



[DATE]

[NAME]

[ADDRESS]

Dear [NAME]:

NOTICE OF DATA BREACH

The Campus Store was recently notified by PrismRBS, one of its service providers, that PrismRBS had suffered a security incident that could affect the payment card information of some customers who made purchases on <https://bookstore.wilmu.edu>, between April 13th and April 26th, 2019. As a precaution, we are providing this notice to make affected customers aware of the incident and provide information on steps you can take to help protect yourself. We take the security of our customers' information very seriously and deeply regret any concern this may cause you.

What Happened

The Campus Store recently learned that PrismRBS, a vendor that works with the Campus Store 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 Campus Store website. This incident was isolated to PrismRBS, and we have no knowledge that any Wilmington University systems were involved in this incident.

What Information Was Involved

PrismRBS has told us that the unauthorized party was able to access payment card information on PrismRBS's systems, including cardholder names, card numbers, expiration dates, card verification codes, billing address and phone number, for certain transactions made through the website during a specific and limited timeframe from April 13th to April 26th, 2019. Because the Campus Store does 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://bookstore.wilmu.edu>

between April 13th and April 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. PrismRBS is taking steps to enhance the security of its systems, including implementing additional threat monitoring and detection tools. We are also working with our security team to determine whether any additional security measures are needed on Wilmington University systems and will be evaluating our relationship with PrismRBS moving forward.

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, Wilmington University is 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 a dedicated call center at 877-239-1287, Monday through Friday from 9 a.m. to 9 p.m. ET. You may also reach us at our business address: 320 N. DuPont Highway New Castle, DE 197203. Again, we sincerely regret any concern this incident may cause.

Sincerely,

[NAME]

[TITLE]

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.

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.

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 freezes by contacting the FTC or one of the national credit reporting agencies listed below.

<p>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</p>	<p>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</p>	<p>TransUnion (www.transunion.com) General Contact, Fraud Alerts and Security Freezes: P.O. Box 2000 Chester, PA 19022 888-909-8872</p>
---	--	--