



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

November 4, 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 QPS Holdings, LLC (“QPS”) located at 3 Innovation Way, Newark, Delaware 19711, and write to notify your office of an event that may affect the security of certain personal information relating to Maryland residents. By providing this notice, QPS 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 August 5, 2024, QPS learned of suspicious activity related to a QPS employee email account. QPS promptly launched an investigation to assess the security of its email tenant and to confirm the full nature and scope of the activity. This investigation revealed that an unknown actor accessed a QPS e-mail account for limited periods of time between April 29, 2024, and July 28, 2024. Out of an abundance of caution, QPS performed a thorough review of the contents of the impacted email account to determine if they contained personal information and, if so, to whom the information related. Once complete, QPS reviewed its records to confirm the identities of those individuals and locate address information to provide notifications. This review recently completed.

The information that could have been subject to unauthorized access for Maryland residents includes: name and banking information.

Notice to Maryland Residents

On or about November 4, 2024, QPS provided written notice of this event to potentially affected individuals, including approximately four (4) 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 identifying the event, QPS moved quickly to investigate and respond, assess the security of its email tenant, and identify potentially affected individuals. Further, QPS reported the event to federal, and local law enforcement. QPS is also working to implement additional safeguards and training to its employees. QPS is providing access to credit monitoring services for one (1) year through IDX, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, QPS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. QPS 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.

QPS is providing written notice of this event to appropriate state privacy regulators.

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/jh

Enclosure

EXHIBIT A

[QPS Logo or Letter Head]

<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

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

<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>> <<Name 2>>:

QPS Holdings, LLC (“QPS”) writes to notify you of a recent event that may affect the security of some of your information. Although there is no indication that your information has been misused in relation to this event, we are providing you with information about the event, our response to it, and what you may do to better protect your information, should you feel it appropriate to do so.

What Happened? On or about August 5, 2024, we learned of suspicious activity related to a QPS employee email account. In response, we launched an investigation to assess the security of our email systems and to confirm the full nature and scope of the activity. This investigation revealed that an unknown actor accessed a QPS e-mail account for limited periods of time between April 29, 2024, and July 28, 2024. Out of an abundance of caution, we performed a thorough review of the contents of the impacted email accounts to determine if they contained personal information and, if so, to whom the information related. Once complete, we reviewed our records to confirm the identities of those individuals and locate address information to provide notifications. This review recently completed.

What Information was Involved? While we currently have no evidence that any personal information has been misused, the investigation determined the following types of your information were contained in one of the email accounts at the time of the event: name, address, [Types of impacted data].

What We Are Doing. We take this event and the security of information in our care very seriously. Upon learning of this event, we immediately secured the accounts and undertook a comprehensive investigation. We also took action to further enhance our security measures already in place to protect our email systems. As an added precaution, we are also offering you twelve (12) months of credit monitoring and identity restoration services at no cost to you through IDX Enrollment instructions 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 credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Personal Information* for useful information on what you can do to better protect against possible misuse of your information. You may also enroll in the free credit monitoring services we are providing for you.

For More Information. If you have additional questions, please contact Catherine Han at Catherine.Han@qps.com. You may also write to QPS at 3 Innovation Way, Newark DE 19711.

Sincerely,

Ben Hsu
Chief Operating Officer
QPS Holdings, LLC

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://response.idx.us/customending>

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

Enrollment Code: XXX

Enrollment Deadline: 12/31/2025

Steps You Can Take to Help Protect Personal Information

Enroll in Monitoring Services



1. Website and Enrollment. Go to <https://response.idx.us/customending> / <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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. However, consumers should be aware 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 Avenue NW, 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. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately [X] Rhode Island residents that may be impacted by this event.