

December 20, 2019

[Name]
[Address]
[Address]

Re: Notification of Security Incident

Dear Sir or Madam,

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, and that we are committed to fully protecting all of the information you have entrusted to us. 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, the Ramsey County Information Services Department (the “IS Department”) became aware that an attack had occurred against county information systems. The attack attempted to take control of email accounts used by approximately 28 Ramsey County employees who work or worked in eleven different county departments. After initial investigation, the county found that the perpetrators of the attack tried to divert paychecks for several of these county 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.

What information may have been accessed?

It appears that the attackers were trying to steal paychecks from county employees. Because the attackers obtained access to the email accounts of county employees, the attackers may have been able to see other information included in those accounts. Due to county employees using email for communications related to a range of county functions, the attackers may have been able to access the names, addresses, social security numbers or other personally identifiable information of individuals whose data is maintained by the county. Your information may have been visible to the attackers.

What we are doing to protect your information?

Ramsey County acted quickly to address the issue. On August 9, 2018, the county issued an alert to all employees describing the attack, warning them to be vigilant and that all passwords would be reset that day. Employees were required to change and strengthen their log-in passwords. The majority of county passwords were reset by 4:45 p.m. that day.

The county hired data forensics firms to assist in investigating the incident. Those firms’ assessment indicates that your information may have been exposed to the attackers.

In addition to addressing the immediate issue, the county has adopted further safeguards going forward. For example, the county has implemented multifactor authentication for greater network security and a password strength tool. The county has also increased user education for all employees and purchased data security software that provides enhanced auditing and monitoring capabilities. In addition to law enforcement, the county has also informed the Minnesota State Auditor of the attack.

What you can do to protect yourself.

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 any suspected incidents of identity theft to proper law enforcement authorities, 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

P.O. Box 9530
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
1-800-525-6285
www.equifax.com

TransUnion

P.O. Box 6790
Fullerton, CA 92834
1-800-680-7289
www.transunion.com

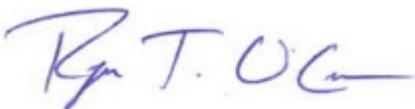
Each credit reporting agency is required to notify the others when it receives a fraud alert. You will receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report. When you receive your credit reports, look them over carefully. Look for 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 will be able to 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 **651-266-2275** or 1-833-812-4159 between 8 a.m. and 4:30 p.m. Monday through Friday.

Sincerely,



Ryan T. O'Connor, County Manager

