,071 non-Payoneer email addresses contained in the compromised employee's mailbox. Of those, 875 were sent successfully.

As part of the investigation, Payoneer engaged a third party to conduct a detailed analysis of the contents of the affected email mailbox. That analysis identified that, depending on the individual in question, the unauthorized third party may have acquired a copy of one or more of the following categories of personal information with respect to such individual: names, addresses, social security numbers, financial account or credit card numbers,

passport numbers, usernames and passwords permitting access to an online account, or medical information.

Payoneer anticipates it will begin sending these individuals notice on September 18, 2020. A sample of the notification letter is attached. As stated in the letter, Payoneer is offering to provide individuals 24 months of free identity theft and credit monitoring services through Equifax.

As an immediate response to the incident and to prevent recurrence of this type of incident in the future, Payoneer forced a password reset for the affected employee, warned all recipients of the phishing email of its malicious nature, and is reviewing the security measures applied to the authentication protocols used to access employee mailboxes to identify appropriate improvements.

Payoneer takes this incident and the protection of data seriously, and is committed to answering any questions that your office may have. Please do not hesitate to contact me at the address above, at 1-212-909-6577, or agesser@debevoise.com.

Respectfully yours,

Avi Gesser

Avi Gesser

Partner

Attachment: Sample Notification Letter

Payoneer GO BEYOND 150 West 30th Street, Suite 600,
New York, NY 10001

September 18, 2020

00549-FININS-AUTO 000001

[INSERT NAME]
[INSERT ADDRESS]

NOTICE OF DATA BREACH

Dear [INSERT NAME]:

We are writing to inform you of an incident involving some of your personal information held by Payoneer Inc. ("Payoneer").

WHAT HAPPENED?

On or about August 3, 2020 we learned that an unauthorized third party was able to gain remote access to one of our employees' business email mailbox with the apparent aim of sending phishing emails to individuals whose email addresses the mailbox contained.

After we became aware of the incident, we quickly took steps to terminate the unauthorized access and began a thorough investigation. Based on our investigation to date, the unauthorized access began on or before July 26, 2020, and was terminated on or about August 3, 2020, the day we discovered it.

On August 5, 2020, we identified that the unauthorized access might have allowed the third party to acquire a copy of files including certain individuals' personal information, although this could not be confirmed definitively. As part of our investigation, we have analyzed the contents of the affected email mailbox and determined that it contained your personal information and that the unauthorized third party might have accessed or acquired a copy of it.

WHAT INFORMATION WAS INVOLVED?

The incident may have involved your [INSERT EXTRA 1].

00549-FININS-AUTO-G0001--000001-000001-000-1/3

September 18, 2020
Activation Code: [INSERT CODE]
Expiration Date: December 31, 2020

WHAT WE ARE DOING

We have reset the password for the impacted account, conducted a thorough investigation of activity taken by the unauthorized third party against the mailbox and are notifying appropriate regulatory authorities.

We have also arranged for you to receive a complimentary two-year membership of Equifax Credit Watch Gold with Web Detect (U.S.), which helps detect misuse of your personal information and provides you with identity protection focused on identification and resolution of identity theft.

Equifax® Credit Watch™ Gold with 3-in-1 Credit Monitoring provides you with the following key features:

- 3- Bureau credit file monitoring[1] and alerts of key changes to your Equifax®, Transunion®, and Experian® credit reports
- One Equifax 3-Bureau credit report
- Automatic Fraud Alerts[2] With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Wireless alerts (available online only) Data charges may apply.
- Access to your Equifax® credit report
- Up to $1 MM Identity Theft Insurance[3]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

To sign up online for online delivery go to www.myservices.equifax.com/tri

1. Welcome Page: Enter the Activation Code provided above in the "Activation Code" box and click the "Submit" button.

2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, review the Terms of Use and then check the box to accept and click the "Continue" button.

4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

To sign up for US Mail delivery, dial 1-855-833-9162 for access to the Equifax Credit Watch Gold with 3-in-1 Credit Monitoring automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Activation Code: You will be asked to enter your Activation Code provided above.

2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.

September 18, 2020
Activation Code: [INSERT CODE]
Expiration Date: December 31, 2020

3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.

4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

You need to activate your membership in order to receive your benefits, and must do so no later than **December 31, 2020**. **Your Activation Code will not work after this date**.

If you have questions about our provision of this complementary credit monitoring service to you, please contact us at DPO@payoneer.com.

WHAT YOU CAN DO

We strongly encourage you to take advantage of the credit monitoring and identify theft protection services we are offering. We have also enclosed additional steps that you can take to protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

Payoneer sincerely regrets any inconvenience this unfortunate incident has caused. If you have any questions, you can contact us at DPO@payoneer.com.

Payoneer, Inc.

September 18, 2020
Activation Code: [INSERT CODE]
Expiration Date: December 31, 2020

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements 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 also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian**:	**TransUnion**:
equifax.com equifax.com/personal/credit-report-services P.O. Box 740241 Atlanta, GA 30374 866-349-5191	experian.com experian.com/help P.O. Box 2002 Allen, TX 75013 888-397-3742	transunion.com transunion.com/credit-help P.O. Box 1000 Chester, PA 19016 888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. 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 accounts in your

name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For New York residents: You may contact the Office of the New York Office of the Attorney General, The Capitol, Albany NY 12224-0341, https://www.ag.ny.gov/, 1-800-771-7755.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226.

For Georgia and New Jersey 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 report(s).

00549-FININS-AUTO-G0001--000001-000005-000-3/3

September 18, 2020
Activation Code: [INSERT CODE]
Expiration Date: December 31, 2020

For Tennessee residents:

TENNESSEE CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze must be requested in writing by certified mail or by electronic means as provided by a consumer reporting agency. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. If you are actively seeking a new credit, loan, utility, or telephone account, you should understand that the procedures involved in lifting a security freeze may slow your applications for credit. You should plan ahead and lift a freeze in advance of actually applying for new credit. When you place a security freeze on your credit report, you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a period of time after the freeze is in place. To provide that authorization you must contact the consumer reporting agency and provide all of the following:

(1) The personal identification number or password;

(2) Proper identification to verify your identity; and

(3) The proper information regarding the period of time for which the report shall be available.
A consumer reporting agency must authorize the release of your credit report no later than fifteen (15) minutes after receiving the above information.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account, that requests information in your credit report for the purposes of fraud control, or reviewing or collecting the account. Reviewing the account includes activities related to account maintenance.
You should consider filing a complaint regarding your identity theft situation with the federal trade commission and the attorney general and reporter, either in writing or via their web sites.

You have a right to bring civil action against anyone, including a consumer reporting agency, who improperly obtains access to a file, misuses file data, or fails to correct inaccurate file data.

***