

Sean J. Bowen
Direct Dial: 248.402.4067
E-mail: sbowen@mcdonaldhopkins.com

RECEIVED

JUL 31 2026

CONSUMER PROTECTION

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

July 24, 2026

VIA U.S. MAIL

Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Hilldun Corporation – Incident Notification

To Whom It May Concern:

McDonald Hopkins, PLC represents Hilldun Corporation (“Hilldun”), located at 36 East 31st Street, 12th Floor, New York, NY 10016. Hilldun is providing notification, pursuant to N.H. Rev. Stat. § 359-C:19 *et seq.*, of an incident that may affect the security of personal information of two (2) New Hampshire residents. By providing this notice, Hilldun does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Hilldun learned that an unauthorized party accessed a limited number of systems within its network from on or about August 29, 2025, to on or about September 9, 2025. Upon learning of this issue, Hilldun immediately launched an investigation and contained and secured its internal environment. As part of the investigation, Hilldun worked very closely with third-party cybersecurity professionals experienced in responding to these types of incidents. Hilldun conducted an extensive forensic investigation and manual document review, and, through these efforts, determined that certain personal information was included within the impacted data accessed and/or acquired by the unauthorized party. Further, Hilldun worked to identify the list of potentially impacted individuals and the most recent contact information to notify these individuals. This process was completed on or about July 8, 2026. The personal information contained within the potentially impacted data, as it relates to New Hampshire residents, included first and last name and Social Security number.

Hilldun is not aware of any reports of identity fraud or improper use of the impacted information as a direct result of this incident. Nevertheless, out of an abundance of caution, Hilldun wanted to inform you (and the potentially affected residents) of the incident and to explain the steps that it is taking to help safeguard the potentially affected residents against identity fraud. Hilldun is providing the potentially affected residents with notification of this incident, commencing on or about July 24, 2026. The notice will be in substantially the same form as the letter attached hereto. Hilldun is also offering the potentially affected residents whose Social Security numbers were potentially impacted with complimentary credit-monitoring services. Hilldun is advising the potentially affected residents to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. Hilldun is also advising the potentially affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the potentially affected residents are being provided with contact information for the consumer reporting agencies and the Federal Trade Commission.

July 24, 2026
Page 2

Protecting the privacy of personal information is a top priority for Hildun. Hildun remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Hildun continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (248) 402-4067 or email me at sbowen@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink, appearing to be 'S. Bowen', with a long horizontal flourish extending to the right.

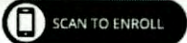
Sean J. Bowen

Encl. Individual Notice Letter.

EXHIBIT A



Membership Number: [REDACTED]
Enrollment Deadline: [REDACTED]
Coverage Length: [REDACTED] Months



Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Hilldun Corporation ("Hilldun"). We are writing with important information regarding a data security incident that may have impacted some of your information to provide you with information about the incident, tell you about the services that we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

Hilldun learned that an unauthorized party accessed a limited number of systems within its network from on or about August 29, 2025, to on or about September 9, 2025.

What Hilldun Is Doing.

Upon learning of this issue, we immediately launched an investigation and contained and secured the network. As part of the investigation, Hilldun worked very closely with third-party cybersecurity professionals experienced in responding to these types of incidents. The investigation determined the unauthorized party may have accessed or exfiltrated certain data from the network environment. After a thorough forensic investigation and manual document review, on July 8, 2026, Hilldun discovered that the potentially impacted data may have included a limited amount of your personal information.

What Information Was Involved?

The data involved contained your [REDACTED]

What You Can Do.

To date, we are not aware of any reports of identity fraud or identity theft or any other misuse of personal information as a direct result of this incident. Nevertheless, out of an abundance of caution, we wanted to make you aware of the incident. To protect you from the potential misuse of your information, we are offering you a complimentary [REDACTED]-month membership of Kroll's identity monitoring. For more information on identity theft prevention and the identity-monitoring product being offered to you, including instructions on how to activate your complimentary [REDACTED]-month membership, please see the additional information provided below in this letter in the section labeled, "Other Important Information."

This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information we maintain and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. If you have any further questions regarding this incident, please call the dedicated toll-free response line we have established to respond to questions at [REDACTED]. The response line is available Monday through Friday, [REDACTED] a.m. to [REDACTED] p.m. Eastern Time, excluding holidays.

Sincerely,

Hilldun Corporation

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED] Month Identity Monitoring.

To help protect your identity, we are offering complimentary access to Kroll's identity monitoring for [REDACTED] months. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit [REDACTED] to activate and take advantage of your identity monitoring services.

You have until [REDACTED] to activate your identity monitoring services.

Membership Number: [REDACTED]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

2. Placing a Fraud Alert on Your Credit File.

You may wish to consider placing an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any of the three (3) major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three (3) nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three (3) credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the identity monitoring service as described above, you will need to remove the freeze in order to sign up for the identity monitoring service. After you sign up for the identity monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one (1) free credit report every twelve (12) months from each of the above three (3) major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web 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. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.

Rhode Island Residents: You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. There was ■ Rhode Island resident impacted.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

* * *