



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 27, 2022

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

Dear Sir or Madam:

We represent V2 Logistics Corp. ("V2") located at 15 Grumman Road West, Suite 1500, Bethpage, New York 11714, and write to notify your office of an event that may affect the security of certain personal information relating to approximately fourteen (14) Maryland residents. This notice may be supplemented if significant new facts are learned subsequent to its submission. By providing this notice, V2 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 June 17, 2022, V2 identified that certain company computer systems had become encrypted due to a sophisticated cyber-attack by an unknown actor. V2 immediately launched a comprehensive investigation to determine the nature and scope of the event and worked to quickly secure its systems, restore access to its systems to continue to operate without disruption, and determine whether there was any impact to information maintained on its systems. V2 also promptly reported this event to federal law enforcement. Through the investigation, V2 determined that the unknown actor gained access to certain systems between June 13, 2022, and July 7, 2022 and certain data on those systems was viewed or downloaded.

Upon completion of the investigation, V2 conducted a thorough review of information stored on the impacted systems to determine what information was affected and to whom the information related. V2 then undertook a manual review of its records to confirm the identities and contact information for potentially affected individuals to issue notifications. V2 recently completed this review.

The information that could have been subject to unauthorized access for Maryland residents includes name, driver's license number, and passport number.

Notice to Maryland Residents

On October 27, 2022, V2 provided written notice of this event to potentially affected individuals, including approximately fourteen (14) Maryland residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, V2 moved quickly to investigate, assess the security of its systems, and identify potentially affected individuals. V2 also implemented additional technical safeguards and training to its employees. Further, V2 is providing access to credit monitoring and identity restoration services for twelve (12) months, through Experian, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, V2 is providing impacted individuals with guidance on how to better protect against identity theft and fraud. V2 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.

V2 is providing written notice of this event to other appropriate state regulators, and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Sica', with a stylized flourish at the end.

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/jlm
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 27, 2022

i5139-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 GENERAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



[Variable Text]

Dear Sample A. Sample:

V2 Logistics Corp. (“V2”) is writing to notify you of an event that may involve some of your information. Although there is no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response to it, and additional measures you can take to protect your information, should you feel it appropriate to do so.

What Happened? On June 17, 2022, V2 identified that certain of our computer systems had become encrypted due to a sophisticated cyber-attack by an unknown actor. We immediately launched an extensive investigation to determine the nature and scope of the event and worked quickly to: (1) secure our systems; (2) restore access to our systems to continue to operate without disruption; and (3) investigate what happened and whether this resulted in any impact to information housed on our systems by the unknown actor. We also promptly reported this event to federal law enforcement. Through the investigation, we determined that the unknown actor gained access to certain systems between June 13, 2022 and July 7, 2022 and certain data on those systems was viewed or downloaded.

We then conducted a comprehensive review of information stored on the impacted systems to determine what information was affected and to whom the information related. We then undertook a manual review of our records to determine the identities and contact information for potentially affected individuals to issue notifications. We recently completed our review.

What Information Was Involved? Our investigation determined that at the time of the event, your name and [Data Elements] were stored within the impacted systems.

What We Are Doing. We take this event and information security seriously. Upon learning of the activity, we immediately took steps to further secure our systems and investigate the event. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional administrative and technical safeguards to further enhance our information security posture.

As an additional precaution, V2 is offering you access to [##] complimentary credit monitoring and identity restoration services through Experian. Details of this offer and instructions on how to activate these services are enclosed with this letter.



What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed document, *Steps You Can Take to Help Protect Your Information*, which contains information on what you can do to safeguard against possible misuse of your information. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. If you have additional questions, please contact our toll-free dedicated assistance line at 1-833-256-3157. This toll-free line is available Monday through Friday from 09:00 am ET to 11:00 pm ET and Saturday through Sunday from 11:00 am ET to 08:00 pm ET (excluding U.S. holidays). You may also write to V2 at 15 Grumman Road West, Suite 1500, Bethpage, NY 11714.

Sincerely,

V2 Logistics Corp.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [##] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [##] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [##]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below

- Ensure that you **enroll by** January 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-256-3157 by January 31, 2023. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [##]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.



- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. 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 one-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, however, 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 credit 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	888-397-3742	833-395-6938
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. 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

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 event. There are 6 Rhode Island residents impacted by this event.



