RECEIVED

APR 08 2019

CONSUMER PROTECTION

BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

April 5, 2019

Via Overnight Mail

Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Incident Notification

Dear Sir or Madam:

On behalf of our client, Santa Barbara City College ("SBCC"), we are writing to notify you of a security incident involving two New Hampshire residents.[1]

On March 4, 2019, SBCC was notified by one of its service providers, PrismRBS, that some customers who provided payment card information on SBCC's book store website may have been impacted by a security incident. This incident involved an unauthorized individual installing malicious software on the website designed to capture payment card information between January 19, 2019 and January 26, 2019, including cardholders' names, card numbers, expiration dates and card verification codes.

Upon discovering this unauthorized access, the vendor informed SBCC that they engaged a leading data security team to assist in their investigation and that they have implemented several additional security measures to help prevent this type of incident from reoccurring in the future. On March 11, 2019, PrismRBS mailed notification letters to the two affected New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20 in substantially the same form as the attached letter.

Although driver's license numbers and Social Security numbers were not impacted as part of this incident, as an added precaution the vendor is offering eligible potentially affected individuals a complimentary one-year membership in credit monitoring and identity theft protection services from

[1] This report does not waive SBCC's objection that New Hampshire lacks personal jurisdiction related to this matter.

Experian. The vendor has also provided a telephone number for potentially affected individuals to call with any questions they may have.

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

Sincerely,

M. Scott Koller

M. Scott Koller
Partner

Enclosure

Prism|rbs
retail business solutions

March 11, 2019

[NAME]
[ADDRESS]

Dear [NAME]:

Notice of Data Breach

The SBCC Bookstore Online was recently notified by one of its service providers of a security incident that could affect the payment card information of some customers who made purchases on our website, https://www.sbccbooks.com, between January 19th and January 26th, 2019. As a precaution, we are providing this notice to make potentially affected customers aware of the incident and provide information on steps they can take to help protect themselves. We take the security of our customers' information very seriously and deeply regret any concern this may cause you.

What Happened

The SBCC Bookstore Online recently learned that PrismRBS, a vendor that works with the SBCC Bookstore Online to provide its eCommerce website, experienced a security incident in which an unauthorized party was able to install malicious software designed to capture payment card information on some of the eCommerce servers that host the SBCC Bookstore Online website.

What Information Was Involved

Based on the forensic investigation, it appears that the unauthorized party was able to access payment card information, including cardholder names, card numbers, expiration dates and card verification codes, for certain transactions made on the website. Because we do not collect sensitive information such as Social Security, passport or driver's license numbers, this type of information was not affected by this incident. Please note that this incident affected only eCommerce transactions made on https://www.sbccbooks.com between January 19th and January 26th, 2019; transactions made outside of this period of time, those made in our on-campus facility and other university transactions were not affected by this incident.

What We Are Doing

We take the privacy of personal information seriously and deeply regret that this incident occurred. The vendor has informed us that they engaged a leading cybersecurity firm to assist in their investigation. Additionally, the vendor has implemented several additional security measures to help prevent this type of incident from reoccurring in the future.

Prism|rbs
retail business solutions

What You Can Do

You can review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed. Remain vigilant and continue to monitor statements for unusual activity going forward. If you see something you do not recognize, immediately notify the financial institution as well as the proper law enforcement authorities. In instances of credit or debit card fraud, it is important to note that cardholders are not typically responsible for any fraudulent activity that is reported in a timely fashion.

Although Social Security numbers and other sensitive personal information were not at risk in this incident, as a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. As an additional precaution, we are providing information and resources to help individuals protect their identities. This includes an "Information about Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

As an added precautionary measure, we are offering **one year** of identity protection services through IdentityWorks. Call 877-239-1287 for instructions on how to take advantage of this service.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact 877-239-1287, between of the hours of 9 AM to 9 PM ET, Monday through Friday. Again, we sincerely regret any concern this incident may cause.

Sincerely,

Jim Clark

Jim Clark
Director of IT

Prism|rbs
retail business solutions

Information about Identity Theft Protection

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Security Freezes and Fraud Alerts:

You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 you are a victim of identity theft, you are entitled to an

extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and an incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a "security freeze" on your credit report.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf,https://www.consumerfinance.gov/learnmore/, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com) **General Contact:** P.O. Box 740241 Atlanta, GA 30374 800-685-1111 **Fraud Alerts**: P.O. Box 740256, Atlanta, GA 30374 **Credit Freezes**: P.O. Box 105788, Atlanta, GA 30348	Experian (www.experian.com) **General Contact:** P.O. Box 2002 Allen, TX 75013 888-397-3742 **Fraud Alerts and Security Freezes:** P.O. Box 9554, Allen, TX 75013	TransUnion (www.transunion.com) **General Contact, Fraud Alerts and Security Freezes:** P.O. Box 2000 Chester, PA 19022 888-909-8872