Issued 7/7/17

Sabre Says Stolen Credentials Led to Breach

The travel agency in charge of hotel bookings for Google's employees has suffered a breach, with details such as names, contact details, and credit card information possibly exposed. Google has already issued a warning to the State of California and sent a letter to affected employees, explaining that Social Security numbers, passport, and driver's license information were not compromised.

The breach impacted a reservation system called Sabre Hospitality Solutions SynXis, which is also being used by Carlson Wagonlit Travel (CTW), a travel agency that makes hotel bookings for Google employees leaving on business trips. Sabre first learned about the breach in early May and started notifying customers shortly after that. More than 32,000 hotels worldwide are said to be using the reservation system. "Sabre notified CWT, which uses the SynXis CRS, that an unauthorised party gained access to personal information associated with certain hotel reservations made through CWT. CWT subsequently notified Google about the issue on June 16, 2017, and we have been working with CWT and Sabre to confirm which Google travelers were affected," Google explained in a letter submitted to affected employees.

“Sabre's investigation discovered no evidence that information such as Social Security, passport, and driver's licence numbers were accessed.

However, because the SynXis CRS deletes reservation details 60 days after the hotel stay, we are not able to confirm the specific information associated with every affected reservation.” Google goes on to explain that names, contact information and credit card details might have been exposed, revealing that hackers had access to the reservation system for several months between August 10, 2016 and March 9, 2017. Travel industry giant Sabre said Wednesday an intruder using stolen account credentials for its widely used reservations software had access to payment card details and personal information over a seven-month period. But it declined to say how many people are affected. Sabre, which is based in Southlake, Texas, disclosed in early May a suspected breach affecting its SynXis Central Reservations system.

The software-as-a-service system is used by travel agencies, hotels and booking services for such functions as rate and inventory management. The exposure period started in August 2016 and ran through March. The information at risk includes payment cardholder names, card numbers and expiration dates, Sabre says. For some reservations, the three-digit security code on the reverse of the card was exposed, but a "large percentage" of bookings were made without the code, the company says. Some bookings were made using virtual payment card numbers, it adds. Guest names, phone numbers, addresses and other information were at risk, but not Social Security, driver's license or passport numbers, according to Sabre.

Sabre did not give a figure for how many payment cards or individuals were affected. Sabre spokesman Tim Enstice tells Information Security

Media Group that "less than 15 percent of the average daily bookings" using the reservation system were viewed. Enstice declined to answer how many daily bookings, on average, are made. But the SHS reservation system is used at 36,000 locations, from small hotels to large global chains, as well as for property management. If each location only made one booking a day, the number of transactions would exceed 1 million in a month. At the bare minimum, 15 percent exposure would mean 150,000 transactions a month would be at risk. Enstice disputed that estimate, saying it was "pure speculation." But Computerworld reported in August 2015 that Sabre's various software systems processes 2 billion transactions per day affecting 1 billion travelers a year.

Sabre says it has contacted travel management companies and travel agencies that do not use SHS reservations software, as well as those that do. "We have engaged Epiq Systems to provide complimentary notice support for those customers that determine they have a notification obligation," Sabre says. The breach is at least the second cybersecurity incident for Sabre in as many years. In an Aug 4, 2015, filing with the U.S. Securities and Exchange Commission, Sabre said it was investigating a "cybersecurity incident involving several servers managed by a third party." Bloomberg reported a month later that investigators believed hackers linked with China attacked Sabre as well as American Airlines.

The hacking group was suspected to be the same one that struck health insurer Anthem and the U.S. government's personnel office. In February 2016, Sabre said it concluded its investigation, writing in its annual report that it found "no loss of traveler data, including no unauthorized access to or acquisition of sensitive protected