



Bert Bender, Esq.
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, Pennsylvania 19103
bbender@constangy.com
445-308-1588

VIA ONLINE SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509
Tel: 402-471-2683

August 15, 2025

Re: Notice of IMDataCenter Data Security Incident

Dear Attorney General Mike Hilgers:

Constangy, Brooks, Smith & Prophete LLP represents Apex Class Action, LLC in connection with the recent data security incident described in greater detail below. Apex Class Action provides class action administration and settlement services and this incident involved unauthorized access to the environment of IMDataCenter, Apex's address lookup vendor. By providing this notice, Apex does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

1. Nature of the Incident

Apex was alerted to possible unauthorized access to IMDataCenter's environment on July 14, 2025. Apex immediately investigated, including requesting additional details from IMDataCenter to assess the scope of risk to any information. As a result of the investigation, Apex determined on July 25, 2025 that certain data was accessed without authorization from IMDataCenter's network on July 8, 2025. Apex then undertook a comprehensive review of the data to identify individuals whose information was accessed. Apex has no evidence any of the information was used to commit identify theft or fraud.

2. Number of Affected Residents & Information Involved

The incident involved personal information for approximately one (1) Nebraska resident. The information involved in the incident for the affected Nebraska resident may have included name as well as their address, phone number, and Social Security Number.

3. Notification to Affected Individual(s)

On or about August 15, 2025, Apex mailed notification letters. Apex has no evidence of fraudulent misuse, or attempted misuse, of the potentially impacted information. However, the letter provides steps individuals can take to protect their personal information. The notification letter also offers

13270251v3

August 15, 2025

Page 2

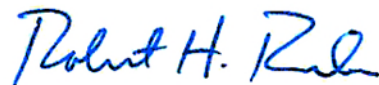
individuals the opportunity to enroll in complimentary identity protection services, including credit monitoring, and identity remediation services, as well as a phone number to call, should any individual have questions about the incident. A sample notification letter sent to the impacted individual(s) is included with this correspondence.

4. Steps Taken Relating to the Incident

Upon discovering the event, Apex moved quickly to investigate the activity and to identify necessary information so it could notify potentially affected individuals. Apex is also reviewing its vendor engagement engagements and no longer works with IMDataCenter after this incident.

If you have any questions or need additional information, please contact us at 445-308-1588 or bbender@constangy.com.

Sincerely,

A handwritten signature in blue ink that reads "Robert H. Bender". The signature is fluid and cursive, with the first name "Robert" and last name "Bender" clearly legible.

Bert Bender
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter

Apex Class Action, LLC
P.O. Box 54668
Irvine, CA 92619

<<First Name>> <<Last Name>>
<<Address1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

<<Date: August 15, 2025>>

Subject: Notice of IMDataCenter Data [Variable Text 1: Event / Breach]

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a recent incident which included your personal information. Apex Class Action provides class action administration services and we take the privacy and security of all information provided to us very seriously. This recent incident involved unauthorized access to our address lookup vendor IMDataCenter's environment and did not involve unauthorized access to our network. This letter contains information regarding the incident and steps that you can take to help protect your information, including enrolling in complimentary identity protection services.

What Happened. On July 25, 2025, we learned that some of your personal information was involved in this incident. We were first alerted on July 14, 2025 of possible unauthorized access to IMDataCenter's environment and immediately investigated. Our investigation discovered that data was accessed from IMDataCenter's environment without authorization. We then undertook a comprehensive review of the data to determine what information was involved and determined that some of your information was included. We received this information through the administration of a class action, and/or PAGA, matter in which you were involved.

What Information Was Involved. The information may have included your Social Security number. Please note, we have no evidence any of this information was used to commit identity theft or fraud.

What We Are Doing. As soon as we discovered this incident, we immediately investigated to understand the scope of risk to information. We are reviewing policies and processes to confirm the security of information entrusted to us, including updating our vendor engagement processes. We have not used IMDataCenter for any services since the third quarter of 2024.

We are also offering you complimentary identity protection services through Transunion, a leader in consumer identity protection. These services include 24 months of 3 bureau credit monitoring, credit reporting, dark web monitoring, proactive fraud assistance, and identity theft and fraud solution services. The deadline to enroll in these services is January 15, 2026. Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services. Please use your unique Membership Number / Enrollment Code: <<Number/Code>>

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complementary services offered to you through Transunion by using the enrollment code provided above.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance with the complimentary services, please call 1-800-888-4213 Monday through Friday from [Insert Times] 9 a.m. to 9 p.m. Eastern Time (ET). If you have questions regarding the incident, please feel free to reach out to us at 1-800-355-0700, Monday through Friday from 8:00 a.m. to 5:00 p.m. Pacific Standard Time (PST).

Sincerely,

Apex Class Action, LLC

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.

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 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

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.

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.

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
www.marylandattorneygeneral.gov/Pages/CPD
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

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

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
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

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

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify the identity of the filer for an electronic or paper tax return. You can learn more and obtain an IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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.