

## Frequently Asked Questions

### 1) **What happened?**

On December 14, 2023, Coleman Professional Services, Inc. learned that an unauthorized user gained access to a few of our employees' email accounts that contained personal information. Based on our investigation, we learned that unauthorized connections were made to the email accounts between September 18, 2023 and October 31, 2023. We were unable to confirm whether any specific emails or attachments stored within those affected accounts were viewed or acquired as a result of this incident. Out of an abundance of caution, emails stored in the affected email accounts were reviewed to determine whether any of those emails contained personal information.

### 2) **When did Coleman become aware of this incident?**

We learned on December 14, 2023, that unauthorized connections were made to a limited number of Coleman email accounts that contained personal information.

### 3) **What information was involved?**

Unauthorized connections were made to a limited number of Coleman email accounts. The type of personal information involved depended on the personal information that was present in an affected email account. Notification letters were mailed to individuals whose personal information was present in an affected email account during the relevant timeframe. The notification letters identify the types of personal information involved.

### 4) **What is Coleman doing as a result of this incident?**

As soon as we learned of this situation, we immediately launched an investigation. We took steps to block unauthorized users from connecting to the affected email accounts, reset the relevant passwords, reviewed the contents of the documents in the email accounts to determine whether they contained personal information, and took additional measures to prevent unauthorized users from accessing employees' email accounts in the future. Additionally, as a precaution, enrollment information has been mailed to those individuals whose Social Security Numbers were present in an affected email account during the relevant time frame.

### 5) **Has my personal information been misused?**

At this time, we have no evidence that there has been any misuse of personal information as a result of this incident.

### 6) **Tell me more about the identity protection services you are offering.**

Out of an abundance of caution, we are providing identity theft protection services through Kroll at no cost to those individuals whose Social Security Numbers were present in an affected email account during the relevant time frame. Enrollment instructions and information about the services were included in the letter mailed to those individuals. The

identity theft protection services include single bureau credit monitoring, fraud consultation with a Kroll fraud specialist, and identity theft restoration through an experienced Kroll licensed investigator. If your letter did not include identity theft protection services, your Social Security Number was not involved in the incident.

**7) Will my bank or credit card company re-issue a new payment card to me because of this incident?**

Each bank or credit card company determines on its own whether to re-issue new cards based on the company's policies and procedures. If you have any questions, we recommend that you call the telephone number on the back of the card.

**8) I believe I have a fraudulent charge on my credit card, how can you assist me?**

Typically, as long as you report any suspicious activity to your credit card company in a timely manner, you will not be responsible for any fraudulent charges. If you have not already done so, you should report any suspicious activity to the credit card company or bank that issued your card immediately.