Our ref 1338831

Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6795

Nicholas.Jajko@kennedyslaw.com

August 3, 2026

Via Online Reporting
Nebraska Office of Attorney General
Consumer Affairs Response Team
2115 State Capitol
Lincoln, NE 68509

Re: Malin + Goetz – Notice of Data Event

Dear Sir or Madam:

We represent Malin + Goetz, a skincare and personal care product manufacturer based in New York, NY. We write in accordance with the Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, NEB. REV. STAT. § 87-801*, et seq.* (2016), to report a data event involving the personal information of nine (9) residents of the State of Nebraska. In making this submission, Malin + Goetz does not waive its rights or defenses regarding the applicability of Nebraska law or personal jurisdiction.

On June 15, 2026, Malin + Goetz received confirmation from a third-party service provider relating to a potential compromise on its e-commerce website which it was investigating. The investigation into the activity identified unauthorized code on its site that may have captured certain information entered on the checkout/payment page, at times between May 22, 2026 and June 10, 2026. Malin + Goetz took immediate action to analyze the transactions identified as at risk and determine which customers' information could have been captured to notify them accordingly. The information that may have been involved includes details entered during checkout, namely: customer name and payment card information.

On August 3, 2026, Malin + Goetz provided written notice of the event to potentially impacted individuals, including 9 Nebraska residents, via First Class U.S. mail. A sample copy of the notification letter is attached as Exhibit A.

Kennedys

Malin + Goetz's notice of this event includes a brief description of the incident and encouragement to remain vigilant for incidents of fraud or misuse, from any source, by reviewing payment card account statements. The notice also includes the recommendation to file a report with law enforcement, notify their state attorney general, and/or contact the Federal Trade Commission for more information. Malin + Goetz confirmed the personal information subject to unauthorized access (payment card information) and enclosed contact information for the major consumer reporting bureaus, state-specific regulators, and the number for a dedicated call center for obtaining resources to protect against fraud or misuse, should the individual find it appropriate to do so. Malin + Goetz is offering twelve (12) months of complimentary identity monitoring and restoration services through Experian which is focused on dark web monitoring of the payment card information, rather than credit monitoring as Malin + Goetz does not collect Social Security number as part of its account registration or guest payment process. Therefore, Social Security number was not involved in this incident.

Upon becoming aware of this incident, Malin + Goetz removed the unauthorized code and is working with specialists to actively monitor the situation, to help ensure no unauthorized code is reintroduced and to further strengthen its safeguards, Malin + Goetz informed the card brands and its payment processing partners to monitor for any evidence of fraud or misuse of the data. Malin + Goetz is also reviewing its existing security controls, policies, and procedures it has in place to remain resilient against future threats. Finally, Malin + Goetz is reporting the event to other regulators as required.

This notice provides your Office with all information necessary to comply with Nebraska law. Please do not hesitate to contact me directly if you have additional questions.

Respectfully,

Nicholas S. Jajko

Nicholas Jajko
Partner
for Kennedys

Exhibit A

MALIN+GOETZ
Return Mail Processing
PO Box 999
Suwanee, GA 30024

13 3 3097 ******************AUTO**All For SCF 112
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

August 3, 2026

Re: Notice of [Extra1]

Dear Sample A. Sample:

We are writing to inform you of a cyber incident that may have affected your personal information when using our website at Malin + Goetz.

What Happened? On June 15, 2026, we received confirmation from a third-party service provider relating to a potential compromise on our website which we were investigating. The investigation into the activity identified unauthorized code on our site that may have captured certain information entered on the checkout/payment page, at times between May 22, 2026 and June 10, 2026. We took immediate action to analyze the transactions identified as at risk and determine which customers' information could have been captured to notify them accordingly.

What Information Was Involved? The information that may have been involved includes details entered during checkout, such as your name and payment card information. This would also include any contact information (e.g. email address, billing/shipping address, home or mobile phone) you provided as part of the transaction. *We stress that Social Security number is never collected from you as part of our account registration or guest payment process.*

What We Are Doing. After becoming aware of this incident, we removed the unauthorized code and are working with specialists to actively monitor the situation, to help ensure no unauthorized code is reintroduced and to further strengthen our safeguards. We informed the card brands and our payment processing partners to monitor for any evidence of fraud or misuse of the data.

To help provide peace of mind, we are offering you complimentary access to Experian IdentityWorks[SM] for 12-months. Registration instructions, your unique code and additional product information are enclosed with this letter. Please note that Identity Restoration assistance is available to you for 12 months from the date of this letter, by calling the toll-free number (TFN) listed below, and does not require any activation of IdentityWorks[SM] on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

What You Can Do. It is prudent to remain vigilant for incidents of fraud or identity theft, from any source. You should review and monitor your payment card account statements for suspicious transactions, and report any such activity to the card issuer. You may enroll in the IdentityWorks^{SM} monitoring and take advantage of the Identity Restoration services being offered. Please also refer to the enclosed "Steps You Can Take to Help Protect Your Information", which contains additional resources you may take advantage of, should you find it appropriate to do so.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks^{SM} as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by October 31, 2026 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/identity
- Provide your activation code: ABCDEFGHI

For More Information. Protecting your personal information is extremely important to us and we are taking this matter very seriously If you have questions about the incident, the Experian IdentityWorks^{SM} product, need assistance with Identity Restoration, or would like an alternative to enrolling in Experian IdentityWorks^{SM} online, please contact Experian's customer care team by October 31, 2026 at 1-833-931-4203 Monday - Friday, 8 am - 8 pm Central Time (excluding major U.S. holidays). Please be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian. We thank you for your continued support.

Warm regards,
Malin + Goetz

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Identity Monitoring Information: To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 12 months. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

A credit card is not required for enrollment in Experian IdentityWorks^{SM}. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks^{SM}:

- Internet Surveillance: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE^{TM}: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts and Credit Reports: It is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, complete the Annual Credit Report Request Form on the Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. 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 below.

Credit Freeze Instructions: As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	**Experian**	**Equifax**
1-800-680-7289	1-888-397-3742	1-888-298-0045
www.transunion.com	www.experian.com	www.equifax.com
TransUnion Fraud Alert	**Experian Fraud Alert**	**Equifax Fraud Alert**
P.O. Box 2000	P.O. Box 9554	P.O. Box 105069
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30348-5069
TransUnion Credit Freeze	**Experian Credit Freeze**	**Equifax Credit Freeze**
P.O. Box 160	P.O. Box 9554	P.O. Box 105788
Woodlyn, PA 19094	Allen, TX 75013	Atlanta, GA 30348-5788

Additional Information: This notice has not been delayed by law enforcement. If you experience identity theft or fraud, you have the right to file a police report with your local law enforcement agency. When filing a report, you may be required to provide documentation showing that you have been a victim, and you are entitled to obtain a copy of the report for your records. If you discover suspicious activity on your credit reports or otherwise believe your information is being misused, you should promptly contact local law enforcement to file a report.

Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. A complaint may be filed with the FTC online at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Complaints submitted to the FTC are added to its Identity Theft Data Clearinghouse and made available to law enforcement for investigative purposes. The FTC also provides additional information about fraud alerts and security freezes.

For D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-727-3400, or https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New Mexico Residents, You also have rights under the federal Fair Credit Reporting Act (FCRA) and Identity Security Act, which governs the collection and use of information pertaining to you by consumer reporting agencies. These rights include the right to access the information in your file, dispute incomplete or inaccurate information, and request correction or deletion of inaccurate, incomplete, or unverifiable information. For more information about the FCRA and your rights, you may visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. or www.ftc.gov.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; or www.ncdoj.gov.

For *Rhode Island residents*, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or www.riag.ri.gov. There are 12 Rhode Island residents whose information was involved in this incident.