



Lauren Godfrey, Partner
Cybersecurity & Data Privacy Team
322 North Shore Drive, Building 1B
Suite 200
Pittsburgh, PA 15212
lgodfrey@constangy.com
Telephone: 412.870.4129

October 7, 2025

VIA ONLINE SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Protection Division
2115 State Capital
Lincoln, NE 68509
Email: ago.consumer@nebraska.gov

Re: Notice of Data Security Incident - Supplement

Dear Attorney General Hilgers:

Constangy, Brooks, Smith & Prophete, LLP represents Decisely in conjunction with their response to a recent information security incident discussed below. Decisely is headquartered in Alpharetta, Georgia, and provides benefits brokerage and human resources services, specializing in integrated technology solutions for small businesses. The purpose of this letter is to notify you of the incident in accordance with Nebraska's data breach notification statute.

This is a supplemental notification to Decisely's prior notices on June 13, 2025 and July 21, 2025. Decisely is providing this supplemental notice on its own behalf as well as on behalf of certain current or former partner organizations to which Decisely is a service provider.

1. Nature of the Security Incident

As previously advised, on or about May 29, 2025, Decisely learned that some personal information related to one of Decisely's partners, MetLife, may have been involved in a data security incident Decisely experienced. The incident began on December 17, 2024, when Decisely discovered suspicious activity related to its cloud storage platform. Decisely then promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. Decisely also engaged cybersecurity experts to conduct an investigation into what happened and to assist with determining whether personal information was accessed or acquired without authorization. The investigation determined that some data may have been acquired on December 16, 2024.

Decisely then completed a comprehensive analysis of the data potentially involved to identify what personal information was impacted and to whom it belonged. Decisely identified data subjects related to data owner MetLife and worked with them so they could validate and confirm this data. That process was completed on May 29, 2025, and Decisely mailed a first wave of notices on behalf of MetLife on June 13, 2025. Decisely issued two additional waves of letters on July 15 and 18, 2025, on behalf of MetLife.

On August 18, 2025, Decisely provided notification to its remaining partner organizations and provided them with access to a list of data subjects whose information was potentially involved. Decisely worked with them to effectuate notice. On September 30, 2025, Decisely issued a fourth wave of notices to consumers on behalf of 225 partner organizations.

The potentially affected information may have included individuals' name, dates of birth, address, phone number, Social Security number, email address, passport number, bank account number and digital signature.

2. Number of Nebraska Residents Affected

On September 30, 2025, Decisely notified approximately 157 Nebraska residents within the potentially affected population, via USPS First-Class Mail. A total of 823 Nebraska residents have been notified of this incident to date. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as Decisely learned of the unusual network activity, it took steps to secure its systems and launched an investigation to learn more about what happened and what information could have been affected. Decisely is providing those whose Social Security number was involved with identity protection services through Kroll for 12 months. In addition, Decisely has established a toll-free call center through Kroll to answer questions about the incident and address related concerns.

Additionally, Decisely is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Decisely is also providing individuals with information on how to place a fraud alert and security freeze on their credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Finally, Decisely notified the Federal Bureau of Investigation, and Decisely will cooperate in any efforts to hold the perpetrators accountable.

Attorney General Mike Hilgers

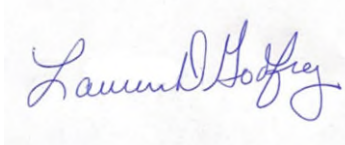
October 7, 2025

Page 3

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at Lgodfrey@constangy.com or 412.870.4129.

Sincerely,

A handwritten signature in blue ink, reading "Lauren Godfrey". The signature is fluid and cursive, with the first name "Lauren" and last name "Godfrey" clearly distinguishable.

Lauren Godfrey
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter
List of Partner Organizations

cc: Suzie Allen, Associate Attorney, Constangy Cyber Team

List of Partner Organizations

- 1638 _ Chick-fil-A San Marcos, and Escondido
- 5231 _ Chick-fil-A Leland Town Center
- 5852 _ Chick-fil-A Waterloo FSU
- 6348 _ Chick-fil-A Parma
- 6507 _ Franchise Management Investors LLC
- 7463 _ Medallion Dental Laboratory Inc
- 9050 _ Dingman's Collision Center, Inc.
- 9269 _ Great Lakes Management Group



<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



<<Date>> (Format: Month Day, Year)

<<b2b_text_1 (Re: [Variable Header])>>

Dear <<first_name>> <<last_name>>:

Decisely Insurance Services, LLC (“Decisely”) is writing to notify you of a data security incident which may have involved your personal information. Decisely provides insurance benefits brokerage and human resources administration, compliance, payroll and retirement services to employers. We held limited information related to you due to our relationship with <<b2b_text_2 (Data Owner Name)>>. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information, including activating the complimentary identity monitoring services we are making available to you.

What Happened? Recently, we learned that some of your personal information may have been involved in a data security incident we experienced. The incident began on December 17, 2024, when we discovered suspicious activity related to our cloud storage platform. We promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. We engaged cybersecurity experts to conduct an investigation into what happened and to assist us with determining whether personal information was accessed or acquired without authorization. The investigation determined that some data may have been acquired on December 16, 2024. We then completed a comprehensive analysis of the data potentially involved to identify what information was impacted and to whom it belonged. We notified <<b2b_text_2 (Data Owner Name)>> and worked with them so they could validate and confirm this data. We then coordinated with that entity to issue this notification to you.

Please note that we have no evidence of fraudulent misuse, or attempted misuse, of the potentially impacted information. However, you should remain vigilant by reviewing account statements and monitoring free credit reports.

What Information was Involved? The information that may have been involved in this incident includes your name as well as <<b2b_text_3 (Data Elements)>>.

What Are We Doing? As soon as the incident was discovered, we took the steps discussed above. In addition, we reported the incident to law enforcement. To reduce the likelihood of a similar incident occurring in the future, we implemented additional measures to enhance the security of the network.

We are also providing you with access to <<Monitoring Term Length (Months)>> months of identity monitoring services through Kroll.

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

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.

What You Can Do. You can follow the recommendations included with this letter to help protect your information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately. In addition, you can contact Kroll representatives who will work on your behalf to help resolve issues you may experience as a result of this incident.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call (866) 461-3640 toll-free Monday through Friday from 8:00 am – 5:30 pm Central Time (excluding major U.S. holidays).

We take your trust in Decisely and this matter very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Decisely Insurance Services, LLC
12735 Morris Road, Suite 350
Alpharetta, Georgia 30004

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.

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](http://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](http://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
[\[#\] of Rhode Island residents](#)

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

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



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data, for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.