



March 4, 2024

VIA EMAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street,
Concord, NH 03301
DOJ-CPB@doj.nh.gov

RE: NOTICE OF DATA SECURITY INCIDENT

Dear Attorney General John Formella:

Constangy, Brooks, Smith & Prophete, LLP, represents Harvey Construction Corporation's ("Harvey Construction") in connection with a recent data security incident at a third-party service provider described in greater detail below. Harvey Construction takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent on behalf of Harvey Construction because personal information for New Hampshire residents may have been involved in the incident.

I. NATURE OF THE SECURITY INCIDENT

On November 30, 2023 our external payroll and benefits provider, Paycor, notified us that it was one of many organizations across the globe that were recently affected by the MOVEit software vulnerability, and the incident resulted in some Harvey Construction files being downloaded by an unauthorized actor on May 31, 2023. Paycor utilizes the MOVEit tool to transfer data to and from its clients, including Harvey Construction. Paycor enlisted third-party experts to review and analyze certain Paycor servers, logs and devices that were potentially exposed to the unauthorized access. Paycor informed us that, based on its review, the impacted files contained personal information for some of Harvey Construction's current and former employees.

Harvey Construction reviewed the affected file and took steps to provide notification to all members whose information was contained therein.

II. NUMBER OF NEW HAMPSHIRE RESIDENTS INVOLVED

On February 27, 2024, Harvey Construction determined that the notification population included 122 New Hampshire residents. On March 4, 2024, Harvey Construction provided notification by first-class U.S. mail to these individuals via the attached notification letter template or a substantially similar version thereof.

Alabama Arkansas California Colorado District of Columbia Florida Georgia Illinois
Indiana Maryland Massachusetts Minnesota Missouri New Jersey New York
North Carolina Oregon Pennsylvania South Carolina Tennessee Texas Virginia Washington

Per Paycor, the personal information involved in this incident includes individuals'

III. STEPS TAKEN TO ADDRESS THE INCIDENT

As soon as Harvey Construction was alerted to the incident by Paycor, Harvey Construction undertook a review of the affected file to identify the information it contained, the individuals to whom the information pertained, and arranged for notification to all affected individuals.

Harvey Construction has established a toll-free call center through IDX to answer questions about the incident and address related concerns. Harvey Construction is also offering of complimentary credit and identity monitoring services to the potentially affected individuals.

IV. CONTACT INFORMATION

Harvey Construction remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at

Sincerely,

Maria Efaplatidis
Partner
Constangy, Brooks, Smith & Prophete, LLP

Encl. Sample Notification Letter



4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

March 4, 2024

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>:

I am writing to notify you about a cybersecurity incident at one of Harvey Construction Corporation’s (“Harvey Construction”) external vendors that may have affected your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened: On November 30, 2023 our external payroll and benefits provider Paycor notified us that it was one of many organizations across the globe that were recently affected by the MOVEit software vulnerability, and the incident resulted in some Harvey Construction files being downloaded by an unauthorized actor on May 31, 2023. Paycor utilizes the MOVEit tool to transfer data to and from its clients, including Harvey Construction. Paycor enlisted third-party experts to review and analyze certain Paycor servers, logs and devices that were potentially exposed to the unauthorized access. Paycor informed us that, based on its review, the impacted files contained personal information for some of Harvey Construction’s current and former employees. Paycor provided us with a list of those individuals, and we took immediate steps to issue notification letters as quickly as possible.

What Information Was Involved: The information involved may have included your number. Please note that we have no evidence of any actual or suspected misuse of this information.

What We Are Doing: Paycor retained a leading cybersecurity firm to conduct a forensic investigation into the incident, which confirmed that there was no evidence of compromise beyond the MOVEit transfer platform. Further, none of Harvey Construction’s systems were affected. Paycor also reported the incident to law enforcement and implemented technical measures to fix the MOVEit vulnerability shortly after it was publicized. Harvey Construction is reviewing our relationships with each of our vendors to ensure that they are maintaining the necessary security standards and procedures to reduce the chances of a similar incident occurring again.

While there is no evidence your information has been misused, out of an abundance of caution we are offering you complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: <<12/24>> months of credit¹ and CyberScan monitoring, a \$1,000,000 identity theft insurance reimbursement policy, and fully managed identity theft recovery services. To enroll, please call 1-800-939-4170 or visit <https://app.idx.us/account-creation/protect> and provide the enrollment code at the top of this page. Please note that the deadline to enroll is .

To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What You Can Do: We encourage you to enroll in the complimentary credit protection services we are offering. With this protection, IDX can help you resolve issues if your identity is compromised. Please also review the guidance included with this letter which lists additional resources you may utilize to help protect your information.

For More Information: If you have questions or need assistance, please contact 1-800-939-4170, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

Miranda Diversi
Harvey Construction
10 Harvey Road
Bedford, NH 03110

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports 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 incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

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 <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. 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 potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. 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 insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave,
NW Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.