DEPARTMENT OF HUMAN SERVICES

April 9, 2019

Sen. Michelle Benson, Chair
Senate Health & Human Services Finance & Policy
3109 Minnesota Senate Building
St. Paul, MN 55155

Sen. Jim Abeler, Chair
Senate Human Services Reform Finance & Policy
3215 Minnesota Senate Building
St. Paul, MN 55155

Sen. Jeff Hayden, Ranking Minority Member
Senate Human Services Reform Finance & Policy
2209 Minnesota Senate Building
St. Paul, MN 55155

Sen. John Marty, Ranking Minority Member
Senate Health & Human Services Finance & Policy
2401 Minnesota Senate Building
St. Paul, MN 55155

Rep. Tina Liebling, Chair
House Health & Human Services Finance
477 State Office Building
St. Paul, MN 55155

Rep. Rena Moran, Chair
House Health & Human Services Policy
575 State Office Building
St. Paul, MN 55155

Rep. Joe Schomacker, Ranking Minority Member
House Health & Human Services Finance
209 State Office Building
St. Paul, MN 55155

Rep. Debra Kiel, Ranking Minority Member
House Health & Human Services Policy
255 State Office Building
St. Paul, MN 55155

Dear Senators and Representatives:

I am writing to let you know that a state email account of a Minnesota Department of Human Services (DHS) employee has been compromised as a result of a cyberattack, potentially exposing the personal information of approximately 11,000 individuals. This incident occurred on or about March 26, 2018. We currently have no evidence that the personal information contained in this account was viewed, downloaded or misused in any way.

DHS has reported this incident to the Office of the Legislative Auditor, and MNIT has reported this incident to the Federal Bureau of Investigation. Today, DHS will report this incident to the U.S. Department of Health and Human Services, consumer reporting agencies, and the media; mail individual notification letters to the people who may be impacted by this incident; and post information about this incident to its homepage.

During this cyberattack, the hacker used the state email account of an employee in our Direct Care and Treatment administration to send legitimate-looking emails to one of the employee's co-workers. This email asked the co-worker pay an "invoice" via a wire transfer. The employees then recognized that these emails were suspicious, did not wire any money and, consistent with their training and DHS/MNIT policies, reported the emails to MNIT. The hacker would have had the ability to view, download, or otherwise obtain some of the account's contents during this cyberattack. MNIT is unable to identify what, if any, information was viewed or obtained by the hacker.

After the DHS employees reported the suspicious emails to MNIT, MNIT took action to secure the compromised account and investigated the incident. MNIT told DHS about the results of this investigation on February 15, 2019.

Upon receiving the results of MNIT's investigation, DHS hired a contractor to review the account's contents and provide DHS with the names of people whose personal information was in the account at the time it was compromised. DHS decided to use this contractor because of the account's size and complexity, and the need to identify and notify people who may be impacted by this incident as quickly as possible. This contractor finished its work on March 21, 2019.

At the time it was compromised, the account contained various types of personal information about DHS' clients, employees and applicants, including but not limited to first and last names, dates of birth, contact information, treatment data and legal history. The account also contained the Social Security numbers of two individuals at the time it was compromised; it did not contain any financial account information.

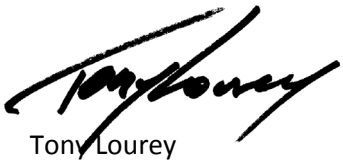
MNIT and DHS have taken important steps to help prevent such incidents from happening in the future. Notably, in February 2019, MNIT deployed a new cybersecurity tool that blocks malicious links and attachments in emails intended for state employees. This tool could have prevented many of the breaches experienced by DHS, including the breach described in this letter. MNIT and DHS also continue to train employees on how to identify and report the increasingly sophisticated cyberattacks being perpetrated against DHS, and have revised their policies and procedures to ensure that they can appropriately and quickly respond to data security incidents.

Although we are not aware of any misuse of the information contained in the DHS employee's email account, our notification letter to the individuals who may be impacted by this incident includes suggestions about how they can protect against identity theft and other forms of fraud. I have included a sample letter for your reference.

This cyberattack is an assault on our efforts in state government to provide quality services to Minnesotans in need. We pledge to do everything we can to uphold the privacy of the Minnesotans who receive services through our programs. We apologize for any concern or other negative impact due to this incident.

If you have any questions, don't hesitate to contact me.

Sincerely,



Tony Lourey
Commissioner

Enclosure

cc: Senators Warren Limmer and Ron Latz;
Representatives John Lesch and Peggy Scott

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

April 9, 2019

[INSERT NAME]
[INSERT ADDRESS 1]
[INSERT ADDRESS 2 – IF EXISTS]
[INSERT ADDRESS CITY, STATE, ZIPCODE]

Dear [INSERT FIRST & LAST NAME]:

Because the Minnesota Department of Human Services (DHS) respects and values the privacy of your personal information, we want you to know about a data security incident involving the compromise of the state email account of a DHS employee. We currently have no evidence that the information contained in this account was actually viewed, downloaded, or misused in any way. However, in an abundance of caution, we are providing you with this notice.

What happened? Minnesota's executive agencies, including DHS, are the frequent target of increasingly sophisticated cyberattacks. Partnering with Minnesota IT Services (MNIT), we have been able to successfully defend against the vast majority of these cyberattacks. Unfortunately, on or before March 26, 2018, a hacker was able to gain access to the state email account of an employee in the Direct Care and Treatment (DCT) administration of DHS. Once the hacker gained access to this account, the hacker pretended to be the DCT employee and sent two emails to one of the DCT employee's co-workers, asking this co-worker to pay an "invoice" via a wire transfer. The employees quickly recognized that these emails were suspicious, did not wire any money, and reported the emails to MNIT. It is possible that, while in the account, the hacker viewed or downloaded some of the account's contents.

What information was involved? The email account contained information about some people who have interacted with DCT, including you. Examples of the type of information found in the email account at the time it was compromised include: first and last names, dates of birth, contact information, other demographic data, treatment data, legal history data, and/or information about you or your family's interactions with DCT. This account did not contain your Social Security number or financial account information at the time it was compromised.

How did we respond to these data security incidents? MNIT is the information technology agency for all of Minnesota's executive branch, including DHS. Upon learning of this incident, MNIT immediately took steps to secure the email account. MNIT then investigated this incident, and told us about the results of its investigation on February 15, 2019. We also reported these incidents to the Federal Bureau of Investigation, the Minnesota Office of the Legislative Auditor, and the U.S. Department of Health and Human Services.

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 prevent and 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 email account, we suggest that you consider taking these steps to help protect against identity theft:

- 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 (Equifax, Experian, and TransUnion). You may request these reports online at www.annualcreditreport.com, by telephone at 877-322-8228, or by completing an Annual Credit Report Request Form (available from www.annualcreditreport.com) and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

- Place a fraud alert or credit freeze on your credit files by contacting Equifax, Experian, or TransUnion. More information about fraud alerts and credit freezes is available on the Federal Trade Commission's website (www.consumer.ftc.gov).

- Call the telephone number listed on the credit report or visit the Federal Trade Commission's website on identity theft at www.consumer.gov/idtheft/ if you see anything in your credit report that you do not understand.

- Check your credit report and other financial statements for any transactions or accounts that you do not recognize. If you find suspicious activity on your report or statements, contact your local police or sheriff's office to file a report.

Where can you get more information? If you have any questions or would like more information about this data security incident, please write, email, or call us:

Minnesota Department of Human Services
Anoka Metro Regional Treatment Center
ATTN: Health Information
3301 Seventh Avenue N.
Anoka, MN 55303

MN_DHS_DCTHealthInformation@state.mn.us

651-431-5020 or toll free 833-246-8262

We will also post information about this incident to our website (https://mn.gov/dhs/) and prepare a report about this incident. You may ask us to send you a copy of this report by writing, emailing, or calling us.

We sincerely regret this data security incident and apologize for any impact it may have on you or your family.

Sincerely,

Tony Lourey
Commissioner

651-431-3206

Attention. If you need free help interpreting this document, call the above number.

ያስተውሉ፡ ካለምንም ክፍያ ይህንን ዶኩመንት የሚተረጉምሎ አስተርጓሚ ከፈለጉ ከላይ ወደተጻፈው የስልክ ቁጥር ይደውሉ።

إم: أنلاحظة: اتصقذه الوثيه ةمرجتنية للاجم ةعداسم تدرا ى. الرقم أعلاهلع ل،ة

သတိ။ ဤစာရွက်စာတမ်းအားအခမဲ့ဘာသာပြန်ပေးခြင်း အကူအညီလိုအပ်ပါက၊ အထက်ပါဖုန်းနံပါတ်ကိုခေါ်ဆိုပါ။

កំណត់សំគាល់ ។ បើអ្នកត្រូវការជំនួយក្នុងការបកប្រែឯកសារនេះដោយឥតគិតថ្លៃ សូមហៅទូរស័ព្ទតាមលេខខាងលើ ។

請注意，如果您需要免費協助傳譯這份文件，請撥打上面的電話號碼。

Attention. Si vous avez besoin d'une aide gratuite pour interpréter le présent document, veuillez appeler au numéro ci-dessus.

Thov ua twb zoo nyeem. Yog hais tias koj xav tau kev pab txhais lus rau tsab ntaub ntawv no pub dawb, ces hu rau tus najnpawb xov tooj saum toj no.

ဟ်သူဉ်ဟ်သးဘဉ်တက့်. ဖဲနမ့်လိဉ်ဘဉ်တ်မၤစၢၤကလီလၢတ်ကကျိးထံဝဲဒဉ်လ်ာ တိလံာ်မိတခါအံၤန္ဉ်,ကိးဘဉ်လီတဲစိနိ််ဂ်ၢ်လၢထးအံၤန္ဉ်တက့်. 알려드립니다. 이 문서에 대한 이해를 돕기 위해 무료로 제공되는 도움을 받으시려면 위의 전화번호로 연락하십시오.

ໂປຣດຊາບ. ຖ້າຫາກ ທ່ານຕ້ອງການການຊ່ວຍເຫຼືອໃນການແປເອກະສານນີ້ຟຣີ, ຈົ່ງໂທຣໄປທີ່ໝາຍເລກຂ້າງເທິງນີ້.

Hubachiisa. Dokumentiin kun tola akka siif hiikamu gargaarsa hoo feete, lakkoobsa gubbatti kenname bilbili.

Внимание: если вам нужна бесплатная помощь в устном переводе данного документа, позвоните по указанному выше телефону.

Digniin. Haddii aad u baahantahay caawimaad lacag-la'aan ah ee tarjumaadda qoraalkan, lambarka kore wac.

Atención. Si desea recibir asistencia gratuita para interpretar este documento, llame al número indicado arriba.

Chú ý. Nếu quý vị cần được giúp đỡ dịch tài liệu này miễn phí, xin gọi số bên trên.

LB2 (8-16)

ADA Advisory

For accessible formats of this information or assistance with additional equal access to human services, write to MN_DHS_DCTHealthInformation@state.mn.us, call 651-431-3206, or use your preferred relay service. ADA1 (2-18)