CONSTANGY BROOKS, SMITH & PROPHETE LLP

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

Alyssa Watzman, Partner
Cybersecurity & Data Privacy Team
1801 Broadway, 529
Denver, CO 80202
awatzman@constangy.com
Direct: 720.536.3234

July 29, 2025

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509

VIA PORTAL ONLINE

Re: Notice of Data Security Event

To Whom It May Concern:

We represent EverCommerce, located at 3601 Walnut Street, Suite 400, Denver, Colorado 80205, and are writing to notify your office of an incident that may have affected the security of certain personal information belonging to a Nebraska resident. This notice will be supplemented with any new significant facts learned about the incident subsequent to its submission. By providing this notice, EverCommerce does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, personal jurisdiction, or any other potentially applicable rights or defenses.

1. Nature of the Data Event

On May 26, 2025, EverCommerce learned that an unknown actor may have accessed limited EverCommerce information. In response, EverCommerce immediately took steps to ensure the security of the impacted environment and launched an investigation to determine what happened. As a result of the investigation, EverCommerce learned that an unauthorized actor accessed or acquired limited EverCommerce information between May 25, 2025 and May 27, 2025. EverCommerce undertook a time-intensive review of the impacted dataset to confirm what information was involved and to whom it belonged and then worked diligently to identify contact information for such individuals to complete notification.

The information that could have been subject to unauthorized access includes first and last name, as well as Social Security number.

2. Notice to Nebraska Resident

On or about July 29, 2025, EverCommerce provided written notice of this incident to one (1) Nebraska resident. Written notice is being provided in substantially the same form as the letter attached.

3. Other Steps Taken and To Be Taken

Upon becoming aware of the event, EverCommerce moved quickly to investigate and respond to the incident, assess the security of the relevant EverCommerce environment, and identify the potentially affected individual. EverCommerce is also working to implement additional safeguards and training to its employees. EverCommerce is providing access to credit monitoring services for twelve (12) months, through TransUnion, to the individual whose personal information was potentially affected by this incident, at no cost to the individual.

Additionally, EverCommerce is providing the impacted individual with guidance on how to better protect against identity theft and fraud. EverCommerce is providing the individual 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 information about how to contact the Federal Trade Commission, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 720.536.3234.

Very truly yours,

Alyssa Watzman of
Constangy, Brooks, Smith & Prophete LLP

Encl.

EverCommerce
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P 00001010 2G0500

July 25, 2025

Re: Notice of Data

Dear ,

We are writing to inform you of a recent data security incident that may have involved your personal information. EverCommerce takes the privacy and security of all information within our possession very seriously. That is why we are notifying you of the incident and providing you with information about steps you can take to help protect your personal information.

What Happened. On May 26, 2025, we became aware that an unauthorized actor may have accessed limited EverCommerce employee information. We immediately took steps to ensure the security of the impacted environment and launched an investigation to determine what happened. As a result of the investigation, we learned that an unauthorized actor accessed or acquired limited EverCommerce information between May 25, 2025 and May 27, 2025. We partnered with third-party forensic experts to undertake a time-intensive review of the impacted dataset to confirm what information was involved and to whom it belonged. We worked diligently to identify contact information for the individuals whose information we located in the dataset to complete notification. This review was completed on July 24, 2025.

Importantly, the investigation yielded no evidence of the successful or attempted misuse of any information potentially impacted in connection with this incident. Our third-party forensics experts have continued to monitor the dark web for the posting of this information and no potentially impacted information has been identified as having been posted.

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

What We Are Doing. As soon as we learned of the incident, we took the measures described above and implemented additional security features to reduce the risk of a similar incident occurring in the future. We are also providing you with information about steps you can take to help protect your personal information.

Additionally, we are offering you the opportunity to enroll in Single Bureau Credit Monitoring and identity protection services provided by Cyberscout, a TransUnion company at no cost to you. The services, which are free to you upon enrollment, include months of credit monitoring. Please note the deadline to enroll is 90 days from the date of this letter.

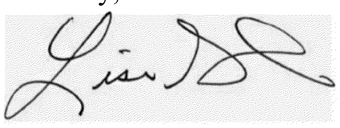
What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through Cyberscout at no cost to you. 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.

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: . 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.

For More Information. If you have questions about the incident, please call at 1-800-405-6108, Monday through Friday from 7:00 a.m. to 7:00 p.m. Central Time. Representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

We deeply regret any concern or inconvenience that this may cause you.

Sincerely,



Lisa Storey
Chief Legal Officer
EverCommerce

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	Experian	TransUnion
P.O. Box 105851	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-833-799-5355
www.equifax.com	www.experian.com	www.transunion.com/get-credit-report

0000102028000 P

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. For TransUnion: www.transunion.com/fraud-alerts.

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. For TransUnion: www.transunion.com/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, 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

Missouri Attorney General
207 W. High Street
P.O. Box 899
Jefferson City, MO 65102
ago.mo.gov
573-751-3321

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

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

New York Attorney General
The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

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

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.