



Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
aweaver@constangy.com
Mobile: 941.875.5335

May 15, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: Idtheft@oag.state.md.us

RE: Notice of Data Security Incident

Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Davis, Brown & Company in connection with a recent data security incident described below. Davis, Brown & Company is notifying affected individuals of the incident. The purpose of this letter is to provide formal notice to your office pursuant to Md. Code Ann., Comm. Law § 14-3504.

I. Nature of the Security Incident

On February 15, 2024, Davis, Brown & Company confirmed claims that an unauthorized actor gained access to its former cloud storage application, SmartVault, and downloaded data therefrom. Davis, Brown & Company previously utilized SmartVault to store and transfer documents to and from its clients. After learning of this issue, Davis, Brown & Company promptly worked to review the potentially affected information and identify contact information needed to provide notice to all potentially affected individuals, which process concluded on May 1, 2024.

SmartVault, like most data storage applications, is a third-party web-based system. There is no evidence of access to Davis, Brown & Company internal network systems. Davis, Brown & Company is not aware of any publication or exposure of the potentially affected data.

II. Number of Maryland Residents Affected

Based on Davis, Brown & Company's investigation, information for approximately three (3) Maryland residents may have been involved in this issue. Notification letters were sent to these individuals via first class U.S. mail on May 9, 2024. A sample copy of that notification letter is enclosed.

III. Actions Taken in Response to the Incident

As soon as Davis, Brown & Company discovered the incident, it launched an investigation and notified the IRS. Davis, Brown & Company has not been made aware of any fraud related to this

Alabama Arkansas California Colorado District of Columbia Florida Georgia Illinois
Indiana Maryland Massachusetts Minnesota Missouri New Jersey New York
North Carolina Oregon Pennsylvania South Carolina Tennessee Texas Virginia Washington
11116673v1

Attorney General Anthony G. Brown
May 15, 2024

Constangy, Brooks, Smith & Prophete, LLP

issue. Davis, Brown & Company then worked diligently to determine what personal information may have been affected, the individuals to whom the information pertained, and the addresses for those individuals to provide appropriate notification.

Davis, Brown & Company has established a toll-free call center through IDX to answer questions about the incident and address related concerns. In addition, Davis, Brown & Company is offering Maryland residents 12 months of complimentary credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

IV. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 215.770.4234 or aweaver@constangy.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Aubrey Weaver', with a stylized, flowing script.

Aubrey Weaver
Partner, Cybersecurity & Data Privacy Team



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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

May 8, 2024

Re: Notice of Data <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident that may have affected your personal information. At Davis, Brown & Company, PLLC ("Davis, Brown & Company"), we are committed to maintaining our clients' trust and demonstrating our commitment to the privacy and security of all information in our possession. That is why we are writing to notify you of this incident, to offer you complimentary credit monitoring and identity protection services, and to inform you about steps that can be taken to help safeguard your information.

What Happened: On February 15, 2024, Davis, Brown & Company confirmed claims that an unauthorized actor gained access to our former cloud storage application, SmartVault, and downloaded data therefrom. Davis, Brown & Company previously utilized SmartVault to store and transfer documents to and from its clients. In May 2023, Davis, Brown & Company began migrating its cloud storage to Qount; however, certain legacy information was contained in SmartVault while completing the migration. SmartVault, like most data storage applications, is a third-party web-based system. There is no evidence of access to Davis, Brown & Company internal network systems, and we are not aware of any publication or exposure of the potentially affected data.

After learning of this issue, we promptly worked to review the potentially affected information and identify contact information needed to provide notice, which process concluded on May 1, 2024.

What Information Was Involved: The potentially affected information includes the information reflected on your tax return and related documents, including your name, date of birth, Social Security number, and/or financial account number. If you had dependents listed on your tax return, their Social Security number(s) could have also been involved.

What We Are Doing: Upon discovering this matter, we immediately notified the IRS in an effort to protect all clients' information, and have not been made aware of any fraud related to this issue. We have also reported this incident to the Federal Bureau of Investigation and will cooperate with any resulting investigation into this matter.

In addition, we are offering you complimentary credit monitoring and identity protection services through IDX, a data breach and recovery services expert. IDX services include the following: <<Membership Offering Length>> of credit¹ and CyberScan monitoring, fully managed identity recovery services, and \$1 million insurance reimbursement policy, and fully managed identity theft and protection services.

¹ Credit monitoring is available only for adult enrollees.

We have also arranged to offer IDX identity protection services to all dependents whose information may have been involved. If you had dependents listed on your tax return, they can be enrolled in the IDX services using the code(s) listed below.

Minor Dependent Enrollment Code: ZD4KU6AUQ
Adult Dependent Enrollment Code: ZD46QUBXF

You can enroll in the free IDX services by calling **TFN** or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code(s) provided above. IDX representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please note the deadline to enroll is August 8, 2024.

What You Can Do: We encourage you to activate your complimentary services using the enrollment code(s) provided in this letter. We also recommend that you review the guidance included with this letter about how to protect your personal information.

For More Information: If you have questions or need assistance, please call **TFN**, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Davis, Brown & Company takes your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

Davis, Brown & Company PLLC

Davis, Brown & Company, PLLC
100 Country Club Drive, Suite 202
Hendersonville, TN 37075

Steps You Can Take to 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 (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 <http://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 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
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 <http://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
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.