



Kristofer Swanson, CPA/CFF, CFE, CAMS
Vice President and Practice Leader, Forensic Services
312.619.3313 Direct
773.551.0293 Mobile
kswanson@crai.com

October 20, 2023

To Whom It May Concern:

Paycor, Inc., engaged Charles River Associates ("CRA"), through legal counsel, on June 1, 2023, to assist Paycor with two work streams related to the information security incident that compromised the MOVEit Transfer platform ("Incident") first reported publicly by Progress Software on May 31, 2023.

1. **Forensic Investigation**. CRA conducted a forensic investigation to assess if the scope of the Incident extended beyond the MOVEit Transfer platform, to include Paycor's information systems. CRA completed this work on July 19, 2023, and found no evidence of compromise beyond the MOVEit Transfer platform.

2. **Data Analysis**. CRA conducted an analysis of certain Paycor servers, logs and devices that were potentially exposed to unauthorized access as a result of the Incident. The purpose of this analysis was to identify which Paycor customers may have had sensitive data exposed as a result of the Incident. CRA commenced this analysis on June 6, 2023, and completed its analysis on October 20, 2023.

Very truly yours,

A handwritten signature in cursive script that reads "Kristofer Swanson".

Fwd: Notice of Security Incident Regarding the MOVEit Transfer Cyber Vulnerability

Roberta Giuliano <ragiuliano@comcast.net>

Wed 12/13/2023 11:51 AM

To: Kevin Giuliano <kgiuliano@pediatricspecialists.com>

----- Original Message -----

From: Paycor Data Privacy Office <no_reply@paycor.com>

To: ragiuliano@comcast.net

Date: 11/30/2023 11:00 AM EST

Subject: Notice of Security Incident Regarding the MOVEit Transfer Cyber Vulnerability



Dear Valued Customer,

We are contacting you today to let you know about a privacy concern involving some of your organization's information.

On May 31, 2023, Progress Software announced that it had discovered a previously unknown "zero-day" cyber vulnerability in its MOVEit Transfer software. MOVEit Transfer is used globally by governments and organizations, including Paycor and other human capital management (HCM) software providers, to send and receive certain data.

Paycor immediately took steps to address the issue, including launching a forensic analysis with the assistance of outside experts. The analysis shows the incident's scope was limited to the third-party MOVEit Transfer platform. An unauthorized third party exploited the cyber vulnerability on the MOVEit Transfer platform to obtain certain files transferred through the software. At no time during this incident was Paycor's HCM software impacted.

Paycor has completed an extensive data analysis and determined that some of your company's sensitive information was affected as a result of this incident. In line with best practices and pursuant to Paycor's legal duties, you are receiving this notification letter, which includes instructions for accessing a secure portal, which contains:

- a description of the individual(s) and data affected,
- FAQs and best practices, and
- a summary of the analysis completed by Charles River Associates, the industry-leading expert who completed both the forensic and data analysis on Paycor's behalf.

Please note that your company may have notification requirements, under applicable state law, to the individual(s) affected. Whether you notify any affected employees is at your sole discretion. Paycor is not your legal counsel and cannot provide you with legal advice.

Instructions For Accessing Information:

To learn more about the incident, the impacted data, and the resources available, please visit our MOVEit Transfer Security Incident Portal hosted by Kroll <https://www.krollnotification.com/redeem> and create an account. Kroll is a leading provider of risk and financial solutions, including cyber incident communication. When you access the Portal, **please enter access code – XVX32MXVJH – and Paycor's zip code 45212– to set up your account. You have until December 29, 2023 to access this information.**

For More Information:

We have established a dedicated response team to assist you with questions. This team is only able to speak to authorized business contacts and will not be able to answer questions from your employees directly. If you have questions:

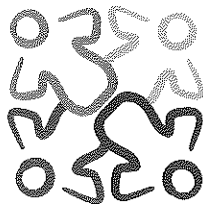
- Please call (866) 846-0912
- Hours of availability: Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.
- Please be prepared with your access code XVX32MXVJH

Paycor takes any matter that could affect information security seriously and remains committed to safeguarding the data entrusted to us. We sincerely regret any inconvenience or concern caused by this incident.

Paycor Data Privacy Office

ELN-20211

132 Central Street, Suite 116
Foxborough, MA 02035
508-543-6306



155 South Street
Wrentham, MA 02093
508-384-7867

PEDIATRIC SPECIALISTS
FOXBOROUGH · WRENTHAM

[INSERT NAME]
[INSERT STREET ADDRESS]
[INSERT CITY, STATE ZIP]
VIA REGULAR MAIL AND E-MAIL

December 13, 2023

Dear (Mr. /Ms. last name):

On behalf of Pediatric Specialists of Foxborough & Wrentham, LLP (the “Company”), I am writing to inform you that the Company recently received notice from its payroll company, Paycor, Inc. (“Paycor”), that Paycor recently experienced a breach of security affecting some of your personal information.

Right To File And/Or Obtain A Police Report

Under Massachusetts law, you have the right to file a police report in connection with this incident. In addition, if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You also have the right to obtain any police report that has been, or is, filed in regard to this incident. The Company has not filed a police report concerning this matter.

Requesting A Credit Report Security Freeze

You may request a credit report security freeze at no charge by contacting the three credit agencies at the phone numbers or contact information found at the links listed below. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

If you wish to obtain a security freeze, you should contact all three of the following credit reporting agencies:

Equifax Security Freeze

(888) 298-0045

<https://www.equifax.com/personal/help/security-freeze/>

Experian Security Freeze

(888) 397-3742

<https://www.experian.com/freeze/center.html#content-01%C2%A0>

TransUnion Security Freeze

(888) 909-8872

<https://www.transunion.com/credit-freeze/place-credit-freeze>

You will need the following information to request a credit report security freeze:

- Full name, address, Social Security number, and date of birth;
- Addresses where you lived over the previous five years;
- Proof of current address such as a utility or phone bill, rental agreement, or deed;
- A legible photocopy of a government issued identification card (state driver's license ID card, military identification, etc.);
- Social Security Card, pay stub, or W2;
- If you are an identity theft victim, include a copy of the police report, investigative report, or complaint.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

Credit Monitoring

If you would like to monitor your credit, you can request a complimentary credit report from Experian by using the following link: <https://www.experian.com/consumer-products/credit-monitoring.html>

In addition, the Company is offering you complimentary credit monitoring services for not less than 18 months. We have contracted with Norton to secure a Lifelock Ultimate Plus plan more each individual affected. Please refer to the Lifelock brochure for plan details. Enrollment instructions are included in this mailing as well. We strongly recommend you enroll in this complimentary monitoring service. In addition, you should also remain vigilant regarding your accounts and report any incidents of suspected identity theft to the Company.

If you have any questions concerning this notification, please feel free to reach out to me directly at kgiuliano@pediatricspecialists.com.

Sincerely,

Kevin Giuliano
Chief Operations Officer