



The University of Vermont

CHIEF INFORMATION / PRIVACY OFFICER

August 10, 2016

Dear

I believe that you are already aware of a recent incident regarding your personal information. Still, the University takes the privacy and security of your personal information very seriously, and it is important to us that you have this information. You may have already received a notification email, a phone call, or both from the University. Please be advised that this letter is in relation to the same incident, not another. However, guidance issued by the Vermont Attorney General's office recommends that official notifications be sent via regular mail.

On July 1, 2016, we discovered that your UVM NetID and password were used to gain access to UVM's Human Resources PeopleSoft Self-Service Module. Our investigation revealed that the unauthorized access, affecting a small number of employees, was the result of compromised UVM credentials for each affected employee (UVM NetID and password), which appear to have been stolen as part of a "phishing" scam. The email may have contained the subject "Message from UVM Staff Portal" or it could have contained a link that infected the computer you were using with malicious software.

It appears that the motivation for unauthorized access was an unsuccessful attempt to divert direct deposit payments to another account. The specific information viewed was your financial account information related to the direct deposit of your paycheck. Those intruders could also have viewed other personal information available through UVM's Human Resources People Soft Self-Service Module, but we have no indication that they did so. That information includes certain personal information that could contribute to the risk of identity theft for you, including your Social Security Number; University-provided medical or dental plans that you and your dependents have enrolled in; the amount of your flexible spending pledge for 2016; and the first and last name, Social Security Numbers, and dates of birth of your dependents that are covered by University medical and dental plans.

After discovering this incident on July 1, we began an investigation to determine the facts, and we have notified the Vermont Attorney General. The University has taken steps to prevent future illicit access, including invalidating the stolen password and requiring you to set a new one. While this investigation is ongoing, we wanted to provide timely notice to you in order for you to take steps to protect yourself.

We recommend that you monitor your credit reports and financial statements for potential identity theft for one year. For more information about obtaining a credit monitoring service and other additional steps you may consider taking, please see the attached information or visit the Federal Trade Commission's website at: <https://www.identitytheft.gov/Info-Lost-or-Stolen>.

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 his or her personal information. UVM will *never* ask you to disclose your NetID and password. Any email or message that asks you to provide your password on a non-[uvm.edu](http://uvm.edu) website is fraudulent. If you have any questions, please contact (866) 236-5752.

Sincerely,

Mara Saule  
Chief Privacy Officer