



Brian Craig
2112 Pennsylvania Avenue NW
Suite 500
Washington, D.C. 20037
Brian.Craig@lewisbrisbois.com
Direct: 202.926.2904

October 13, 2021

VIA ONLINE PORTAL

Attorney General Aaron Frey
Maine State Attorney General's Office
Security Breach Notification
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, Maine 04330
Fax: 207-624-7730
breach.security@maine.gov

Re: Notice of Data Security Incident

Dear Attorney General Frey:

We represent Magers & Quinn Booksellers, an independently owned new and used bookseller. Magers & Quinn has headquarters in Minneapolis, Minnesota. This letter is being sent pursuant 10 Me. Rev. Stat. Ann. §§ 1346-1350B, because the personal information of six (6) Maine residents may have been affected by a recent data security incident. Magers & Quinn takes the privacy and security of the information within its control very seriously and is taking significant steps to help prevent a similar incident from occurring in the future.

1) Nature of the data security incident.

On July 8, 2021, Magers & Quinn detected unusual activity relating to its online store. Upon discovering this activity, Magers & Quinn immediately engaged a team of cybersecurity experts to secure the digital environment and conduct an investigation to determine whether any personal information may have been impacted. Magers & Quinn's cybersecurity experts determined on September 15, 2021, that certain payment card information may have been exposed as a result of the incident. Magers & Quinn then worked diligently to identify addresses for the individuals whose information may have been involved. Magers & Quinn completed that process on October 12, 2021. This process identified Maine residents who may have been impacted by this incident.

2) Type of Information and Number of Maine Residents Involved

The incident involved the personal information of six (6) Maine residents. The information involved for the impacted residents included payment card information.

ARIZONA • CALIFORNIA • COLORADO • MASSACHUSETTS • FLORIDA • GEORGIA • ILLINOIS • INDIANA • KANSAS • KENTUCKY
MASSACHUSETTS • MARYLAND • MASSACHUSETTS • MISSOURI • NEVADA • NEW JERSEY • NEW MEXICO • NEW YORK
NORTH CAROLINA • OHIO • OREGON • PENNSYLVANIA • RHODE ISLAND • TEXAS • UTAH • WASHINGTON • WEST VIRGINIA

On October 13, 2021, Magers & Quinn notified the affected Maine residents via the attached sample letter. Magers & Quinn has also taken measures to enhance the security of its network to minimize the likelihood that an event like this might occur again in the future.

3) Measures Taken to Address the Incident

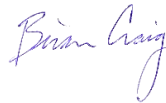
In response to the incident, Magers & Quinn retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise.

Additionally, as discussed above, Magers & Quinn is notifying the affected individuals and providing them with steps they can take to protect their personal information.

4) Contact Information

Magers & Quinn is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident please contact myself at brian.craig@lewisbrisbois.com or my colleagues, Shelly Hall or Shaun Goodfriend at shelly.hall@lewisbrisbois.com or shaun.goodfriend@lewisbrisbois.com, respectively, should you have any questions.

Sincerely,



Brian Craig of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Magers & Quinn Booksellers (“M&Q”) is writing to notify you of a data security incident relating to your purchase through our online store (www.magersandquinn.com) that may have involved your payment card information. At M&Q, we take the privacy and security of your information very seriously. We want to inform you of the incident and to advise you about certain steps you can take to ensure your information is protected.

What Happened? On July 8, 2021, we learned of suspicious activity in our online store. Upon discovery, M&Q immediately engaged a team of cybersecurity experts, including a digital forensic firm and privacy counsel, to secure the digital environment and conduct an investigation to determine whether any personal information may have been impacted. M&Q’s cyber security experts advised on September 15, 2021, that certain payment card information may have been exposed as a result of the incident. M&Q immediately began preparing to notify you, securing monitoring services, and coordinating delivery of the notification materials.

What Information Was Involved? The payment card information that may have been compromised included names, card numbers, expiration dates, and security codes.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. Also, we are providing you with this notice and information about steps you can take to help protect your personal information. In addition, we are offering you 12 months of complimentary identity monitoring services.

What You Can Do. Please review this letter, along with the enclosed recommendations regarding additional steps you can take to help protect your information. We also recommend you activate the identity monitoring services we are offering at no cost to you.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

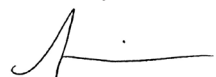
You have until **January 9, 2022** to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For More Information. Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please contact us at 1-855-732-0772, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major US holidays. To receive identity monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Kroll representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we regret any worry or inconvenience that this may cause you.

Sincerely,



Jessi Blackstock, Manager
Magers & Quinn Booksellers

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Washington Attorney General

1125 Washington Street SE
PO Box 40100
Olympia, WA 98504
[https://www.atg.wa.gov/
recovering-identity-theft-or-fraud](https://www.atg.wa.gov/recovering-identity-theft-or-fraud)
1-360-753-6200

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.