CASE STUDY ONE:
IMPORTANCE OF ENCRYPTION AND PHYSICAL SAFEGUARDS

A client selected a claims processor in a different state. As part of the onboarding process with the new vendor, the client sent a flash drive containing personal information to the vendor via a national carrier. When the envelope arrived at the destination, the envelope was empty – the flash drive was missing. Our client now had a security breach on their hands. But, what happens next?

Under Wisconsin law, potentially impacted individuals are notified only if there is a material risk of identity theft or fraud. Therefore, we needed to analyze whether there was a material risk that unauthorized access to the data would result in identity theft or fraud.

We determined the flash drive was neither encrypted or password protected. We contacted the national carrier and learned when the mail sorter processes envelopes containing "bulky" items such as flash drives, they are frequently caught in the sorter and ripped out of the envelope. The carrier could attest its policy is to safely dispose of flash drives discovered at the facility.

We determined that although there was a security breach event, there was no material risk of identity theft or fraud. However, at this point, thousands of dollars had been spent on the investigation and analysis.

TIP:

Implement proper physical safeguards when shipping items containing personal information and take measures to encrypt data.

Ruder 100 Ware
SINCE 1920
BUSINESS ATTORNEYS FOR BUSINESS SUCCESS®
wausau | eau claire | green bay ruderware.com
visit our blogs at *blueinklaw.com*

CASE STUDY TWO:
DUAL VERIFICATION METHODS, PHISHING, AND EMPLOYEE TRAINING

Client indicates they were contacted via e-mail by their Indonesian supplier requesting to modify payment destination for the most recent shipment of goods. They proceed with the request. Two weeks later, the vendor contacts client and indicates payment is past due. Client proceeds to explain they have already paid, but vendor indicates they never received it. Client has fallen victim to a phishing attack.

TIP:

Train employees on recognizing phishing attempts. Furthermore, having dual verification methods in place when receiving new payment instructions is crucial (for example, an email followed up by a phone call).