



1900 M Street NW, Suite 250
Washington, DC 20036

Phone: (202) 296-3585
Website: www.zwillgen.com

Marci Rozen
(202) 706-5226
marci@zwillgen.com

December 17, 2025

Via Online Submission

Attorney General Mike Hilgers
Attorney General's Office
1445 K. Street, Room 2115
Lincoln, NE 68508

Re: Notice of Data Security Incident

Dear Attorney General Hilgers:

ZwillGen represents McIntosh Laboratory, Inc. ("McIntosh") in connection with the recent data security incident described below. The purpose of this letter is to notify you of the incident and provide you with a copy of the notice sent to impacted residents.

1. Nature of the Security Incident

On October 21, 2025, McIntosh detected suspicious activity and experienced a disruption of access to certain digital systems. In response, it took immediate steps to secure its network and engaged forensic experts to investigate. Based on the investigation, McIntosh determined that the perpetrator of the cyber-attack accessed and acquired certain data between October 17 and 19, 2025. Upon learning this, McIntosh conducted a prompt review of the impacted data in order to determine what information was potentially affected and identify contact information for affected individuals. On November 18, 2025, McIntosh determined that certain individuals' personal information was affected by this data security incident.

The affected information varies by individual but may include individuals' names and email addresses and account passwords for individuals' McIntosh online accounts.

2. Number of Nebraska Residents Affected

On December 17, 2025, McIntosh notified forty-four (44) Nebraska residents of this incident via first class U.S. mail. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

3. Steps Taken in Response to the Incident

As noted above, McIntosh and its forensic experts conducted a thorough investigation and promptly secured McIntosh's systems from this threat. Out of an abundance of caution, McIntosh has also provided individuals with information about steps they can take to protect their personal information.

4. Contact Information

McIntosh remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at 202-706-5226 or via email at marci@zwillgen.com.

Sincerely,

A handwritten signature in black ink that reads "Marci Rozen". The signature is fluid and cursive, with the first name "Marci" and last name "Rozen" clearly distinguishable.

Marci Rozen

Encls: Sample Consumer Notification Letter

cc: Melissa Maalouf, melissa@zwillgen.com
Jamie Elbert, jamie.elbert@zwillgen.com



Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>><<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<ZIP Code>>

December 17, 2025

Subject: Notice of Data <<Security Incident/Breach>>

Dear <<first name>> <<last name>>:

We are writing to inform you that McIntosh Laboratory, Inc. ("McIntosh") recently experienced a cyber attack that may have impacted some of your information. This letter explains the incident and steps you can take to help protect your personal information.

What Happened? On October 21, 2025, McIntosh detected suspicious activity and experienced a disruption of access to certain of our digital systems. In response, we took immediate steps to secure our network and engaged forensic experts to investigate. Based on the investigation, we have determined that the perpetrator of the cyber attack accessed and acquired certain data between October 17 and 19, 2025. Upon learning this, we conducted a prompt review of the impacted data in order to determine what information was potentially affected and identify contact information for affected individuals. On November 18, 2025, McIntosh determined that some of your personal information was potentially affected by this data security incident.

What Information Was Involved? The data that may have been acquired without authorization included your name and <<data elements>>.

What We Are Doing. As noted above, we and our forensic experts conducted a thorough investigation and promptly secured our systems from this threat. Out of an abundance of caution, we are also providing you with information about steps that you can take to help protect your personal information.

What You Can Do. You can follow the recommendations included with this letter to help protect your information.

For More Information. For more information about how you can protect your information, please review the resources on the following page. If you have questions regarding the incident, please call 1-833-772-7062, Monday through Friday, 9 a.m. to 9 p.m. Eastern Time, excluding holidays.

The security of your information is a top priority for McIntosh. We take your trust in us and this matter very seriously, and we regret any concern or inconvenience this incident may cause you.

Sincerely,

McIntosh Laboratory, Inc.
2 Chambers St.
Binghamton, NY 13903

Additional 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
1-833-799-5355
www.transunion.com/get-credit-report

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. For TransUnion: www.transunion.com/fraud-alerts.

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. For TransUnion: www.transunion.com/credit-freeze.

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
<https://oag.maryland.gov>
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

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

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](http://oag.dc.gov/consumer-protection)
202-442-9828

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

Rhode Island: McIntosh has notified <<total number of notices sent>> individuals of this incident.

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.