



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

August 5, 2024

VIA E-MAIL

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 Event

To Whom It May Concern:

We represent David S. Brown Enterprises, Ltd. (“DSB”) located at 100 Painters Mill Road, Owings Mills, MD 21117, and are writing to notify your office of an incident that may affect the security of certain personal information relating to three thousand nine hundred and ninety-eight (3,998) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, DSB does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 7, 2023, DSB discovered suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that there was unauthorized access to DSB’s environment between March 6, 2023, and March 7, 2023. The investigation also determined that an unauthorized actor had the ability to access certain information stored on the network during this period of time. Therefore, DSB engaged a third-party specialist to conduct a comprehensive review of the data potentially affected to assess whether it contained any sensitive information. On March 11, 2024, this review was completed and DSB began working to identify address information for these individuals. On July 31, 2024, DSB confirmed address information for the impacted individuals.

The information that could have been subject to unauthorized access for Maryland residents includes name, Social Security number, driver's license number or state identification number, financial account information, passport number, username with password or access code, and medical or health insurance information.

Notice to Maryland Residents

On or about August 5, 2024, DSB provided written notice of this incident to three thousand nine hundred and ninety-eight (3,998) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, DSB moved quickly to investigate and respond to the incident, assess the security of DSB systems, and identify potentially affected individuals. DSB is also working to implement additional safeguards and training to its employees. DSB is providing access to credit monitoring services for twelve (12) months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, DSB is providing impacted individuals with guidance on how to better protect against identity theft and fraud. DSB is providing individuals with information on how to place a fraud alert and security freeze on one's 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/crm
Enclosure

EXHIBIT A



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Notice of Data <<Variable Data 2>>

Dear <<Full Name>>:

David S. Brown Enterprises, Ltd. ("DSB") writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your information, should you feel it appropriate to do so.

What Happened? On or about March 7, 2023, DSB discovered suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation which was conducted with the assistance of third-party forensic specialists determined that there was unauthorized access to our environment between March 6, 2023 and March 7, 2023. The investigation also determined that an unauthorized actor had the ability to access certain information stored on the network during this period of time. Therefore, DSB undertook a comprehensive review of the data potentially affected to assess whether it contained any sensitive information. On March 11, 2024, DSB completed this review and determined the data contained certain information related to you. On July 31, 2024, we confirmed address information for the impacted individuals.

What Information Was Involved? DSB determined the type of information potentially impacted by this incident includes your <<Data Elements>>.

What We Are Doing. DSB takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we immediately commenced an investigation to confirm the nature and scope of the incident. We also took steps to implement additional safeguards and review our policies and procedures relating to data privacy and security.

DSB is providing you with access to <<CM Duration>> months of credit monitoring and identity protection services through Epiq at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information*. You can also enroll to receive the complimentary credit monitoring and identity protection services through Epiq. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions, or need assistance, please call 888-244-3141, Monday through Friday 9 am to 9 pm ET (excluding holidays). You may also write to DSB at 100 Painters Mill Road, Owings Mills, MD 21117.

DSB takes the privacy and security of the information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

David S. Brown Enterprises, Ltd.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Identity Monitoring

1. Visit app.identitydefense.com/enrollment/activate/dsb
2. Enter your unique Activation Code: <<Activation Code>>
3. Click 'Redeem Code'
4. Follow the prompts to create your account

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you

make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.Experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<RI Count>> Rhode Island residents impacted by this incident.