Minnesota Statutes, Section 13.055 Investigation Report

September 17, 2019

The data in this report is **public** under Minnesota Statutes, section 13.02, subdivision 19, and Minnesota Statutes, section 13.43, subdivision 2(a)(5).

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

Minn. Stat. § 13.055, subd. 2(b) Investigation Report
September 17, 2019

Minnesota Statutes, section 13.055, subdivision 2(b) requires government entities, including Ramsey County (the "County"), to "prepare a report on the facts and results of the investigation" into "any breach in the security of data". Pursuant to this statute, this report must, at a minimum, contain the following information:

(1) "a description of the type of data that were accessed or acquired";

(2) "the number of individuals whose data was improperly accessed or acquired";

(3) "if there has been final disposition of disciplinary action for purposes of [Minnesota Statutes,] section 13.43, the name of the employee determined to be responsible for the unauthorized access or acquisition, unless the employee was performing duties under [Minnesota Statutes,] chapter 5B"; and

(4) "the final disposition of any disciplinary action taken against each employee in response".

A breach in the security of the data held by the County occurred on or about August 9, 2018, when 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 information of approximately 113,265 individuals may have been in the email account at issue. The County notified these individuals on or about September 17th, 2019. 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.

I. A description of the type of data that were accessed or acquired

The email account that contained information relevant to the Program 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

The FBI is aware of this incident, and is solely responsible for any related investigation that it may choose to conduct.

II. The number of individuals whose data was improperly accessed or acquired

Data about approximately 113,265 individuals was in the email account at the time it was compromised.

The County mailed letters to each of these individuals on or about September 17, 2019. On this same day, the County provided information about these data security incidents to the media, the Office of Civil Rights, and posted a notice to its webpage (https://www.ramseycounty.us/your-government/open-government/public-notices). This notice includes a link to the notification letter. The Minnesota Office of the Legislative Auditor was also notified of the incident by the Department.

III. If there has been a final disposition of disciplinary action for purposes of section 13.43, the name of each employee determined to be responsible for the unauthorized access or acquisition, unless the employee was performing duties under chapter 5B

The County did not find that the County employee whose email account was compromised was negligent or otherwise at fault for these data security incidents. Accordingly, the County did not impose any discipline on this employee.

The County continues to educate all of its employees about detecting and reporting suspicious emails and links, and email best practices.

IV. The final disposition of any disciplinary action taken against employee in response

N/A