Travel-booking site Orbitz confirmed that it has suffered a major data security breach, in which details of up to 880,000 credit cards were compromised.

In an official notice, Orbitz said that an attacker potentially accessed personal information from purchases made between 1 January 2016 and 22 June 2016 against customers using the Orbitz consumer platform, and between 1 January 2016 and 22 December 2017 against partner travel sites which use Orbitz as their booking engine, such as Amextravel.com (owned by American Express). Information accessed included customers’ full names, payment card information, date of birth, phone number, email address, physical and/or billing address and gender. Orbitz did not find evidence that passport and travel itinerary information and Social Security numbers were involved in the incident.

The attack, which is believed to have taken place in October – December 2017, was not discovered until 1 March 2018, during an investigation of a legacy Orbitz travel booking platform. Orbitz claimed that its current website, Orbitz.com, has not been affected.

Travel company Expedia Inc. bought Orbitz in September 2015. The breach may have arisen from a failure to update or integrate legacy IT systems and infrastructure as part of the acquisition, since the current Orbitz.com website was unaffected. Legacy IT systems are a major risk to cyber security, since they often go unmonitored without regular updates and patches, making them a common attack point for hackers.

Orbitz is offering affected customers a complimentary credit monitoring and identity protection service for 12 months. However this attack highlights the vulnerability of legacy IT systems, and the importance for companies to maintain strong cyber security practices and updated IT systems. We have seen a number of similar breaches occur amongst our clients.

Sarah Goegan also contributed to this post.

Copyright 2019 K & L Gates