

Jennifer Miller

11/07/2018

Office of the Attorney General Gordon J. MacDonald
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301



Dear Attorney General MacDonald:

On June 6, 2018, Jennifer Miller Ltd., discovered that its system was compromised and as a result, the personal information of some of your state's residents may have been disclosed.

The details of the incident are as follows:

- Between February 1, 2018 and February 15, 2018 an executable file containing rogue code was inserted by unknown persons into the Jennifer Miller website's checkout page. The code was designed to download an executable file to the user's browser while on the Jennifer Miller Ltd. website and capture any information entered by a customer at the checkout page and send that data to a remote endpoint.
- The code was removed on July 15, 2018.
- From July 15, 2018 until October 17, 2018, two outside IT/Security consultancies, retained by Jennifer Miller, investigated the source of the breach and delivered a list of affected customers.
- We have determined that, between February 1, 2018 and July 15, 2018, the personal information of 1,050 individuals may have been compromised, including 2 residents of your state.
- The types of information that may have been compromised are: name, billing address for a credit card, telephone number, email address, and credit card information including card number, name on card, issuer, expiration date, and security code.

Upon learning of the unauthorized access, Jennifer Miller Ltd. took immediate measures to remove the code and to investigate and implement additional security measures to prevent a similar incident from occurring.

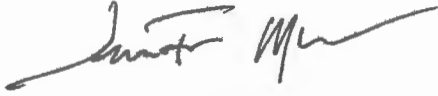
To address the incident, Jennifer Miller Ltd. is taking the following actions:

- We are implementing vigorous, whitelist-based access controls and password policies, as well as deploying a more robust intrusion detection system. All company technical and operational security is being audited and, where necessary, redesigned.
- We plan to notify all potentially affected customers, including 2 residents of your state, with an email by November 12, 2018.
- We will notify these affected residents about checking credit accounts for unauthorized activity, setting up credit alerts or freezes with the three major credit reporting agencies, and have provided a direct contact customer service line for affected customers to contact Jennifer Miller.

Additional details about the affected individuals are available upon request. A copy of a letter we are sending to residents to your state is enclosed. We have also provided notice to the FBI, and credit reporting agencies where ever required by state laws.

We regret that this situation occurred and will be working to reduce the risks of similar situations happening in the future. If you have any questions, please contact Amanda Terreros at amanda@jennifermillerjewelry.com.

Sincerely,



Jennifer Miller
President
Jennifer Miller Ltd.

STATE OF NJ
DEPT OF JUSTI
2018 NOV 13 AM 11:58

Jennifer Miller

11/12/2018

Re: NOTICE OF DATA BREACH

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information. We understand how important your privacy is, and we take the protection of your information very seriously. Our company is built on honesty, trust and transparency, which is why we are reaching out personally to let you know about what happened and what we're doing to address it.

What Happened?

On June 6, 2018, we learned that there was unauthorized access by electronic means to our data by a person or persons whose identities remain unknown. The unauthorized access occurred sometime between February 1, 2018 and February 15, 2018. The unauthorized access involved the insertion of rogue code into our checkout page. The code was designed to capture the name, billing address, phone number, and email address of certain customers, as well as their credit card information, and then send that data to a remote endpoint. Although we cannot be sure that any of your information was accessed or misappropriated, we are sending you this notice to make you aware of the situation and to provide you with other helpful information. The customer order dates for potentially compromised information are February 1, 2018, until July 15, 2018. We began an investigation on June 20, 2018, and fully resolved the unauthorized access on July 15, 2018. From that moment forward, we engaged two security consulting agencies to perform a full sweep of our infrastructure and to identify affected clients.

What Information Was Involved?

The information that was accessed without authorization could have included name, billing address for a credit card, telephone number, email address, and credit card information including card number, name on card, issuer, expiration date, and security code.

What Are We Doing?

We take our obligation to safeguard your personal information very seriously. Upon learning of the potential unauthorized access, we conducted an examination of the breach and employed technical measures to help ensure that further breaches do not occur in the future. We are implementing vigorous, whitelist-based access controls and password policies, as well as deploying a more robust intrusion detection system. All company technical and operational security has been audited and, where necessary, redesigned. We have also notified the FBI and we intend to fully cooperate with law enforcement if they determine that further investigation of the situation is warranted.

What You Can Do?

Given the nature of the information involved, we recommend that you:

Review and monitor your account statements and order a credit report. Under federal law, all citizens are entitled to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, call toll free at 1-877-322-8228 or visit www.annualcreditreport.com. If you wish to contact the credit reporting agencies directly, their contact information is as follows:

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-888-766-0008

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-680-7289

If you do become aware of any unauthorized use of your credit card, make sure to report that to your bank or card issuer immediately. You may also wish to report the unauthorized activity to the FBI, the federal Attorney General's Office, your local police and/or the Attorney General's Office for your state of residence.

You can contact the Federal Trade Commission to learn more about how to protect yourself in the event you become a victim of fraud or identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

You may also contact the Office of the Attorney General of the United States:

U.S. Department of Justice
950 Pennsylvania Avenue, NW Washington, D.C. 20530-0001
202-514-2000 www.justice.gov/contact-us

You may also consider placing a fraud alert or credit freeze on your credit file. A fraud alert helps protect you against an identity thief opening a new credit account in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The merchant can then take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any of the credit reporting agencies identified above. You may obtain more information about fraud alerts by contacting the Federal Trade Commission or the credit reporting agencies identified above. You may also consider placing a credit freeze, also known as a security freeze, on your file. A credit freeze, or security freeze, is designed to prevent potential creditors from accessing your credit file at the credit reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a freeze, which generally range from \$5-20. Unlike a fraud alert, you will need to separately place a freeze at each consumer reporting agency. For more information on freezes, you may contact either the FTC or the credit reporting agencies identified above. The instructions for placing a freeze differ from state to state, and the credit reporting agencies can provide more information on the requirements. These agencies may ask you to provide the following in connection with any such request: your full name with middle initial, social security number, date of birth, all addresses where you have lived for the past five years, a copy of government issued identification, and proof of your current residential address, such as a utility bill.

You may also have additional rights under the Fair Credit Reporting Act or other federal or state consumer protections laws.

Additional information for residents of Maryland, North Carolina, Rhode Island and Massachusetts:

- For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

• For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

• For residents of Rhode Island: You may contact the office of the Attorney General for The State of Rhode Island:

Rhode Island Attorney General's Office
150 South Main Street Providence, Rhode Island 02903, (401) 274-4400, www.riag.gov

Residents of Rhode Island have the right to file or obtain police reports. Fees may be applicable for services provided by credit reporting agencies.

• For residents of Massachusetts: You may contact the office of the Attorney General for The State of Massachusetts:

Massachusetts Office of the Attorney General, 1 Ashburton Place, Boston, MA 02108-1518 (617) 727-8400, www.mass.gov/ago/contact-us.html
Residents of Massachusetts have the right to obtain police reports.

For More Information

If you have further questions or concerns about this incident, you can contact Jennifer Miller at (347) 709-5879, Monday through Friday, 10:00 a.m. to 5:00 p.m. Eastern Time (excluding U.S. holidays). We at Jennifer Miller truly value you, and the trust that we have established with our customers. We want to reiterate that we take our obligation to protect your personal information very seriously. We've set up the above customer service line where our staff would love to talk to you about the situation. Please feel free to reach out with questions or additional information.

Very truly yours,



Jennifer Miller
President
Jennifer Miller Ltd.