



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

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

October 27, 2023

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 Quorum Information Technologies, Inc. (“Quorum”) located at B28 6020-2nd Street SE, Calgary, Alberta T2H 2L8, Canada, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Quorum 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 April 13, 2023, Quorum became aware of suspicious activity on its computer network. Quorum immediately initiated response protocols and launched an investigation into the nature and scope of the incident with the assistance of third-party computer forensic specialists and determined that its systems had been infected with malware which prevented access to certain files. The investigation determined that an unknown actor gained access to Quorum’s network and acquired certain archived files. In response, Quorum completed a comprehensive and time intensive review of the affected files to identify what information is contained therein and to whom that information relates. On July 25, 2023, Quorum completed its review and determined that personal information related to certain individuals may have been impacted by this event. However, for certain individuals, the documents potentially impacted didn’t have address information. As such, Quorum was required to conduct address look up services. This project was completed on September 18, 2023, and Quorum determined that a Maryland resident was impacted by this event.

Quorum is not aware of any actual or attempted misuse of any individual's personal information as a result of this event.

The information potentially impacted by this event for the Maryland resident includes name and Social Security number.

Notice to Maryland Resident

On October 27, 2023, Quorum provided written notice of this incident to one (1) Maryland resident. 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, Quorum moved quickly to investigate and respond to the incident, assess the security of Quorum systems, and identify potentially affected individuals. Further, Quorum notified federal law enforcement regarding the event. Quorum is also working to implement additional safeguards to its network. Quorum is providing access to credit monitoring services for two (2) years through TransUnion to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Quorum 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. Quorum 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) 930-4788.

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

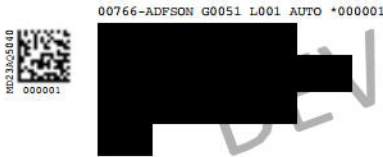
PTM/jc2
Enclosure

EXHIBIT A



240 Waterford Bridge Road, Suite 2200
St. John's NL A1E 1E2
Canada

October 26, 2023



NOTICE OF SECURITY INCIDENT

Dear [REDACTED]

Quorum Information Technologies Inc. ("Quorum") writes to notify you of an event that may impact some of your personal information. Quorum provides software services to John Jones Auto Group, a car dealership with which you have previously done business, or is your current or former employer. We are providing you with information about the event so that you can understand what happened, and the steps that can be taken, should you feel it appropriate to do so.

What Happened? On April 13, 2023, we became aware of suspicious activity on our computer network. We immediately initiated response protocols and launched an investigation with the assistance of third-party computer forensic specialists and determined that our systems had been infected with malware which prevented access to certain files. The investigation determined that this was a sophisticated attack which led to an unknown third party gaining access to our network and acquiring certain archived files. We are notifying you because the investigation determined that certain information of yours may have been impacted.

What Information Was Involved? The information that may have been impacted by this event includes your name, [REDACTED]

What We Are Doing. The privacy and security of our customers' information is one of our highest priorities, and we have strict security measures in place to protect all information in our care. Following discovery of this event, we reviewed our existing security policies and enhanced security tools to further protect the information in our systems. As part of our ongoing commitment to the privacy of personal information in our care, we are also reviewing processes for the storage and access of personal information.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take to Help Protect Personal Information* to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact moreinfo@quoruminfotech.com.

We apologize for any inconvenience this event may cause. Please rest assured that protecting information entrusted to us is extremely important to us, and we remain committed to safeguarding all data in our control.

Yours sincerely,

Quorum Information Technologies

Maury Marks
Chief Executive Officer



DEV

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring Services



Activation Code: GJJM6GDP8G

We have retained the assistance of Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged a **24-month** subscription to an online monitoring service, at no cost to you. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

<https://secure.identityforce.com/benefit/qiti>

You will be prompted to enter the following activation code:

GJJM6GDP8G

Please ensure that you redeem your activation code before 02/24/2024 to take advantage of the service.

Upon completion of the enrollment process, you will have access to the following features:

- ✓ Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- ✓ Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- ✓ Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- ✓ Identity theft insurance of up to \$1,000,000 in coverage to protect against potential damages related to identity theft and fraud¹.
- ✓ Assistance with reading and interpreting credit reports for any possible fraud indicators.
- ✓ Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-877-694-3367.

¹ In the unlikely event that your information is abused, services offered include a personal fraud specialist who will help to resolve any identity fraud issues including working with relevant agencies, business and institutions for the duration of your subscription. Once you have enrolled in the Cyberscout subscription, should you experience fraud resulting in a financial loss, you will gain access to a \$1,000,000 insurance reimbursement policy. The expense reimbursement insurance benefit for members is underwritten by certain Underwriters at Lloyd's, under a master group policy issued in the name of Cyberscout Limited, Sontiq Inc. and all subsidiaries for the benefit of members.



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 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 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 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>.