

January 29, 2021

[Name]

c/o Parent or Guardian (if minor child)

[Address]

[Address]

Re: Notification of Security Incident

To whom it may concern:

We are writing to let you know about a security incident that occurred at Netgain Technology, LLC ("Netgain"). Netgain provides technology services to Ramsey County and other companies. The security incident may have resulted in the possibility of unauthorized access to your personal information. Please be assured that we have taken steps to address this incident. We want to be as transparent as possible and share what additional steps you can take to guard against potential fraud and identity theft.

Background

On Dec. 2, 2020, Netgain notified Ramsey County that it had experienced a security incident by a malicious outside hacker. We learned that the hacker was seeking to extort payment from Netgain. This practice is often called "ransomware." The hacker's actions suggest it was not ultimately seeking personal information of Ramsey County clients but was instead looking to extort payment.

What information may have been accessed?

Netgain determined that the ransomware incident affected data within an application used by Ramsey County's Family Health Division to document home visits. **Please know that the hacker may not have accessed your information, but we are notifying you out of an abundance of caution and in compliance with federal law.** The following types of information may have been exposed in the incident: name, addresses, dates of birth, dates of service, telephone numbers, account numbers, health insurance information, and medical information. For a small number of individuals, it may also include Social Security number.

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 the consequences. The county immediately stopped using Netgain's services and switched to backup processes. Law enforcement and the federal Office for Civil Rights were notified of the incident. We also consulted with other local governments that were impacted.

What can you do to protect yourself?

Although there was no financial information exposed in the breach, to help reduce the risk of identity theft, 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 the following three credit reporting agencies:

Experian

P.O. Box 4500
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

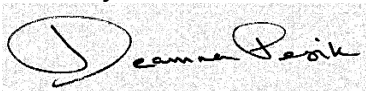
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

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, as an ongoing best practice, 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 and once it is complete, it will be posted to www.ramseycounty.us/publicnotice. You may also request a report by sending an email to datarequests@ramseycounty.us or a written request to 15 W. Kellogg Ave. #250, 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 (toll free) or 651-266-2275** between 8 a.m. and 4:30 p.m. Monday through Friday.

Sincerely,



Deanna Pesik
Chief Compliance & Ethics Officer