

Notice of Data Security Incident

Decisely learned of a data security incident that may have involved personal and/or protected health information of certain individuals. We have taken steps to notify individuals for whom we were able to obtain a mailing address.

Recently, we learned that some personal and/or protected health 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 personal and/or protected health information was impacted and to whom it belonged. We also notified associated owners of the data and worked with them to determine contact information necessary to provide this notice of what happened.

Please note that we have no evidence of fraudulent misuse, or attempted misuse, of the potentially impacted information.

Based on the review of potentially impacted data, the following information may have been affected as a result of the incident: names, dates of birth, phone number, passport number, digital signature, and/or Social Security numbers. Individuals began receiving notification of this incident on June 13, 2025. Decisely is offering individuals whose Social Security number was involved access to credit monitoring and fully managed identity theft recovery services through Kroll.

We have established a toll-free call center to answer questions about the incident and address related concerns. Call center representatives are available Monday through Friday from 8:00 am to 5:30 pm Central Time, and can be reached at (866) 461-3640.

As soon as we discovered the incident, we took the steps discussed above to investigate the incident and to notify appropriate individuals. To reduce the likelihood of a similar incident occurring in the future, we also implemented additional measures to enhance the security of our network environment. The privacy and protection of personal and protected health information is a top priority for Decisely, and we appreciate everyone's patience as we respond to this incident.

We are providing the following information to help those wanting to know more about steps they can take to protect themselves and their 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 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.

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.