wyrickrobbins

Wyrick Robbins Yates & Ponton LLP
ATTORNEYS AT LAW
4101 Lake Boone Trail, Suite 300, Raleigh, NC 27607
PO Drawer 17803, Raleigh, NC 27619
P: 919.781.4000 F: 919.781.4865 www.wyrick.com
MEMBER OF MERITAS LAW FIRMS WORLDWIDE

December 20, 2023

New Hampshire Department of Justice
Consumer Protection and Antitrust Bureau
1 Granite Place South
Concord, New Hampshire 03301

Re: Notification of Paycor Security Incident

To whom it may concern:

I am writing to notify you pursuant to N.H. Rev. Stat. § 359-C:20 of a security incident experienced by Paycor, Inc. ("Paycor"), which acts as a payroll support vendor for our client, MED-EL Corporation, USA ("MED-EL").

On May 31, 2023, Paycor learned that it was part of the global incident involving a zero-day vulnerability of the file transfer tool called MOVEit. Paycor waited months before it contacted its customers about "a potential privacy concern" related to the MOVEit incident. Paycor was not able to confirm whether MED-EL was affected. MED-EL made repeated efforts to determine the nature of the concern and whether MED-EL employee data was impacted. MED-EL received delayed and conflicting information from Paycor. For example, Paycor first notified MED-EL that "some of your company's data may have been in the platform resulting from transferring files from your previous provider to Paycor." Then, Paycor notified MED-EL that it was "not impacted by the MOVEit breach, and no data was compromised." But on November 30, 2023, Paycor notified MED-EL that specific MED-EL employee information was impacted and provided a list of impacted individuals.

Paycor informed MED-EL that this incident impacted one New Hampshire resident. Paycor's investigation revealed that the information affected included the following data elements: . We sent notification letters to impacted individuals on December 20, 2023. MED-EL is providing those individuals with free credit monitoring for . We have enclosed an example of the notification letter.

Thank you for your time and attention to this matter. Please let us know if you have any questions or concerns regarding this notice or the incident.

Sincerely,

Elizabeth H. Johnson

MED EL

Address1
Address2
City, State, Zip Code

Date (Format: Month Day, Year)

Notice of Paycor Data Breach

Dear Recipient's FirstName and Last Name,

We are writing to make you aware of a Paycor security incident that affected your personal information. Paycor is MED-EL's payroll support vendor. MED-EL did not experience a security issue: this matter affected Paycor, which had access to information about you due to the services it provided to MED-EL. This letter describes the Paycor security incident, what we are doing in response, and what you can do.

What Happened?

Paycor contacted its customers, including MED-EL, and notified them that Paycor had identified unusual activity within the file transfer software Paycor uses to transfer files. Paycor initiated a forensic investigation and determined that unauthorized parties had infiltrated its file transfer system, a product called MOVEit.

Although Paycor discovered the unusual activity on May 31, 2023, it waited months to inform MED-EL and was not able to confirm whether MED-EL was affected. From the time we were first notified, we made repeated efforts to obtain more information from Paycor, including confirmation that MED-EL was affected. While Paycor's investigation was pending, on October 24, 2023, we notified all our current employees that the Paycor security incident may have impacted MED-EL. On November 30, 2023, Paycor notified us that MED-EL was affected, and identified your personal information among the information impacted by this incident.

What Information Was Involved?

Paycor has advised us that the affected personal information included your

.

What We Are Doing.

Although MED-EL's own systems were not impacted, we are coordinating with Paycor to ensure this incident is addressed and remediated.

To help protect your identity, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: of Credit and CyberScan monitoring, a $1,000,000 insurance

reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. We encourage you to enroll in free IDX identity protection services by going to https://app.idx.us/account-creation/protect, calling 1-800-939-4170, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. **Please note the deadline to enroll is .What You Can Do.**

Please review the enclosed "Additional Resources" document. This document provides instructions on how to enroll in IDX identity protection services and describes additional steps you can take to help protect yourself, such as remaining vigilant by regularly reviewing your account statements and monitoring credit reports. This document also provides contact details for the Federal Trade Commission and credit reporting agencies as well as information on how to place fraud alerts and security freezes.

For More Information.

We sincerely regret you were impacted by this event. If you have questions, please contact:

Sincerely,

Poonam Khullar
Compliance Manager
MED-EL Corporation, USA

MED EL

Additional Resources

These additional resources are provided to assist you to identify measures you may take to help protect yourself and your information. For example, this information includes contact details for the Federal Trade Commission and credit reporting agencies, from which you can obtain information about fraud alerts and security freezes.

Enroll in Free IDX Identity Protection Services:
Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Review your account statements and notify law enforcement of suspicious activity: As a precautionary measure, we recommend you remain vigilant for incidents of fraud and identity theft, including 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 can also report fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

FTC 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 FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the FTC at: Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Credit Reporting Agencies: 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 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	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800

MED-EL Corporation • 2645 Meridian Parkway • Suite 100 • Durham, NC 27713
Tel 888-633-3524 • Fax 919-484-9229 • implants.us@medel.com • www.medel.com

www.equifax.com www.experian.com 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 stays on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests 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.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This prevents new credit from being opened in your name without the use of a PIN 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.

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, visit www.consumer.ftc.gov\\articles\\pdf-0096-fair-credit-reporting-act.pdf.

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

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, 1-877-566-7226.

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 Washington, D.C. residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, www.oag.dc.gov, 1-202-727-3400. You also have the right to obtain a credit freeze at no cost to you. Please see instructions above for how to request a security freeze on your credit file.

MED-EL Corporation • 2645 Meridian Parkway • Suite 100 • Durham, NC 27713
Tel 888-633-3524 • Fax 919-484-9229 • implants.us@medel.com • www.medel.com