



Julie Hess, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, Pennsylvania 19102
jhess@constangy.com
Direct: 610.416.9236

November 19, 2025

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
Tel: 207-626-8800

Email: breach.security@maine.gov

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents WEL Companies, Inc. ("WEL") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident.

1. Nature of the security incident.

On January 31, 2025, WEL noted unusual activity on its network. In response, WEL immediately took steps to secure its digital environment and engaged a leading, independent, cybersecurity firm to conduct an investigation. As a result of the investigation, it was learned that certain data stored on WEL systems may have been accessed or acquired without authorization and that certain individuals' personal information may reside in the potentially affected data. A comprehensive review of the types of personal information involved, the identification of potentially impacted individuals, and verification of current mailing addresses for those individuals was then conducted. On November 12, 2025, it was determined that personal information belonging to certain Maine residents may have been impacted in connection with this incident. Please note that we have no current evidence to suggest misuse or attempted misuse of any personal information in conjunction with this incident.

2. Number of Maine residents affected.

WEL notified 515 Maine residents of this incident via first class U.S. mail on November 18, 2025. The information potentially impacted in connection with this incident includes name, Social Security Number and driver's license or state ID.

A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

13758246v3
13771508v1

3. Steps taken relating to the Incident.

As soon as WEL discovered this incident, WEL took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal information potentially impacted. In addition, WEL implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future. Furthermore, complimentary identity protection services are being offered to all individuals notified of this incident.

4. Contact information.

WEL remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me directly by phone 610.416.9236 or email at jhess@constangy.com.

Respectfully,

A handwritten signature in cursive script, appearing to read "Julie Hess".

Julie Hess

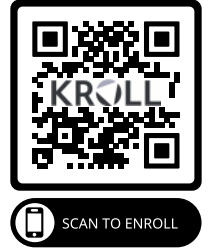
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter



<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



<<Date>> (Format: Month Day, Year)

Subject: <<b2b_text_1 (Notice of Data Security Incident / Breach)>>

Dear <<first_name>> <<last_name>>:

We are writing to notify you of a data security incident which may have affected your information. WEL Companies (“WEL”) takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened. On January 31, 2025, we experienced a network disruption and immediately initiated an investigation of the matter. We engaged independent cybersecurity experts to assist with the process. The investigation determined that certain files were acquired without authorization on March 28, 2025. We then undertook a comprehensive review of those files and, on or about November 12, 2025, learned that some of your personal information was contained within the potentially affected data which is the reason for this notification. 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 <<b2b_text_2 (Data Elements)>>.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. We have also taken additional steps and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future.

We are also offering you identity monitoring at no cost to you for <<ServiceTerminMonths>> months through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number (S_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com

What You Can Do. You can follow the recommendations included with this letter to protect your information. You can also enroll in the complimentary services offered to you through Kroll 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 (844) 354-9425 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any inconvenience this may cause.

Sincerely,

WEL Companies
1625 S. Broadway P.O. Box 5610
De Pere, WI 54115-5610

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 740256
Atlanta, GA 30347
1-800-525-6285
www.equifax.com

Experian

P.O. Box 4500
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. Additional information is available at 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
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
[www.marylandattorneygeneral.gov/
Pages/CPD](http://www.marylandattorneygeneral.gov/Pages/CPD)
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)
877-877-9392

California Attorney General

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

New York Attorney General

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

Rhode Island Attorney General

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

Iowa Attorney General

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

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
[www.dos.ny.gov/consumerprotection/
212.416.8433](http://www.dos.ny.gov/consumerprotection/)

Washington D.C. Attorney General

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

Kentucky Attorney General

700 Capitol Avenue, Suite 118

Frankfort, Kentucky 40601

www.ag.ky.gov

502-696-5300

NC Attorney General

9001 Mail Service Center

Raleigh, NC 27699

ncdoj.gov/protectingconsumers/

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.