

July 23, 2020

Sent by Certified Mail

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

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

**Julie Himo**  
**Partner**  
Direct line 514 971 2497  
julie.himo@nortonrosefulbright.com

Tel +1 514 847 6017  
nortonrosefulbright.com

RECEIVED

JUL 27 2020

CONSUMER PROTECTION

**Re: *Legal Notice of Information Security Incident***

Dear Sirs or Madams:

We write on behalf of our client, Pivot Technology Services Corp. ("**Pivot**"), to notify you of a security incident which resulted in the unauthorized access and exfiltration of the personal information of 1 New Hampshire resident.

On June 12, 2020, Pivot discovered that it was the victim of a cybersecurity attack by an unauthorized third party by which the malicious actor deployed ransomware in an attempt to encrypt Pivot's technology infrastructure.

Upon detection of the attack, Pivot engaged an industry-leading cyber forensic firm, CrowdStrike, to conduct a comprehensive investigation to determine how the security incident occurred, the scope of such incident and to assist it with remediation efforts. With the assistance of the forensic firm, Pivot immediately implemented countermeasures to minimize the encryption of its systems. As a result, some Pivot employees experienced complications with email, however, there were no interruptions to its business operations.

On July 1, 2020, Pivot discovered that the unauthorized third party had in fact gained access to and exfiltrated the personal information of Pivot's employees residing in the United States, and immediately undertook an additional investigation to determine the scope of the information affected. On July 7, 2020, Pivot determined that the following personal information of employees was compromised in the incident: names, addresses, payroll earnings, deductions, 401k, benefits, bank routing and account numbers, bank account names and social security numbers.

From the investigation, we have determined that the unauthorized third party had access to Pivot's systems between June 9, 2020 and June 12, 2020.

In response to the incident, Pivot expedited the implementation process for Multifactor Authentication (**MFA**) for all applications that are accessed remotely. In addition, Pivot will implement additional safeguards in accordance with the recommendations of the forensic firm, including CrowdStrike Falcon, Mimecast URL filtering process, and Cisco Umbrella, a secure gateway to protect users access.

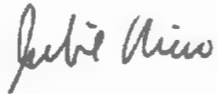
Pivot has also conducted a thorough review of the potentially affected records and continues to review existing policies and procedures designed to try to prevent a similar occurrence from happening again.

In addition, to help protect the identity of impacted individuals, we are offering a complimentary 2 year membership of Equifax ID Patrol. This product provides superior identity detection and resolution of identity theft.

All potentially affected individuals will be notified of the incident on July 24, 2020. A copy of the notification letter is enclosed.

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

Very truly yours,



Julie Himo

Enclosure



[Date]

Dear [Name]

## **Re: Notice of Data Breach**

We are writing to inform you of a security incident at Pivot Technology Solutions, Inc. concerning information held by itself, its subsidiaries and/or affiliates (current and former) including: Pivot Technology Solutions, Ltd., Pivot Technology Services Corp. formally known as New Prosys Corp. and as successor by merger to Sigma Technologies Solutions, Inc. and ACS(US), Inc., TeraMach Technologies, Inc., Pivot Acquisition Corp., ACS (US), Inc., Applied Computer Solutions, Inc., Austin Ribbon & Computer Supplies, Inc., ProSys Information Systems, Inc., Smart-Edge.com, Inc., and Pivot Shared Services, Ltd. (collectively the “Companies”). This incident may have impacted your personal information, and as a result, we also wish to advise you of the steps you can take to help protect your personal information. Your privacy is of the utmost importance to us, and we sincerely regret any concern this incident may cause you.

### **What Happened**

On June 12, 2020, the Companies were the victim of a cybersecurity attack by an unauthorized third party, where the unauthorized party attempted to encrypt parts of the Companies’ technology infrastructure (the “Incident”). On July 1, 2020, the Companies discovered that the unauthorized third party had gained access to and exfiltrated limited personal information of US employees and consultants, and immediately undertook an investigation to determine the scope of the information affected.

### **What Information Was Involved**

On July 7, 2020, the Companies determined that the following personal information of employees and consultants may have been compromised in the Incident: names, addresses, dates of birth, gender, student status, disability status, type of insurance coverage, payroll information (including information with respect to deductions, 401k, income withholdings, and benefits), banking information (including routing and account numbers), social security numbers and dependent information.

### **What We Are Doing**

The Companies have engaged an industry leading cyber forensic firm to conduct a comprehensive investigation to audit the data exposed and assist the Companies in their remediation efforts. Additionally, to help prevent a similar type of incident from occurring in the future, the Companies have implemented additional security protocols designed to protect their network, email environment, systems, and personal information.

### **What You Can Do**

Please review the “Information About Identity Theft Protection Guide” reference, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

Additionally, the Companies are providing you complimentary identity theft and credit monitoring solutions from Equifax free of charge for 2 years. Equifax ID Patrol<sup>®</sup> has the following features:

- 3-Bureau credit file monitoring and alerts of key changes to your Equifax<sup>®</sup>, TransUnion<sup>®</sup> and Experian<sup>®</sup> credit reports;
- Access to your Equifax credit report;
- One Equifax 3-Bureau credit report;
- Wireless alerts (available online only and data charges may apply);



- Automatic Fraud Alerts. With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit (available online only);
- Credit Report Lock Allows users to limit access to their Equifax credit report by third parties, with certain exceptions;
- Internet Scanning Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there;
- Lost Wallet Assistance. If you lose your wallet, we'll help you cancel and re-issue your cards and ID;
- Up to \$1 MM in identity theft insurance; and
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Your unique activation code for your Equifax ID Patrol® is <<CODE>>.

To activate your subscription, visit [www.myservices.equifax.com/patrol](http://www.myservices.equifax.com/patrol) and enter your unique activation code before <<ENROLLMENT DEADLINE>>. The instructions for enrollment are set out below.

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, after reviewing the Terms of Use, 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.

If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity. To be eligible for Identity Restoration, you must complete the enrollment process for the subscription offer by the enrollment deadline above. Call the phone number listed in your online member center for assistance.

#### For More Information

Should you have any further questions or concerns regarding this matter and / or the protections available to you, you may contact our dedicated call center at <<TELEPHONE NUMBER>>.

Sincerely,

Kevin Shank, CEO  
Pivot Technology Solutions, Inc.





## Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
800-525-6285  P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	888-397-3742  P.O. Box 9554 Allen, TX 75013 www.experian.com	800-909-8872  P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

The following information reflects recommendations from the Federal Trade Commission regarding identity theft protection.

**Free Credit Report.** We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, Georgia 30348-5281.

**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 reporting agencies directly to obtain such additional report(s).

**Fraud Alert.** You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Pursuant to the Economic Growth, Regulatory Relief, and Consumer Protection Act, you may place a fraud alert on your file free of charge.

**For Colorado and Illinois residents:** You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

**Security Freeze.** Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.



The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

**For New Mexico residents:** You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

**For Colorado and Illinois residents:** You may obtain information from the credit reporting agencies and the FTC about security freezes.

**Federal Trade Commission and State Attorneys General Offices.** 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 the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT(438-4338).

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

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

**For Rhode Island residents:** You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

**Reporting of identity theft and obtaining a police report.** You have the right to obtain any police report filed in the United States 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.

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

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

**For Rhode Island residents:** You have the right to file or obtain a police report regarding this incident.