



December 14, 2024

Dominik Cvitanovic
(504)-702-1710

Dominik.Cvitanovic@wilsonelser.com

Via Electronic Mail: Idtheft@oag.state.md.us

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

Re: Cybersecurity Incident Involving Maggie Sottero Designs, LLC (“Maggie Sottero Designs”)

Wilson Elser File No: 16516.2319

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Maggie Sottero Designs, LLC (“Maggie Sottero Designs”) an international bridal line, with respect to a recent cybersecurity incident that was first discovered by Maggie Sottero Designs on June 3, 2024 (hereinafter, the “Incident”). Maggie Sottero Designs takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve as notice of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that Maggie Sottero Designs has taken in response to the Incident. We have also included with this letter a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services. By providing this notice, Maggie Sottero Designs does not waive any rights or defenses regarding the applicability of the Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

1. Nature of the Incident

On June 3, 2024, Maggie Sottero Designs discovered suspicious activity in its network environment. Upon discovery of this incident, Maggie Sottero Designs promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Maggie Sottero Designs learned that an unauthorized actor accessed and acquired certain files and data stored within its network.

Upon learning this, Maggie Sottero Designs began a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand whose information was affected. On November 14, 2024, Maggie Sottero Designs identified persons whose sensitive data was included within the impacted data.

The following types of information may have been impacted: name and Social Security number.

2. Number of Maryland residents affected.

A total of 9 Maryland residents may have been potentially impacted by this incident. Notification letters to these individuals were mailed on December 12, 2024. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Maggie Sottero Designs remains committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future in addition to its already robust security controls. Upon discovery of the Incident, Maggie Sottero Designs moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially impacted individuals in an abundance of caution. Specifically, Maggie Sottero Designs engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Maggie Sottero Designs informed its law firm and began identifying the potentially impacted individuals in preparation for notice as soon as possible under the circumstances. Although Maggie Sottero Designs is not aware of any actual or attempted misuse of the personal information at issue, Maggie Sottero Designs offered 12-24 months of complimentary credit monitoring and identity theft restoration services.

4. Contact information

Maggie Sottero Designs remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Dominik.Cvitanovic@wilsonelser.com or 504-702-1710.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Dominik J. Cvitanovic, Esq.

EXHIBIT A



Maggie Sottero Designs, LLC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB09771



December 12, 2024

Notice of Data Breach

Dear _____ :

Maggie Sottero Designs, LLC (“Maggie Sottero Designs”) is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information. Please be assured that Maggie Sottero Designs takes the protection and proper use of your personal information very seriously.

What Happened?

On June 3, 2024, Maggie Sottero Designs discovered suspicious activity in its network environment. Upon discovery of this incident, Maggie Sottero Designs promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Maggie Sottero Designs learned that an unauthorized actor accessed certain files and data stored within our network.

Upon learning this, Maggie Sottero Designs began a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand whose information was affected. On November 14, 2024, Maggie Sottero Designs identified persons whose sensitive data was included within the impacted data. At this time, we have no evidence any of the information has been misused by a third party, but because information related to you was disclosed, we are notifying you so you can take proactive steps to protect your information.

What Information Was Involved?

The following data was acquired by a person not authorized to view them: name and Social Security number.

What We Are Doing?

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate an investigation, which included retaining a leading forensic investigation firm that assisted in conducting an investigation and confirming the security of our network environment. We also deployed additional monitoring tools and will continue to enhance the security of our systems. We take the protection and proper use of personal information very seriously.

As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident, and we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. 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.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

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: **0281AA6** . Please note that the code is case-sensitive and will need to be entered as it appears.

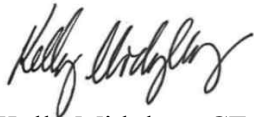
In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled you will have twelve (12) months of monitoring services. At the end of twelve (12) months, the services will be deactivated. 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

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help 1-800-405-6108 and supply the fraud specialist with the unique code listed above. The call center representatives have been fully versed in the incident and can answer questions or concerns you may have regarding the protection of your personal information.

At Maggie Sottero Designs, we take our responsibility to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

A handwritten signature in black ink, appearing to read "Kelly Midgley", written in a cursive style.

Kelly Midgley, CEO

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/ personal/credit-report-services/ credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. Instances of known or suspected identity theft should also be reported to law enforcement or to the Attorney General's office in your home jurisdiction. This notice has not been delayed by law enforcement.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

For Rhode Island residents, this data event involves 0 individuals in Rhode Island. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.