
To Whom It May Concern,

Hythe's payroll provider alerted us to a Cyber Breach. IAW the Maryland OAG website, we have informed all impacted employees. Attached is a sample of the letter provided. We had 10 employees impacted.

At this time, our payroll provider has improved their cyber posture. Hythe continually monitors for opportunities to improve.

Should any further action be required or if you have any questions, please contact the undersigned.

Regards,
Heather

Heather Couvillon Lufburrow
Hythe Research CEO
heather@hytheresearch.com
301.751.6600

The contents of this e-mail and any attachments are intended solely for the use of the named addressee(s) and may contain confidential and/or privileged information. Any unauthorized use, copying, disclosure, or distribution of the contents of this e-mail is strictly prohibited by the sender and may be unlawful. If you are not the intended recipient, please notify the sender immediately and delete this e-mail.

1 December 2023

Subject: Paycor MOVEit Cyber Incident / Data Breach

Dear SAMPLE SAMPLE,

We are contacting you about a data breach that has occurred.

What happened - On 30 November 2023, Hythe received notice that Paycor recently identified unusual activity on one of its third-party file transfer software platforms. This incident is related to Progress Software's MOVEit Transfer cyber vulnerability identified on 31 May 2023, which has been affecting hundreds of companies worldwide. Unfortunately, Paycor was among these companies. An unauthorized third party exploited the cyber vulnerability on the MOVEit Transfer platform to obtain certain files transferred through the software.

What Information was involved - Unfortunately, your personal information, including name, date of birth, and social security number was compromised through a previously unknown "zero-day" cyber vulnerability in its MOVEit Transfer software.

What we are doing - Paycor immediately took steps to address the issue, including launching a forensic analysis with the assistance of outside experts. Paycor had Charles River Associates complete a forensic and data analysis. The analysis shows the incident's scope was limited to the third-party MOVEit Transfer platform. At no time during this incident was Paycor's HCM software impacted.

What you can do - The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111

Experian: experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

We have attached information from the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.

Contact Information - For additional information, you may contact Hythe Research 410-928-4050 or privacy@hytheresearch.com.

We sincerely apologize for the inconvenience this may cause.

Sincerely,



Heather Couvillon Lufburrow, CEO

1 December 2023

Subject: Paycor MOVEit Cyber Incident / Data Breach

Dear SAMPLE SAMPLE,

We are contacting you about a data breach that has occurred.

What happened - On 30 November 2023, Hythe received notice that Paycor recently identified unusual activity on one of its third-party file transfer software platforms. This incident is related to Progress Software's MOVEit Transfer cyber vulnerability identified on 31 May 2023, which has been affecting hundreds of companies worldwide. Unfortunately, Paycor was among these companies. An unauthorized third party exploited the cyber vulnerability on the MOVEit Transfer platform to obtain certain files transferred through the software.

What Information was involved - Unfortunately, your personal information, including name, date of birth, and social security number was compromised through a previously unknown "zero-day" cyber vulnerability in its MOVEit Transfer software.

What we are doing - Paycor immediately took steps to address the issue, including launching a forensic analysis with the assistance of outside experts. Paycor had Charles River Associates complete a forensic and data analysis. The analysis shows the incident's scope was limited to the third-party MOVEit Transfer platform. At no time during this incident was Paycor's HCM software impacted.

What you can do - The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111

Experian: experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

We have attached information from the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.

Contact Information - For additional information, you may contact Hythe Research 410-928-4050 or privacy@hytheresearch.com.

We sincerely apologize for the inconvenience this may cause.

Sincerely,



Heather Couvillon Lufburrow, CEO