

**BakerHostetler**

STATE OF NH  
DEPT OF JUSTICE

2018 NOV 21 AM 10:37

**Baker & Hostetler LLP**

811 Main Street  
Suite 1100  
Houston, TX 77002-6111

T 713.751.1600  
F 713.751.1717  
www.bakerlaw.com

William R. Daugherty  
direct dial: 713.646.1321  
wdaugherty@bakerlaw.com

November 20, 2018

**VIA OVERNIGHT MAIL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol St  
Concord, NH 03301

*Re: Incident Notification*

Dear Attorney General MacDonald:

We are writing on behalf of our client, R.R. Bowker LLC ("Bowker"), to notify you of a security incident.

Bowker was recently informed by certain payment card networks that patterns of unauthorized charges on payment cards were identified after they were legitimately used on Bowker's website, [www.myidentifiers.com](http://www.myidentifiers.com). Upon learning this, Bowker launched an investigation with the assistance of a cybersecurity firm. On October 23, 2018, the investigation identified unauthorized code that was added to the checkout page of [www.myidentifiers.com](http://www.myidentifiers.com). Findings from the investigation indicate that the code may have been present and capable of copying information entered by customers during the checkout process from May 1, 2018 to October 23, 2018. Bowker immediately removed the unauthorized code after identification. The personal information that may have been accessed included individuals' names, addresses, email addresses, payment card numbers, expiration dates, and card security codes (CVV).

Today, Bowker will begin notifying 93 New Hampshire residents via U.S. mail in accordance with N.H. Rev. Stat. Ann. § 359-C:20, in substantially the same form as the enclosed letter. Bowker also provided a telephone number for individuals to call with questions.

To help prevent a similar incident from happening in the future, Bowker has implemented additional security enhancements to the [www.myidentifiers.com](http://www.myidentifiers.com) website. In addition, Bowker is working with law enforcement and is continuing to support law enforcement's investigation into the incident.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Office of the Attorney General  
November 20, 2018  
Page 2

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "William R. Daugherty". The signature is fluid and cursive, with a large, sweeping flourish at the end.

William R. Daugherty  
Partner

Enclosure



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>> <<Date>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

Dear <<Name 1>>:

R.R. Bowker LLC (“Bowker”) was recently made aware by payment card networks of patterns of unauthorized charges occurring on cards after they were legitimately used on www.myidentifiers.com. We launched an investigation with assistance from a leading cybersecurity firm and addressed the incident. However, your payment card information may have been involved. Here are details about the incident, measures we have taken, and some steps you can take in response.

On October 23, 2018, our investigation identified unauthorized code that was added to the checkout page on www.myidentifiers.com. Findings from the investigation indicate that the code may have been present and capable of copying information entered by customers during the checkout process from May 1, 2018 to October 23, 2018. The information entered during checkout that the code could have potentially copied includes name, address, email address, payment card number, expiration date, and card security code (CVV). We are notifying you because you placed, or attempted to place, an order on our website using the payment card(s) ending in <<<Last 4 of Card Number>>> during the relevant time period.

We encourage you to closely review your payment card account statements for any unauthorized activity. You should immediately report any unauthorized charges to the bank that issued the card. Payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. Information on additional steps you can take can be found on the following pages.

We value the relationship we have with our customers and regret this incident occurred. The unauthorized code has been removed and we’ve also implemented additional security enhancements to our website. In addition, Bowker is working with law enforcement and is continuing to support law enforcement’s investigation into the incident. Please accept our apology for any inconvenience.

If you have questions, please call 888-418-0271 Monday through Friday between the hours of 9:00 a.m. and 9:00 p.m. EST.

Sincerely,

Beat Barblan  
Senior Director, Identifier Services

### Additional Steps You Can Take

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you detect any unauthorized activity on your financial account, you should immediately contact your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com) , 1-800-685-1111  
*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**If you are a resident of Connecticut, Maryland, or North Carolina** you may contact and obtain information from your state attorney general at:

*Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)

*Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023 (toll free when calling within Maryland) or 410-576-6300 (for calls originating outside Maryland)

*North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716-6400 or toll free at 1-877-566-7226

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

**Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
**TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)  
**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

**Fair Credit Reporting Act:** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit [www.ftc.gov/credit](http://www.ftc.gov/credit). The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. And you must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.