



Michael Best & Friedrich LLP
Attorneys at Law
Adrienne S. Ehrhardt, CIPP/US, CIPM
T 608.283.0131
E asehrhardt@michaelbest.com

STATE OF NH
DEPT OF JUSTICE
2019 MAY 31 AM 10:07

VIA FEDEX

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

May 30, 2019

RE: Breach of Security of Personal Information

To the Office of the Attorney General:

Pursuant to N.H. Rev. Stat. §359-C:19, et seq., Colgate University (the “University”), through its attorneys Michael Best & Friedrich, LLP, is writing to notify you of an external system breach exposing personal information involving one (1) New Hampshire resident.

One of the University’s third-party service providers, PrismRBS, hosts the University’s online bookstore, and this incident involved purchases made on the University bookstore website. On or about May 3, 2019, PrismRBS informed the University that PrismRBS was investigating an incident relating to the University’s bookstore website. On or about May 9, 2019, PrismRBS notified the University that its ongoing investigation determined that an unauthorized third party obtained access to one of PrismRBS’s servers and installed malicious code designed to capture payment card information on servers that PrismRBS uses to host the bookstore website. That unauthorized third party was able to access information captured on the bookstore website between April 13, 2019, and April 26, 2019. Because this incident occurred on PrismRBS’ systems, only transactions on the University’s online bookstore in that limited time period were affected. This incident did not affect the University’s systems and so did not affect on-campus transactions or other transactions with the University.

PrismRBS believes that the unauthorized party was able to access payment card information, including cardholder names, card numbers, expiration dates and card verification codes, billing addresses, and phone numbers. The University bookstore, however, does not collect or have access to social security numbers or passport or driver’s license numbers. Therefore, this information was not affected by this incident.

PrismRBS hired an outside expert IT forensics firm to respond to and investigate the incident. PrismRBS has also informed us that it has enhanced the security of its systems, including implementing additional threat monitoring and detection tools, and enabling two-factor authentication on its internal email system. In addition, PrismRBS has engaged an independent IT security firm to perform a comprehensive audit of its systems. The University is not aware



May 30, 2019
Page 2

whether PrismRBS's notification to us was delayed as a result of a law enforcement investigation, and no such investigation delayed our notification to you.

The University has also notified its credit card payment processor of the incident so that the card brands are also notified and are aware of the incident.

Attached is a copy of the Notification letter that the University will place in the U.S. Mail today, Thursday, May 30, 2019, to the affected individuals. Please let us know if you have any questions or would like to discuss further.

Sincerely,

MICHAEL BEST & FRIEDRICH LLP

A handwritten signature in black ink that reads 'Adrienne S. Ehrhardt'.

Adrienne S. Ehrhardt

Enclosure

COLGATE UNIVERSITY

<<Customer FirstName>> <<Customer LastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Notice of Security Breach

Dear <<Customer FirstName>>,

We are writing to inform you about a data incident that occurred at one of Colgate University's (the "University") third-party service providers, PrismRBS, that may have involved your personal data. PrismRBS hosts the University's online bookstore, and this incident involved purchases made on the University bookstore website, regardless of whether you are student at the University. We value our relationship with you and take the security of your data seriously.

Please review the information provided in this letter for some steps you may take relating to this incident.

What Happened?

On or about May 3, 2019, PrismRBS informed the University that PrismRBS was investigating an incident relating to the University's bookstore website. On or about May 9, 2019, PrismRBS notified the University that its ongoing investigation determined that an unauthorized third party obtained access to one of PrismRBS's servers and installed malicious code designed to capture payment card information on servers that PrismRBS uses to host the bookstore website. That unauthorized third party was able to access information captured on the bookstore website between April 13, 2019, and April 26, 2019. Because this incident occurred on PrismRBS' systems, only transactions on our online bookstore in that limited time period were affected. This incident did not affect the University's systems and so did not affect on-campus transactions or other transactions with the University.

What Information Was Involved?

PrismRBS believes that the unauthorized party was able to access payment card information, including cardholder names, card numbers, expiration dates and card verification codes, billing addresses, and phone numbers. The University bookstore, however, does not collect or have access to social security numbers or passport or driver's license numbers. Therefore, this information was not affected by this incident.

Here's What We Are Doing and What You Can Do

PrismRBS hired an outside expert IT forensics firm to respond to and investigate the incident. PrismRBS has also informed us that it has enhanced the security of its systems, including implementing additional threat monitoring and detection tools, and enabling two-factor authentication on its internal email system. In addition, PrismRBS has engaged an independent IT security firm to perform a comprehensive audit of its systems. The University is not aware whether PrismRBS's notification to us was delayed as a result of a law enforcement investigation, and no such investigation delayed our notification to you.

The University has also notified its credit card payment processor of the incident so that the card brands are also notified and are aware of the incident with respect to your information.

COLGATE UNIVERSITY

For More Information

In addition, we are providing you with the enclosed information about Identity Theft Protection. You should review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed. If you see something you do not recognize, immediately notify your financial institution.

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 added precautionary measure, PrismRBS is offering **one year** of identity protection services through IdentityWorks. Please call 877-239-1287 for instructions on how to take advantage of this service.

We sincerely apologize for any inconvenience or concern this incident may cause. If you have questions, please call us at 315-228-7151 or send us an email at privacy@colgate.edu.

Sincerely,



Nelson Lee
Director of Information Security and Information Security Officer

Information about Identity Theft Protection

Review Accounts and Credit Reports: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:
Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

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