RAMSEY COUNTY
County Manager's Office

September 17, 2019

Re: Notification of Security Incident

To whom it may concern:

We are writing to let you know about an information security incident that could potentially affect the confidentiality of your personal information. Please be assured that we have taken steps to address this incident. We want to be as transparent as we can about this incident and share what additional steps you can take to guard against potential fraud and identity theft.

Background
On or about August 9, 2018, Ramsey County became aware that an attack had occurred against county information systems (the "attack"). The attack attempted to take control of the email accounts of 26 county employees, including some working in the Social Services Department. The perpetrators tried to divert paychecks of several employees. The county stopped the attack the same day, secured the affected email accounts, and implemented additional security safeguards in its system to secure all employee email accounts. The county also notified law enforcement of the attack that day.

The county retained an external forensics firm to assist in investigating the attack. Following the completion of the firm's work, the county began issuing notifications to individuals served by the Social Services Department whose information may have been exposed.

Several of the employees provide services to multiple departments within the county, which made it difficult to fully evaluate all the information in their email accounts. The county retained a document review firm to assist with this work. In the course of this work, on or about May 21, 2019, the county learned that limited amounts of health-related information were contained in one employee's email account as part of administrative services the county provides to the Minnesota Department of Human Services (the "Department"). These administrative services are in support of the Department's Child & Teen Checkup program (the "Program"). The county and Department have worked together on identifying persons whose information may have been exposed. The county confirmed on or about July 19, 2019 that limited amounts of your information may have been in the email account that was attacked. In the months following the attack, the county has not observed any indications that the attackers had an interest in the exposed data beyond targeting county employees in the scheme to steal their paychecks.

What information may have been accessed?
The email account contained spreadsheets, as well as attachments related to Program appointments. The health-related information in those materials consisted of names, addresses, dates of birth, and other identifiers of some Program participants, such as Woman, Infant, and Children ("WIC") identification numbers, appointment dates and appointment types, patient master index numbers, household identification numbers, along with names of authorized representatives. The county does not know whether any of this information was actually viewed during the attack. No social security numbers, financial or credit card information, prescription or diagnosis information was exposed. The email account of the employee at issue was secured, along with all the others, the very same day the attack occurred.

250 Courthouse
15 West Kellogg Blvd.
Saint Paul, MN 55102
Phone: (651) 266-8000
www.ramseycounty.us

What are we doing to protect your information?
In the immediate aftermath of the attack the county set up an incident response team to address and mitigate its consequences. The county took several other steps as well, including adopting more robust password protections, implementing a host of new technical security measures, improved training, and implementing additional data security software, among others measures. The county is also revamping its email retention procedures. In addition to law enforcement, the county has also informed the State Auditor and federal Office for Civil Rights of the attack.

What can you do to protect yourself?
As noted above, there was no financial information contained in the email account. However, to help reduce the risk of identity theft, as an ongoing best practice, we recommend carefully and regularly reviewing your credit reports, credit card statements and other financial account information. If you find any unauthorized or suspicious activity, you should contact your credit card company or financial institution immediately. You also should promptly report any fraudulent activity or suspected incidents of identity theft to law enforcement, your state attorney general, and/or the Federal Trade Commission.

We also recommend that you consider placing a fraud alert on your credit files. A fraud alert requires potential creditors to use reasonable policies and procedures to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days and is available at no charge to you. To place a fraud alert on your credit files, contact one of the following three credit reporting agencies:

Experian	**Equifax**	**TransUnion**
P.O. Box 4500	P.O. Box 105069	P.O. Box 2000
Allen, TX 75013	Atlanta, GA 30348-5069	Chester, PA 19016
1-888-397-3742	1-800-525-6285	1-800-680-7289
www.experian.com	www.equifax.com	www.transunion.com

Each credit reporting agency is required to notify the others when it receives a fraud alert. You will receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report. When you receive your credit reports, look them over carefully. Look for accounts you did not open, inquiries from creditors you did not initiate and for personal information, such as a home address or social security number, that is not accurate. If you see anything that you do not understand, call the credit reporting agency at the telephone number on the report. You can keep the fraud alert in place by calling again after 90 days.

If you find suspicious activity on your credit reports or other financial documents, call your local police or sheriff's office and file a police report of identity theft. We would suggest obtaining a copy of the police report as you may need to give copies to creditors to clear up your records. Even if you do not find any signs of fraud on your reports, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports periodically.

The county will prepare a report of its investigation into this attack once the county's investigation is complete. You may access the report at www.ramseycounty.us, or request a report by sending an email to datarequests@ramseycounty.us or by sending a written request to 90 W. Plato Blvd, attn. Data Requests, St. Paul, MN 55107. We sincerely apologize for any inconvenience this security incident may cause you. Should you have further questions about this matter, please contact us at **1-833-812-4159 or 651-266-2275** between 8:00 a.m. and 4:30 p.m. Monday through Friday.

Sincerely,

Ryan T. O'Connor, County Manager