



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

March 13, 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 Remotely Piloted Solutions, LLC d/b/a RPS Defense (“RPS Defense”) located at 15305 Dallas Parkway, 12th Floor, Suite 1185, Addison, Texas 75001, and write to notify your office of an event that may affect the security of certain personal information relating to approximately one (1) Maryland resident. By providing this notice, RPS Defense 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 September 21, 2022, RPS Defense identified suspicious activity on its network. RPS Defense immediately took steps to secure its systems and launched an investigation to determine the nature and scope of the activity. It is RPS Defense’s understanding the event originated from a vulnerability in commonly used vendor software, despite the implementation of reasonable security and compliance measures at the time of the event. RPS promptly reported the event to its primary federal regulatory authorities and federal law enforcement. The investigation determined that certain RPS Defense computer systems were accessed by an unknown actor on August 30, 2022 and September 22, 2022, and certain information contained within those systems was viewed or downloaded by an unknown actor. RPS Defense therefore undertook a comprehensive and time-intensive review of the potentially impacted records to determine what information was potentially impacted, to whom the information related, and to identify contact information for purposes of providing notifications. That review recently concluded.

The information that could have been subject to unauthorized access for the Maryland resident includes: name and passport number.

Notice to the Maryland Resident

On or about March 13, 2024, RPS Defense provided written notice of this event to potentially affected individuals, including approximately one (1) Maryland resident. 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 identifying the event, RPS Defense moved quickly to investigate and respond, notify its primary federal regulatory authorities, assess the security of its systems, and identify potentially affected individuals. RPS is also working to implement additional safeguards and training to its employees. RPS Defense also further enhanced their cybersecurity measures, building upon the robust systems they had in place at the time of the event. RPS Defense is providing access to credit monitoring 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, RPS Defense is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud. RPS Defense 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.

RPS Defense is providing written notice of this event to appropriate state regulators, as necessary, and to the three major credit 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,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/jrm
Enclosure

EXHIBIT A



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

March 13, 2024

K9970-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L02 NARROW
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Dear Sample A. Sample:

Remotely Piloted Solutions, LLC d/b/a RPS Defense (“RPS Defense”) writes to inform you of an event that may affect the confidentiality of information related to you. This letter provides information about the event, our response, and resources available to you to help protect your information, should you determine it is appropriate to do so.

What Happened? RPS Defense identified suspicious activity on our network, at which point we immediately took steps to secure our systems and launched an investigation to determine the nature and scope of the activity. It is our understanding the event originated from a vulnerability in commonly used vendor software, despite the implementation of reasonable security and compliance measures at the time of the event. Our investigation determined that certain RPS Defense computer systems were accessed by an unknown actor, and certain information contained within those systems was viewed or downloaded by an unknown actor. We therefore undertook a comprehensive and time-intensive review of the potentially impacted records to determine what information was potentially impacted, to whom the information related, and to identify contact information for purposes of providing notifications. That review recently concluded.

What Information Was Involved? The types of information that may have been subject to unauthorized access includes your name and [Data Elements].

What We Are Doing. We take this event and the security of personal information in our care seriously. Upon learning of this event, we worked to investigate and respond, assess the security of our network, and notify potentially affected individuals. As part of our ongoing commitment to information security, we reviewed our existing policies and procedures and enhanced certain administrative and technical controls to reduce the likelihood of a similar future event. We have also further enhanced our cybersecurity measures, building upon the robust systems we had in place at the time of the event. As an added precaution, we are also offering you complimentary credit monitoring and identity restoration services for 12 months through Experian.

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. We also recommend you review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. In addition, you may enroll in the complimentary credit monitoring services available to you. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, please contact our dedicated assistance line at 1-833-918-8226, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific (excluding U.S. holidays). You may also write to us at RPS Defense, 15305 Dallas Parkway, 12th Floor, Suite 1185, Addison, Texas 75001.

Sincerely,

RPS Defense

B109464

0000002



K9970-L02

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 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 12 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 12-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 June 30, 2024** (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 1-833-918-8226 by June 30, 2024. Be prepared to provide engagement number B109464 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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 ExtendCARETM:** 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 fund transfers.

* 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. Consumers should be aware, however, that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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
1-888-298-0045	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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Ave. N.W., Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. To file a report with law enforcement for identity theft, consumers will likely need to provide

0000002



some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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.