

Notice of Data Security Incident

Notice of Data Security Incident

Revised February 1, 2024

January 9, 2024 – Burr & Forman LLP (“Burr & Forman”), a law firm based in Birmingham, Alabama, recently experienced a data security incident that impacted data belonging to some of its clients. The incident did not impact computer systems belonging to its clients in any way. On January 9, 2024, Burr & Forman began notifying impacted individuals of this incident and provided resources to assist them.

On October 23, 2023, Burr & Forman became aware of anomalous activity on one of the laptops in its network. Burr & Forman activated its Incident Response Plan to initiate an investigation of the incident. Burr & Forman engaged cybersecurity experts to assist with the investigative process. The investigation indicates that an unauthorized actor gained access to and acquired certain documents and information from Burr & Forman’s systems. On or about November 10, 2023, the investigation determined that some personal information was contained within the affected data. Burr & Forman notified Oceans Healthcare and Summit BHC of this incident on November 10, 2023. Since that time, Burr & Forman has been coordinating with Oceans Healthcare and Summit BHC to provide notice to affected individuals. The incident did not affect computer systems belonging to Oceans Healthcare or Summit BHC.

The affected information included individuals’ names as well as Social Security number, medical coding information with dates and descriptions, and insurance information.

Burr & Forman began sending notification letters to impacted individuals with identifiable address information on January 9, 2024. The letters include information about this incident and about steps that impacted individuals can take to monitor and help protect their information. Contact information for some affected individuals was not identified and, as such, this website posting is intended to serve as substitute notice to those individuals.

Burr & Forman has established a toll-free call center to answer questions about the incident and to address related concerns. The call center is available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time and can be reached at (888) 774-8132. The privacy and protection of all information is a top priority for Burr & Forman. Burr & Forman deeply regrets any inconvenience or concern this incident may cause.

Notice of Data Security Incident

The following information is provided to help individuals wanting more information about steps that they can take to protect themselves:

What steps can I take to protect my information?

- If you detect suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also report any fraudulent activity or any suspected incidents of identity theft to law enforcement.
- You may obtain a copy of your credit report at no cost from each of the three nationwide credit reporting agencies. To do so, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies appears at the bottom of this page.
- Notify your financial institution immediately of any unauthorized transactions made, or new accounts opened, in your name.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

What should I do to protect myself from payment card/credit card fraud?

We suggest that you review your debit and credit card statements carefully in order to identify any unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the issuer of the debit or credit card immediately.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. To do so, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies is included in the notification letter and is also listed at the bottom of this page.

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is listed below.

Contact information for the three nationwide credit reporting agencies is as follows:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Notice of Data Security Incident

Experian
PO Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

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

How do I put a security freeze on my account?

You also have the right to put a security freeze on your credit file at no cost. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, placing 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.

Do I have any other rights regarding my credit file?

You also have rights under the Fair Credit Reporting Act (“FCRA”) including 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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

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, and

Notice of Data Security Incident

www.ftc.gov/idtheft

1-877-438-4338

Maryland Attorney General

200 St. Paul Place

Baltimore, MD 21202

oag.state.md.us

1-888-743-0023

New York Attorney General

Bureau of Internet and Technology

Resources

28 Liberty Street

New York, NY 10005

1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center

Raleigh, NC 27699

www.ncdoj.gov

1-877-566-7226

Notice of Data Security Incident

Rhode Island Attorney General

150 South Main Street

Providence, RI 02903

<http://www.riag.ri.gov>

1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW

Washington, DC 20001

oag.dc.gov

1-202-727-3400