14834

The University of Vermont

OFFICE OF AUDIT, COMPLIANCE AND PRIVACY SERVICES
www.uvm.edu/compliance

B159, Billings Library, 48 University Place
Burlington, VT 05405
P: (802) 656-3086 • E: privacy@uvm.edu

March 28, 2019

«First_Name» «Last_Name»
«Street_Address»
«City», «State_Zip»

Dear «First_Name» «Last_Name»:

I write to provide notice of an incident regarding your personal information. The University takes the privacy and security of your personal information very seriously and it is important to us that you have this information.

On January 25, 2019, the University Bookstore received a preliminary report from PrismRBS, the vendor that provides its e-commerce website, that the vendor may have experienced a security incident affecting purchases made at uvmbookstore.uvm.edu/ by Vermont residents and was investigating.

Based on its investigation, PrismRBS notified the University on February 28, 2019 that this incident may have affected transactions that occurred between January 19 and January 23, 2019. Based on our records, you engaged in a transaction during this date range using a payment card belonging to you. This transaction included credit/debit card information (cardholder name, card number, expiration date, card verification code, and billing address).

It is important to note that sensitive information such as Social Security Numbers, passport or driver's license numbers, typically required for Identity Theft, are not collected and **was not affected** by this incident.

After receiving notification from PrismRBS, in addition to notifying you directly, the University has provided notice to appropriate entities as required under applicable state laws. While the vendor's forensics investigation is ongoing, we wanted to provide timely notice to you in order for you to take steps to protect yourself. The vendor continues to conduct a comprehensive investigation and has assured UVM that it has implemented several additional security measures to help prevent this type of incident from reoccurring in the future.

UVM is committed to protecting your personal information, and we have policies and procedures to protect your privacy. Unfortunately, those safeguards are not foolproof, and it is important for each individual to remain vigilant in protecting their personal information. I have attached a copy of the Federal Trade Commission's (FTC) "Data Breaches: What to Know, What to Do"

reference guide which describes steps you may take to protect yourself. You also have the right to file or obtain a police report.

You may request a credit freeze (also known as security freeze) at no charge by contacting each of the nationwide credit bureaus below. You will need to supply your name, address, date of birth, Social Security number, and other personal information.

Equifax
Equifax.com/personal/credit-report-services
800-685-1111

Experian
Experian.com/help
888-EXPERIAN (888-397-3742)

Transunion
TransUnion.com/credit-help
888-909-8872

Additional information from the FTC can be found at https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

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

If you have any questions regarding this notification, please call the Data Breach Information Line at (888) 229-7874 and leave a message including your name, number and a good time to reach you. Someone will call you back within 1 business day.

Sincerely,

Tessa L.C. Lucey, MHA, CHC, CHCP
Director of Compliance Services and Chief Privacy Officer

Cc: Simeon Ananou, Chief Information Officer
Julia Russell, Associate Chief Information Officer
Mark Ackerly, Information Security Officer

PrismRBS Data Breach

FAQ's

What Happened?

The UVM Bookstore recently learned that PrismRBS, a vendor that provides our e-commerce website, experienced a security incident in which an unauthorized party was able to gain access to and install malicious software designed to capture payment card information on some of the e-commerce servers that host uvmbookstore.uvm.edu/. As it relates to the UVM Bookstore website, a total of 147 individuals were affected and the University has taken steps to notify the individuals affected by this incident.

What data was affected?

Based on PrismRBS' forensic investigation, it appears that the unauthorized party was able to access payment card information, including cardholder names, card numbers, expiration dates, card verification codes, and billing address 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.

What about purchases made on other websites or at other venues on campus?

This incident affected only e-commerce transactions made on uvmbookstore.uvm.edu/ between January 19 and January 23, 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 is being done?

Our vendor, PrismRBS, has engaged a Payment Card Industry (PCI) validated forensics data company to conduct a comprehensive investigation. Additionally, the vendor has implemented several additional security measures to help prevent this type of incident from reoccurring in the future.

Is PrismRBS offering credit monitoring services?

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

What you (the customer) 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 your 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.
- Social security numbers and other sensitive personal information were not at risk in this incident. As a good general practice, it is recommended 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, the letter you received included an "Information about Identity Theft Protection" reference guide, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection. Additional information from the FTC can be found at https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

What if I have more questions?

If you have additional questions that are not addressed here, please call the Data Breach Information Line at 888-229-7874 and leave a message including your name, number, and a good time to reach you. Someone will return your call within 1 business day.