



Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
aweaver@constangy.com
Direct: 215.770.4234

March 3, 2025

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Tel: 410-576-6491
Email: Idtheft@oag.state.md.us

Re: Bavaria Sausage, Inc. - Notice of Data Event

To Whom It May Concern:

We represent Bavaria Sausage, Inc. ("Bavaria Sausage"), located at 6317 Nesbitt Road, Fitchburg, Wisconsin 53719, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately 117 Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Bavaria Sausage does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

Bavaria Sausage was recently alerted to unusual activity involving its online store, bavariasausage.com. Upon becoming aware of this activity, Bavaria Sausage engaged an independent digital forensics firm to help investigate the activity and determine whether any customer payment card information had been accessed or acquired without authorization. After a thorough forensic investigation, in January 2025, Bavaria Sausage determined that this incident may have involved payment card information for customers who made a purchase through the online store between April 6, 2024, and January 17, 2025. Bavaria Sausage then worked diligently to identify all potentially affected customers.

The information that could have been subject to unauthorized access includes first and last name, as well as payment card numbers, expiration dates, and security codes.

2. Notice to Maryland Residents

On or about March 3, 2025, Bavaria Sausage provided written notice of this incident to approximately 117 Maryland residents. 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, Bavaria Sausage moved quickly to investigate and respond to the incident, assess the security of its online store, and identify potentially affected individuals. Bavaria Sausage is providing access to identity resolution services, through Cyberscout, a TransUnion company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals, and is encouraging all potentially affected individuals to review their account statements and report any activity they do not recognize to their card's issuing bank. Bavaria Sausage is further providing impacted individuals with guidance on how to better protect against identity theft and fraud.

Bavaria Sausage is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (215) 770-4234.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Aubrey Weaver', with a stylized, flowing script.

Aubrey Weaver of
Constangy, Brooks, Smith & Prophete LLP

Exhibit A

Bavaria Sausage, Inc
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



P
[Redacted]



March 03, 2025

Subject: Notice of [Redacted]

Dear [Redacted]:

Bavaria Sausage, Inc. ("Bavaria Sausage") is writing to notify you of a data security incident relating to our online store that may have involved your payment card information. Bavaria Sausage takes the security of our customers' information very seriously. We are writing to inform you of the incident and to provide information about steps you can take to protect your information.

What Happened? Bavaria Sausage was recently alerted to unusual activity involving our online store, bavariasausage.com. Upon becoming aware of this activity, we engaged an independent digital forensics firm to help us investigate the activity and determine whether any customer payment card information had been accessed or acquired without authorization.

What Information Was Involved? After a thorough forensic investigation, in January 2025, we determined that this incident may have involved payment card information for customers who made a purchase through our online store between April 6, 2024, and January 17, 2025. We then worked diligently to identify all potentially affected customers. The information that may have been involved includes names, email addresses, payment card numbers, expiration dates, and security codes.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. In addition, we are cooperating with our merchant processor and the payment card brands in an effort to protect your information and prevent fraudulent activity. In order to reduce the likelihood of a similar incident occurring in the future, we have implemented additional measures to enhance the security of our website.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

In addition, Bavaria Sausage has arranged to provide its customers complimentary identity resolution services through TransUnion. 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.

If you identify any payment card transactions that you do not understand or that look suspicious, or if you suspect that any fraudulent transactions have taken place, please call 1-833-799-3764 Monday through Friday between 8:00 am and 8:00 pm Eastern Time, excluding US holidays.

000010102G0500

P

For More Information. If you have any questions regarding this letter, we encourage you to contact our dedicated call center at 1-833-799-3764 between 8:00 am and 8:00 pm Eastern Time.

Bavaria Sausage takes our customers' trust in us very seriously. Please accept our sincere apologies for any concern or inconvenience this may cause you.

Sincerely,

Bavaria Sausage, Inc.

6317 Nesbitt Rd

Fitchburg, WI 53719

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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 incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (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 <http://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. Additional information is available at <http://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
888-743-0023

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

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

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



00001020280000

P

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

**New York Bureau of Internet and
Technology**
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

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

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

North Carolina 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 <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> .