Recent Data Security Breaches Involving Third-Party Vendors

Cogent Healthcare

[Breach reported August 2013]

"Vendor Mistake Causes Breach of 32,000 Patients' Data"

A medical transcription vendor that was engaged to transcribe physician care notes suffered a security lapse when patient data was inadvertently stored insecurely on a publically accessible website. The data was from 32,000 patients.

Target

[Breach reported December 2013]

"HVAC Vendor Confirms Link to Target Data Breach"

Hackers gained entry into Target's network via stolen credentials from a third-party HVAC vendor, which had an external connection with Target for electronic billing, contract subsmission, and project management. As a result, around 40 million credit and debit card accounts were stolen.

Lowe's

[Breach reported May 2014]

"Vendor Error Forces Lowe's to Issue Breach Notification Letters"

A driver safety firm suffered a breach when it unintentionally backed up data to an unsecured internet-facing server, exposing personal information of current and former Lowe's drivers. The potentially exposed information included names, addresses, dates of birth, SSNs, driver's license numbers, and other driving record information.

Goodwill Industries

[Breach reported July 2014]

"Goodwill Names Vendor in Breach"

Goodwill suffered a data breach in about 330 outlets after hackers compromised the system of a third-party vendor that deployed cloud-based card processing services for retailers. As a result, data from 868,000 payment card accounts was stolen.

Dairy Queen and TacoTime

[Breach reported July 2014]

"POS Vendor: Possible Restaurant Breach"

A point-of-sale and data security vendor suffered a breach of its corporate LogMeIn account credentials, potentially exposing payment card data from its client businesses.

Home Depot

[Breach reported September 2014]

"Home Depot Hackers Used Vendor Log-on to Steal Data, E-mails"

Hackers used stolen credentials from a third-party vendor to gain access to Home Depot's network, where they purportedly exploited an unpatched vulnerability in the system to gain access to point-of-sale data. As a result, around 56 million payment cards accounts and 53 million email addresses were stolen.

Department of Veterans Affairs

[Breach reported November 2014]

"Vendor Breach Exposes PII of More than 7,000 Vets"

A third-party home telehealth vendor for the Department of Veterans Affairs disclosed a potential security breach of a database that affected the personal information of at least 7,000 VA patients. The personal information included name, address, date of birth, phone number and VA patient ID number.

Zoup

[Breach reported March 2015]

"POS Vendor Investigates Breach"

A point-of-sale provider for food service establishments reported a breach that exposed payment card data for customers that used cards at the Zoup restaurant chain.

Recent Data Security Breaches Involving Third-Party Vendors

AT&T Services, Inc.

[FCC Settlement announced April 2015]

"AT&T Breach by Vendor Awakens New Insider Threat Concerns"

Employees of an AT&T service provider violated privacy guidelines by accessing, without authorization, consumer accounts as part of a scheme to obtain customer names and partial SSNs, which were allegedly used to request unlock codes for stolen mobile phones. As a result of the breach, AT&T agreed to settle an FCC investigation and pay a $25 million fine.

Harbortouch

[Breach reported May 2015]

"Big Credit Card Data Breach Hits Bars and Restaurants Using Harbortouch Point-of-Sale Systems"

Harbortouch, a point-of-sale vendor, announced a breach affecting a small percentage of its restaurant and bar clients that involved malware that extracted payment card data from the affected establishments.

Clif Family (and other wineries)

[Breach reported June 2015]

"Data Breach at Missing Link Leaves Several Vineyards with Taste of Plonk"

An IT service provider that specialized in offering infrastructure services to wineries suffered a breach of its consumer-direct sales platform that exposed payment card information from processed transactions.

Louisville Metro Government

[Breach reported July 2015]

"Data Breach Affects Lou. Metro Government Employees"

A third-party vendor that electronically stored employee medical records suffered a breach, which exposed the names, addresses and SSNs of more than 10,000 current and former Louisville Metro workers. The breach did not involve medical records.

Detroit Zoo

[Breach reported July 2015]

"Credit Card Data Breach Affects Gift Shops at Detroit Zoo"

A third-party vendor that operated retail gift shops at various zoos suffered a breach of payment card data caused by malware that scraped the data from its point-of-sale system. The breach did not affect payment card transactions for tickets and concessions, as those were processed via another system.

CVSphoto.com

[Breach reported July 2015]

"CVS Photo Breach Points to Third-Party Vendor"

A third-party vendor that managed online payments for and hosted CVS's online photo site suffered a breach of payment card data. Financial transactions that took place on CVS's main site (CVS.com) and in-store were not affected.

The California State University

[Breach reported September 2015]

"CSU: 79K Students Had Data Breached on Third-Party Website"

A vendor which administered a sexual assault training program for students at eight CSU campuses suffered an intrusion into its website servers. The breach, which exposed the personal data of 79,000 California State University students, included names, student ID numbers, student email addresses, mailing addresses, gender, and ethnicity, among other things.

Jimmy John's

[Breach reported September 2015]

"PoS Vendor Confirms Jimmy John's Breach Was Their Fault"

A point-of-sale vendor confirmed that a hacker gained entry to its systems and installed malware to capture payment card data from cards swiped at certain restaurants. The breach affected at least 216 stores from the nationwide sandwich chain.