Did You Suffer A Data Breach Under Colorado Law? The Answer May Surprise You

Insights
2.02.21

If someone accessed your business's computer systems without your authorization, did you suffer a data breach under Colorado law? Answering this question correctly is critical, because getting it wrong can expose you to government investigations and lawsuits. It may surprise you to learn that the answer to this question is not always a clear yes. You may be wondering how you can determine if the answer is probably no. If you are wondering, keep reading.

Colorado Data Breach Notice Law

Colorado's notice of security breach statute is part of the Colorado Consumer Protection Act. You must comply with the statute if you are considered a "covered entity" as defined by the statute. A covered entity is any individual, corporation, business trust, estate, trust, partnership, unincorporated association, or two or more thereof having a joint or common interest, or any other legal or commercial entity that "maintains, owns, or licenses **personal information** in the course of the person's business, vocation, or occupation."

Here is how Colorado's security breach statute defines "personal information."

- A Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable; Social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data;
- A Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; or
- A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

The statute goes on to say that "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

Under the statute, a "security breach," which is a synonym for a data breach, means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity." But it's important to take note of the following important exception: "Good faith acquisition of personal information by an employee or agent of a covered entity for the covered entity's business purposes is not a security breach if the personal information is not used for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure."

So When Is The Answer Probably No?

Getting back to the original questions posed at the outset of this publication, your organization probably did not suffer a security breach, *unless* all of the following statements are correct:

- you are a covered entity and you conclude there is sufficient evidence that someone accessed your computer systems without your authorization;
- after accessing (i.e. hacking) your systems, they acquired unencrypted computerized data that is considered "personal information" under Colorado law;
- no federal, state, or local government records or media made that data available to the general public;
- you conclude that the security, confidentiality, or integrity of that personal information was compromised and is subject to further unauthorized disclosure because the person who acquired the personal information was not one of your employees or agents acting in good faith; **and**
- that person might intend to use the personal information for unlawful purposes.

When Is The Answer Probably Yes?

There are three scenarios you should watch for if you're unable to confirm that you did not suffer a data breach after you discover someone accessed your computer systems without authorization.

SCENARIO 1

If you are a covered entity and your answers to all these questions are yes, then you probably suffered a security breach.

1. Is there evidence that someone accessed your computer systems without authorization or in excess of their authorization for purposes unrelated to the corporate mission?
2. Was the information the person accessed unencrypted?
3. Is there evidence that the person who accessed the computer system gained access to any sets of data that contain a Colorado consumer's or employee's (a) first name, (b) last name, and (c) at least one of the following other data elements: Social Security Number; Student, Military, or

least one of the following other data elements: Social Security Number; Student, Military, or Passport Identification Number; Driver's License Number or Identification Card Number; Medical Information; Health Insurance Identification Number; or Biometric Data?

SCENARIO 2

If you are a covered entity and your answers to all these questions are yes, then you probably suffered a security breach.

1. Is there evidence that someone accessed your computer systems without authorization or in excess of their authorization for purposes unrelated to the corporate mission?
2. Was the information the person accessed unencrypted?
3. Is there evidence that the person who accessed the computer system gained access to any sets of data that contain a Colorado consumer's or employee's (a) email account address and (b) the password that would enable the person to gain access to that email account?

SCENARIO 3

If you are a covered entity and your answers to all these questions are yes, then you probably suffered a security breach.

1. Is there evidence that someone accessed your computer systems without authorization or in excess of their authorization for purposes unrelated to the corporate mission?
2. Was the information the person accessed unencrypted?
3. Is there evidence that the person who accessed the computer system gained access to any sets of data that contain a Colorado consumer's or employee's (a) account number or credit or debit card number and (b) any required security code, access code, or password that would permit access to that account?

What's Next?

If you conclude that you probably suffered a security breach under Colorado law, you will probably also conclude that, to comply with the state's security breach notice law, you need to send notices of that breach to the affected Colorado residents in the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determination that a security breach occurred.

For further information, contact your Fisher Phillips attorney, the author, any attorney in our Denver office, or any member of our Privacy and Cyber Practice Group.

Service Focus

Privacy and Cyber

Related Offices

Denver