



Lynda Jensen, Partner
Cybersecurity & Data Privacy Team
800 Boylston Street
Boston, MA 02199
Email: ljensen@constangy.com
Phone: 617.849.7888

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

November 6, 2025

VIA ELECTRONIC MAIL

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

Re: Dealmed Medical Supplies, LLC- Preliminary Notice of Data Event

To Whom It May Concern:

We represent Dealmed Medical Supplies, LLC (the “Company”), located at 3512 Quentin Rd, 1st Floor, Brooklyn, NY 11234, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately one (1) New Hampshire resident. The purpose of this letter is to notify you of the event in accordance with the New Hampshire data breach notification statute. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the Company does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

1. Nature of the Data Security Event

On or about June 7, 2025, the Company became aware of unusual network activity and immediately took steps to secure its systems. The company immediately began an investigation. The investigation determined that certain Company data may have been acquired without authorization on or about June 7, 2025. The Company then undertook a comprehensive review of the potentially affected data, which concluded on October 31, 2025. The Company identified that certain individual information may have been affected.

2. Notice to New Hampshire Residents

On or about November 6, 2025, the Company provided written notice of this incident to approximately one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

3. Other Steps Taken and To Be Taken

Upon discovering the event, the Company moved quickly to investigate and respond to the incident, assess the security of systems, and identify potentially affected individuals.

Additionally, the Company is providing impacted individuals with guidance on how to better protect against identity theft and fraud. The Company is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

If you have any questions or need additional information regarding this event, please do not hesitate to contact me at ljensen@constangy.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Lynda Jensen", with a long horizontal flourish extending to the right.

Lynda Jensen, Partner
Constangy, Brooks, Smith & Prophete LLP

Attachment: Template Consumer Notification Letter



Dealmed Medical Supplies, LLC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1952



[REDACTED]
[REDACTED]
[REDACTED]



November 4, 2025

Subject: Notice of Data Security Incident

Dear [REDACTED]:

Dealmed Medical Supplies, LLC. is writing to inform you of a recent data security event that may have affected your personal information. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the event and steps that you can take to help protect your personal information.

What Happened. On June 7, 2025, we detected unusual activity on our network and promptly investigated to understand the nature and source of the activity. We engaged independent cybersecurity experts to assist with the process. As a result of the investigation, we determined that certain files may have been accessed or acquired without authorization on June 7, 2025. We undertook exhaustive efforts to understand to whom the accessible files related and how to contact those individuals. Our review revealed that the files contain some of your personal information, which is why we are notifying you. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your name and Social Security number.

What We Are Doing. As soon as we discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. In addition, we are offering you complimentary access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. The deadline to enroll in these services is after 3 months of receiving this letter.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please

provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You also can enroll in the complementary services offered to you through CyberScout by using the enrollment code provided above.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-800-405-6108 Monday through Friday from 8:00 a.m. to 8:00 p.m. We take your trust in us and this event very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Dealmed Medical Supplies, LLC.



Steps You Can Take To Help Protect Your Personal 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 (the “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 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 2000
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. You cannot be charged to place or lift a fraud alert. Additional information is available at www.annualcreditreport.com.

Credit Freeze: You have the right to put a credit 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 credit freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a credit freeze may interfere with or delay your ability to obtain credit. You must separately place a credit freeze on your credit file with each credit reporting agency. In order to place a credit 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 cannot be charged to place or lift a credit freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, credit 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
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
[www.marylandattorneygeneral.gov/
Pages/CPD](http://www.marylandattorneygeneral.gov/Pages/CPD)
1-888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
[www.doj.state.or.us/
consumer-protection](http://www.doj.state.or.us/consumer-protection)
1-877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
1-800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
1-800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
1-888-777-4590

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
[www.dos.ny.gov/
consumerprotection/](http://www.dos.ny.gov/consumerprotection/)
1-212-416-8433

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
1-202-442-9828

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
1-502-696-5300

NC Attorney General

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

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.