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

November 11, 2022

[NAME]
[ADDRESS]

Dear [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 October 28, 2022, an email was sent to two students asking that they fill out a form. Attached to the email was supposed to be a blank form; however, the sender accidentally attached a form that had already been filled out. The form contained your social security number.

On October 28, 2022, the University discovered this error and immediately began mitigation efforts. The students who received the form in error were contacted and confirmed that they did not further share the email and also deleted it from their inbox and their deleted folder. We have no reason to believe that anyone else has received this form. This incident was reported to my office for additional review and mitigation.

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 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 my office at (802) 656-3086.

Sincerely,

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

Cc: Simeon Ananou, Chief Information Officer
Sam Hooker, Information Security Officer
Melissa Long, Larner College of Medicine Registrar
Darcy Pientka, Deputy Chief Information Officer

SPECIMEN COPY

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 COMMMISSION
IdentityTheft.gov
September 2016