Iowa Department of Human Services

Kim Reynolds
Governor

Adam Gregg
Lt. Governor

Jerry R. Foxhoven
Director

October 23, 2017

The Honorable Tom Miller
Attorney General of Iowa
Consumer Protection Division
Security Breach Notification
Hoover State Office Building
1305 E. Walnut St.
Des Moines, IA 50319

Dear Attorney General Miller:

Pursuant to Iowa Code Chapter 715C, I am writing to inform you of a data breach that occurred within the Department of Human Services involving the personal information of 710 individuals. Those affected by this data breach includes both adults and minor children including current and former recipients of services from the Department, private citizens who made inquiries to the Department, individuals working under contract with the Department and federal employees conducting mandated reviews of recipient case information. Information in the emails that may have been accessed includes name, social security number, bank account number, and driver's license number.

On August 23, 2017, the Department was the target of a phishing email campaign. The hackers masked their identities and sent very carefully designed phishing emails to Department employees that appeared to have come from other trusted Department employees. As a result, nine employees provided their passwords which gave the hackers access to their email accounts.

The same day the first employee provided her password, the phishing email campaign was identified. All nine employees that provided their passwords changed them as soon as they were identified. All employees were immediately notified of the phishing email campaign to prevent the hackers from obtaining additional passwords and accessing additional employee email accounts.

The Department immediately took action to identify the steps needed to determine the scope of the breach and to minimize the impact to the affected individuals. Because a large number of Department emails containing confidential information are encrypted, the Department was able to eliminate the encrypted emails from the scope of this breach. As a security measure, a small number of confidential Department employees reviewed all unencrypted emails that may have been accessed and viewed to determine the individuals whose confidential information was exposed.

At this time, the Department does not have evidence to indicate the hackers actually accessed any of the exposed emails. Breach notification letters were mailed to the affected individuals on October 20, 2017. The letters include an explanation of the breach, the possible impact to them, actions the Department took, types of information included in the emails, and actions the individuals may take.

While the chance these individuals' personal information will be misused is small, the Department is providing 12 months of credit monitoring through TransUnion Interactive at no charge. The enrollment period is from October 23, 2017 through January 31, 2018. To obtain enrollment instructions, individuals need to call the Iowa Concern Hotline at 1-800-447-1985. This hotline is available Monday through Friday between the hours of 8:00 AM and 8:00 PM through January 31, 2018, excluding federal and state holidays.

This service provides one year of unlimited access to the individual's TransUnion credit report and credit score. Through TransUnion's daily credit monitoring services, individuals will be notified if there are critical changes to their credit file at TransUnion including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. This service also includes up to $1,000,000 in identity theft insurance with no deductible (subject to applicable policy limitations and exclusions).

For affected minors for whom the credit monitoring services do not apply, parents and legal guardians can call the Iowa Concern Hotline to obtain instructions regarding TransUnion's secure services to determine if their child may be a victim of identity theft.

Affected individuals were also provided additional steps they may take if they believe their identity has been stolen. This includes contacting local law enforcement, accessing information on relevant websites including the Attorney General's website, and contacting the Attorney General's Consumer Protection Division by phone, email or regular mail. All contact information is included in the letter.

Because phishing emails are often sent to government agencies, the Department takes a number of steps to continually educate staff on how to recognize and report phishing emails and to protect their usernames and passwords. Information on encrypting all emails that contain confidential information is being sent to all Department employees. The Department is also implementing technological controls to prevent a hacker from accessing email accounts by obtaining a user's password.

In addition, all employees are required to sign an annual confidentiality statement and complete annual confidentiality training which includes detailed information about phishing emails and password protection. The nine employees who inadvertently provided their passwords when they received the phishing email were required to re-take the confidentiality training sessions.

If you have any questions, please do not hesitate to contact me at 515-281-5452 or at jfoxhov@dhs.state.ia.us.

Sincerely,

Jerry R. Foxhoven, Director
Department of Human Services