



Matthew Toldero, Partner
Cybersecurity & Data Privacy Team
One West 4th Street, Suite 850
Winston-Salem, NC 27101
mtoldero@constangy.com
Mobile: 336.448.8552

March 10, 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: Cardi's Department Store Inc. - Notice of Data Event

To Whom It May Concern:

We represent Cardi's Department Store Inc. ("Cardi's"), located at 1 Furniture Way, Swansea, Massachusetts 02777, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately five (5) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Cardi's 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

On February 6, 2025, Cardi's learned that personal information of certain individuals was potentially accessed without authorization. The unauthorized access was the result of a suspicious event first learned of on or about September 30, 2024. Specifically, Cardi's identified suspicious activity on its network disrupting access to certain of its systems. Upon learning of this activity, Cardi's immediately took steps to secure its network and engaged digital forensics specialists to assist with the investigation and determine whether sensitive information may have been accessed or acquired during the incident. Through the investigation, it was discovered that certain files may have been accessed or acquired without authorization. Following this confirmation, Cardi's conducted a comprehensive review of the potentially affected data and determined that personal information belonging to certain individuals, may have been accessed in connection with this incident. Cardi's then worked diligently to effectuate notification to potentially affected individuals.

The information that could have been subject to unauthorized access includes first and last name, as well as Social Security number, driver's license number, health insurance information, and medical condition or treatment information.

2. Notice to Maryland Residents

On or about March 10, 2025, Cardi's provided written notice of this incident to approximately five (5) 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, Cardi's moved quickly to investigate and respond to the incident, assess the security of Cardi's systems, and identify potentially affected individuals. Further, Cardi's notified federal law enforcement regarding the event. Cardi's also implemented additional safeguards and training. Cardi's is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals, and is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Cardi's 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.

Cardi's is providing written notice of this incident to relevant state and federal 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 (336) 448-8552.

Very truly yours,

A handwritten signature in cursive script that reads "Matthew Toldero".

Matt Toldero of
Constangy, Brooks, Smith & Prophete LLP

Exhibit A

Cardi's

FURNITURE & MATTRESSES

P.O. Box 989728

West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

March 10, 2025

Subject: Notice of Data <<Variable Text 1: Security Incident/Breach>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of the recent data security incident experienced by Cardi's Department Store Inc. ("Cardi's") that may have affected your personal information. Cardi's takes the privacy and security of all personal information within its possession seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On September 30, 2024, Cardi's identified suspicious activity on its network disrupting access to certain of its systems. Upon learning of this activity, Cardi's immediately took steps to secure its network and engaged digital forensics specialists to assist with the investigation and determine whether sensitive information may have been accessed or acquired during the incident. Through the investigation, it was discovered that certain files may have been accessed or acquired without authorization. Following this confirmation, Cardi's conducted a comprehensive review of the potentially affected data and on February 6, 2025, we determined that personal information belonging to certain individuals, including you, may have been impacted in connection with this incident. Cardi's then worked diligently to effectuate notification to potentially affected individuals. Please note that Cardi's has no evidence of the misuse or attempted misuse of any potentially accessed information.

What Information Was Involved. The information that may have been accessed in connection with this incident included your name and <<Variable Text 2: Data Elements>>.

What We Are Doing. As soon as Cardi's discovered this incident, Cardi's took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. Cardi's also notified the Federal Bureau of Investigation and will cooperate with any resulting investigation.

Although Cardi's has no evidence of the misuse of any information as a result of this incident, Cardi's is also offering you complimentary identity protection services through IDX, a leader in consumer identity protection. These services include <<12/24>> months of credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. 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. You can enroll in the IDX services by calling 1-877-819-4972 or by going to <https://app.idx.us/account-creation/protect> and using the following Enrollment Code: <<ENROLLMENT>>. Please note the deadline to enroll is June 10, 2025.

What You Can Do. Cardi's urges you to always take steps to avoid identity theft. Review your account statements, credit reports, and other data. Look for errors or suspicious items and report them right away. You can follow the recommendations on the enclosed "Steps You Can Take to Help Protect Your Information" for more information. Cardi's also encourages you to enroll in the complimentary monitoring services being offered to you through IDX by using the enrollment information provided.

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 1-877-819-4972 Monday through Friday from 9:00 am to 9:00 pm Eastern Time, excluding U.S. holidays.

Please know that Cardi's takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Cardi's Department Store Inc.

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. 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
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
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

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

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

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

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

Rhode Island Attorney General

150 South Main Street

Providence, RI 02903

www.riag.ri.gov

401-274-4400

There were 4,141 affected individuals
residing in Rhode Island.

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.