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

July 11, 2019

«BillingName»
«BillAddr1» «BillAddr2»
«BillCity», «BillState» «BillingZipCode»

Dear «BillingName»:

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 May 3, 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 and was investigating. Specifically, PrismRBS' security team discovered that an unauthorized party was able to gain access to and install malicious software designed to capture payment card information on some of the servers that host the UVM Bookstore's website (https://uvmbookstore.uvm.edu/).

On May 9, 2019, PrismRBS notified the University that, based on its investigation, this incident may have affected transactions that occurred between April 13 and April 26, 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. We have included a

copy of our FAQ for this incident which provides additional information and steps that you can take to protect yourself including how to access credit monitoring services provided by PrismRBS. I have also attached a copy of the Federal Trade Commission's (FTC) "Data Breaches: What to Know, What to Do" reference guide which describes additional steps you may take to protect yourself. Additional information from the FTC can be found at https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

If you have any questions regarding this notification, please call the Data Breach Information Line (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 third party obtained access to and was able to 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 670 individuals were affected and the University has taken steps to notify the individuals affected by this incident.

Isn't this the second time this has happened since January?

Yes. PrismRBS learned on April 26 of a security incident in which an unauthorized third party obtained access to one of its servers and was able to install malicious code. Unfortunately as a result, between April 13 and April 26, 2019, payment data could have been affected for orders placed during this window of time. PrismRBS is continuing to take steps to enhance the security of its systems. We apologize for any frustration or concern this may cause.

While this is the second incident since January, this incident involved different tactics and technology employed by the unauthorized party.

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, billing address and phone numbers 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 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 about transactions paid for using financial aid?

This incident was designed to capture payment card information only. Customers using financial aid as their payment type, were not affected.

What is the bookstore doing?

Our website provider, PrismRBS, has engaged a leading IT forensic firm to assist in its comprehensive investigation. The vendor is also taking steps to enhance the security of its systems, including implementing additional threat monitoring and detection tools.

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.

Data Breaches

What to know, What to do

FEDERAL TRADE COMMMISSION

IdentityTheft.gov

Did you recently get a notice that says your personal information was exposed in a data breach? Did you lose your wallet? Or learn that an online account was hacked? Depending on what information was lost, there are steps you can take to help protect yourself from identity theft.

If your information has been exposed, visit IdentityTheft.gov/databreach for detailed advice about your particular situation.

Depending on the type of information exposed, the next page tells you what to do right away. You'll find these steps – and more – at **IdentityTheft.gov/databreach**.

What information was lost or exposed?

Social Security number

- ☐ If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- ☐ Get your free credit reports from **annualcreditreport.com**. Check for any accounts or charges you don't recognize.
- ☐ Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name.

  If you decide not to place a credit freeze, at least consider placing a fraud alert

- ☐ Try to file your taxes early – before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job.

Online login or password

- ☐ Log in to that account and change your password. If possible, also change your username

  If you can't log in, contact the company. Ask them how you can recover or shut down the account.

- ☐ If you use the same password anywhere else, change that, too.
- ☐ Is it a financial site, or is your credit card number stored? Check your account for any charges that you don't recognize.

Bank account, credit, or debit card information

- ☐ If your bank information was exposed, contact your bank to close the account and open a new one.
- ☐ If credit or debit card information was exposed, contact your bank or credit card company to cancel your card and request a new one.

Other information

For guidance about other types of exposed information, visit **IdentityTheft.gov/databreach**.

If your child's information was exposed in a data breach, check out ***Child Identity Theft – What to know, What to do***.

FEDERAL TRADE COMMISSION
IdentityTheft.gov
September 2016