



Minnesota Department of Human Services  
Elmer L. Andersen Building  
Commissioner Emily Piper  
Post Office Box 64998  
St. Paul, Minnesota 55164-0998

October 9, 2018

Dear Sir or Madam:

Because the Minnesota Department of Human Services (“DHS”) respects and values the privacy of your personal information, we want you to know about two recent data security incidents that may have resulted in someone accessing your personal information without permission. We currently have no evidence that this information was actually viewed, downloaded, or misused.

**What happened?** Over the past several months, there has been an increase in the number of attempted “phishing campaigns” targeting Minnesota’s executive agencies, including DHS. Two of these recent phishing campaigns against DHS were successful. These incidents occurred on or around June 28 and July 9, 2018, and involved hackers getting access to the state email accounts of two DHS employees and using these accounts to send out spam emails.

**What information was involved?** The two email accounts contained information about some people who have interacted with DHS, including you. Examples of the type of information found in the email accounts at the time they were compromised include: first and last names, dates of birth, Social Security numbers, addresses, telephone numbers, medical information, educational records, employment records, and/or financial information.

**How did we respond to these data security incidents?** Minnesota IT Services (“MN.IT”) is the information technology agency for all of Minnesota’s executive branch, including DHS. MN.IT immediately took steps to secure the two email accounts and stop the spread of the phishing emails. MN.IT then investigated these incidents, and told us about the results of its investigation on or around August 13, 2018. We also reported these incidents to the Office of Civil Rights and the Minnesota Office of the Legislative Auditor.

**What are we doing to prevent future data security incidents?** We continue to work hard to protect against these and other types of data security incidents. We teach DHS employees about email best practices and how to respond to data security incidents. We use the technology at our disposal to its fullest potential to prevent and mitigate data security incidents, and push for security technology upgrades. We update relevant policies and procedures.

**What should you do?** Although we are not aware of any misuse of the information contained in the two email accounts, we suggest that you consider taking these steps to help protect against identity theft:

October 9, 2018

Page 2 of 2

- Ask to see your credit report. Under federal law, you have the right to receive a free copy of your credit report every 12 months from each of the three consumer credit reporting companies. You may request these reports online at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by telephone at (877) 322-8228.
- Check your credit report for any transactions or accounts that you do not recognize.
- Call the telephone number listed on the credit report or visit the Federal Trade Commission's website on identity theft at <http://www.consumer.gov/idtheft/> if you see anything in your credit report that you do not understand.

**Where can you get more information?** If you have any questions or would like more information about these data security incidents, please write or call us:

Minnesota Department of Human Services  
State Medical Review Team  
P.O. Box 64248  
St. Paul, MN 55164-0248

(651) 431-2255

We will also be preparing a report about these incidents. You may ask us to send you a copy of this report by mail or email by writing or calling us.

We sincerely regret these data security incidents and apologize for any impact they may have on you or your family.

Sincerely,



Emily Piper  
Commissioner