POSTAL VERSION

[180 Medical LETTERHEAD / CONTACT INFORMATION]

[DATE]

[RETURN ADDRESS LINE 1]
[RETURN ADDRESS LINE 2]

[RECIPIENT'S NAME]
[ADDRESS]
[CITY, STATE, ZIP]

EMAIL VERSION – CONVATEC BANNER

SUBJECT: NOTICE OF DATA BREACH

Dear [NAME],

We are required to send this formal notification.

Further to our email on Friday, I am writing on behalf of Convatec's 180 Medical business ("180 Medical," "we," and/or "us") to notify you that 180 Medical recently experienced an isolated data security incident impacting your personal information. We are providing this notification to help you understand what happened and what we are doing in response. We are taking this matter very seriously and sincerely regret any concerns that it may cause you.

What happened: 180 Medical recently experienced an incident in which an email was inadvertently sent to an unauthorized party. We promptly launched an investigation and identified evidence that, on February 18, 2025, the email contained certain employee information, including yours.

What information was involved: The impacted information included information on your W-2 form, including your name, address, and Social Security number.

What we are doing: Upon learning of the incident, we promptly took steps to investigate, secure our systems and contain the incident. To reduce the risk of similar events happening in the future, 180 Medical is working to further enhance its security controls including training and controls to prevent the disclosure of personal information to unauthorized third parties.

We also have also arranged access to, at no cost to you, 24 months of credit monitoring services from Experian. Information regarding these services is included in Attachment 1 to this letter.

What you can do: We encourage you to sign up for the free credit monitoring from Experian. Information about enrollment is included in Attachment 1 to this letter. We also recommend that you remain vigilant by reviewing your account statements and monitoring your free credit reports for signs of suspicious activity, and take the steps outlined in Attachment 3 to protect your tax information and utilize the additional security protections available from the IRS. Please find additional information in Attachments 2 and 3 to this letter.

For more information: If you have questions or concerns regarding this incident, we have setup a toll- free phone number 1-833-918-8060 which you can call Monday through Friday between 8:00am - 8:00pm central time (excluding major U.S. holidays).

Best regards,

Mark Jassey President & Chief Operating Officer, Continence Care & Home Services Group	**Michelle Levin** VP, Chief Data Privacy Officer Convatec

Attachment 1: Credit Monitoring Services Enrollment Information

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for twenty-four (24) months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for twenty-four (24) months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24) -month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by 5/31/2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**: **[Activation Code]**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-918-8060 by 5/31/2025. Be prepared to provide engagement number **B140817** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [24]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Attachment 2: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the Federal Trade Commission (FTC). You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information
Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Whether or not you enroll in the credit monitoring product offered, you also have the right to place an initial fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and is placed on a consumer's credit file. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Fraud alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A fraud alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting agencies is:

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
https://www.experian.com/help/

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
https://www.transunion.com/credit-help

Free Credit Report Information
You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. We encourage you to review your rights pursuant to the FCRA by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a

group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself and prevent such activity. If you are a resident of Iowa, Maryland, New York, North Carolina, or Oregon, you can also reach out to your respective state's Attorney General's office at the contact information below. Residents of all other states can find information on how to contact your state attorney general at https://www.naag.org/ find-my-ag/.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357)
www.ftc.gov/idtheft

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926
www.iowaattorneygeneral.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

New York Attorney General's Office
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/consumer-frauds-bureau/identity-theft

North Carolina Department of Justice
114 West Edenton Street
Raleigh, NC 27603
1-919-716-6400
https://ncdoj.gov/protecting-consumers/identity-theft/

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392
https://justice.oregon.gov

Security Freeze Information

You have the right to request a free security freeze (aka “credit freeze”) on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A credit freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
http://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
https://www.transunion.com/credit-freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Attachment 3: Protecting your Tax Information

The IRS provides additional security controls and methods of viewing your tax records in circumstances where your social security number has been compromised.

Identity protection PIN (IP PIN)
An identity protection PIN (IP PIN) is a six-digit number that prevents someone else from filing a tax return using your Social Security number (SSN) or individual taxpayer identification number (ITIN). The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft.

The fastest way to receive an IP PIN is to request one through your Online Account. If you don't already have an account on IRS.gov, you must register to validate your identity.

Monitor you tax records
The IRS enables individuals to access their Tax Records and transcripts to check for unauthorized filings. For more information on how to request your transcripts either online or via phone or mail see the IRS website.

Report Identity Theft to the IRS
If you suspect your identity has been stolen, you should contact the IRS and report possible identity theft. You will need to File Form 14039 (Identity Theft Affidavit), explaining the situation. You can complete the form online, or return it via mail or fax. You can also call the IRS Identity Protection Specialized Unit at 1-800-908-4490 (Monday–Friday, 7 AM to 7 PM local time) and inform them of the potential theft of your SSN. They can inform you if any fraudulent tax returns have been filed.