

Case Study

Issue:

Disclosure of customers' payment card information

Summary:

After its incident detection and response system indicated that a large amount of data had been exported from two of its servers, a travel, hotel, and entertainment reservation business based in Chicago determined that the exported data included 475,000 sets of Visa, MasterCard, and American Express payment card numbers, CVV2 codes, and customer information. The data were not encrypted and the company has not yet determined why the information had been stored. Initial reports from in-house IT staff indicate the data were sent from the company's server farms in Washington State and North Carolina to an IP address in Russia.

The company's IT director had been advised during an audit undertaken to comply with the Payment Card Industry Data Security Standard that the payment processing system of an entity that the company bought was configured to store unencrypted payment card data. The IT Director had requested budget approval to replace the acquired business's legacy system and the funds had been approved for next year's budget.

Initial actions taken by the company:

- After conferring with his boss and with the company's Privacy Officer, the company's IT director hires a forensic investigator to determine how the penetration occurred and what data were stolen.
- The investigator determines that, in addition to inappropriately storing payment card data, the Internet-facing servers of the acquired business had not had several security patches installed in the months before or after the business was purchased.
- Hackers had penetrated the servers of the acquired business, then gained access through the company's network to other company servers, where the hackers installed software that captured payment card data sets, CVV2 codes, and other customer data in transit.
- Stolen data were apparently stored on several company servers for weeks as data were accumulated, then the information was exported in compressed, encrypted files 10 days ago.
- The investigator is not certain that he has identified all of the data sets that were exported. The 475,000 sets of data he has identified were of customers from each of the 50 United States and from several non-U.S. countries including Canada, the EU, Norway, Japan, Hungary, Australia, and New Zealand.
- No company official has been notified by customers, banks, or payment card associations that fraudulent charges have been traced to the theft from the company. The CEO presumes this means that, at least so far, the stolen data have not been used for fraudulent purposes.
- The company's IT director and his staff have compiled a list of the names, addresses, and email addresses (where they have them) of the 475,000 known customers whose card and personal information has been stolen.

- The company's Privacy Officer has recommended that the company hire an outside firm:
 1. to send the notices to the customers whose data the company knows was stolen;
 2. to craft FAQs on the company's website;
 3. to staff a call-in center to answer customer's questions about the theft; and
 4. to offer one-year's credit monitoring to any customer among those notified who requests it.
- The CEO is uncertain whether the company should hire the firm recommended by the Privacy Officer or even whether it should notify customers – or anyone else – unless the company receives reports that the stolen information has been misused.
- The CEO has asked the company's HR director to investigate whether the IT director or any other company employee should be disciplined for any actions or failures to act that contributed to the theft.

Questions:

- Should the company implement the Privacy Officer's recommendation to hire the outside firm to send the notices and to take the other actions?
 - What legal requirements and other issues should be considered in making this decision?
- Should the company notify anyone other than the customers whose card information was stolen of the theft?
- Was the CEO's conclusion about the lack of fraud related to the theft, at least so far, reasonable?
- Were the responses the company took and is considering sufficient to respond to the breach?
 - If not, what additional steps should it have taken or should it take now?
- Was it reasonable to address the security of the acquired businesses IT systems in the way the company did?
 - If not, what additional or different steps should the company have taken?
- Did the company appear to be adequately prepared to respond to the data breach?
 - If not, what additional steps should the company have taken before the breach occurred?
- Was it reasonable for the CEO to ask the HR director to investigate whether discipline should be imposed?