

15428



The University of Vermont

OFFICE OF AUDIT, COMPLIANCE AND PRIVACY SERVICES  
[www.uvm.edu/compliance](http://www.uvm.edu/compliance)

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

---

July 23, 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 affecting purchases made at [uvmbookstore.uvm.edu/](http://uvmbookstore.uvm.edu/) and was investigating.

Based on its investigation, PrismRBS notified the University on May 9, 2019 that 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. 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](http://Equifax.com/personal/credit-report-services)  
800-685-1111

**Experian**

[Experian.com/help](http://Experian.com/help)  
888-EXPERIAN (888-397-3742)

**Transunion**

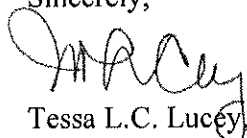
[TransUnion.com/credit-help](http://TransUnion.com/credit-help)  
888-909-8872

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.

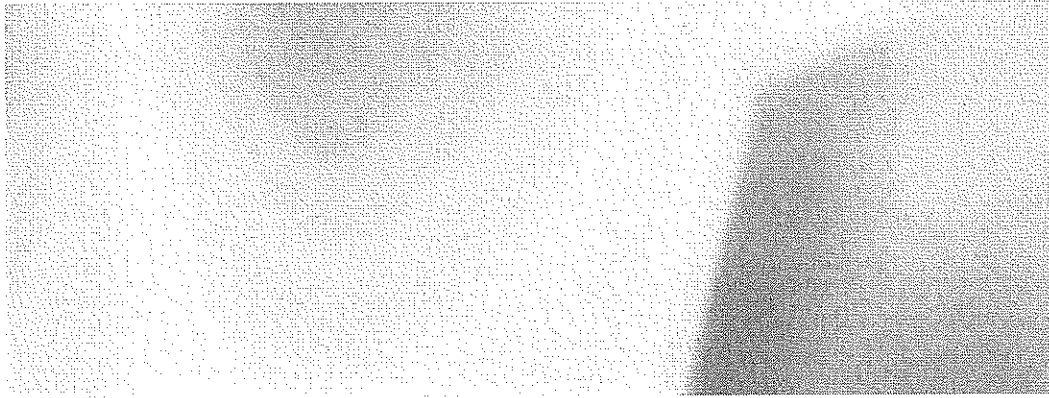
If you have any questions regarding this notification, please call the Data Breach Information Line at (888) 229-7874 and leave a message including your name, number and a good time to reach you. Someone will call you back within 1 business day.

Sincerely,



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

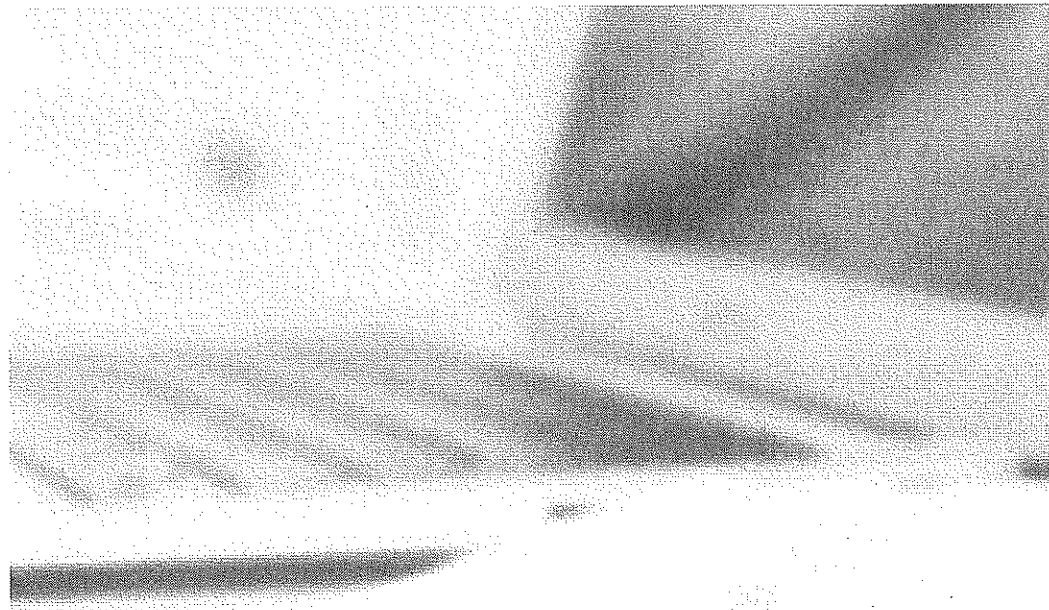
Cc: Simeon Ananou, Chief Information Officer  
Julia Russell, Associate Chief Information Officer  
Mark Ackerly, Information Security Officer



# Data Breaches

---

What to know, What to do



FEDERAL TRADE COMMISSION

[IdentityTheft.gov](https://www.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](https://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](https://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](https://www.ftc.gov/identitytheft).

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