www.investopedia.com /news/5-biggest-credit-card-data-hacks-history/

Equifax Hack: 5 Biggest Credit Card Data Breaches

Full Bio ⋮ 5-6 minutes

In 2016, just five years ago, the huge data breach, or the dark side of technology, was a spectacular cybercrime, with credit cards especially frightening to consumers and the media.

The landscape has changed since then, and the nature of what data is considered valuable info to hack or steal is also different. Data breaches hit a high watermark in 2016, according to James Lee, chief operating officer of Identity Theft Resource Center (ITRC), a San Diego nonprofit that gives guidance about identity compromise and crime.1 Now they seem to be on the decrease, according to the firm's most recent report.

According to ITRC, the number of U.S. data breaches in 2020 totaled 1,108—a sharp 19% decrease from 2019, which saw 1,473 data breaches. Far fewer people were affected, too: 300 million, a 66% plunge from the year before.2 Before this slide in data breaches, a hack on credit bureau Equifax in September of 2017 exposed personal data of 143 million customers, including 209,000 credit card details.

"What's taken the place of the data breach is fraud," Lee said. People shouldn't let their guard down, because newer threats are quite risky, Lee says. "Less data is required, so you don't have these mass data breaches," Lee said. Cybercriminals are looking for specific kinds of information, such as passwords to steal resources from businesses and government agencies, such as Social Security.

Email addresses and passwords now have great value, Lee says. For this reason, password safety and password management now receive more attention. "The least valuable piece of information is the Social Security number," which sells for under $5 on the dark web. "Next would be credit cards," Lee said. It used to be quantity over quality, but now the reverse is true. Quality of data is important, because there are so many players in the cyber crime value game, and each gets a cut. One specialist identifies how to break into a system. Another does the actually breaking in. A third group extracts information, and a fourth group monetizes it. "Everyone along the chain gets paid," Lee said. "When they target an organization, they want to execute efficiently, get the money quickly, and move on.

Below is our analysis of some of the largest credit card breaches in the U.S.

1. 2019: Capital One (106 Million Customers Exposed)

Capital One, the fifth-largest credit card issuer in the Unites States, revealed in July 2019 that a hacker accessed the personal information of around 106 million customers and applicants in the U.S. and Canada. The information that was accessed included highly personal details on consumers and small businesses, including names, social security numbers, income and dates of birth as of the time they applied for one of several credit card products from 2005 through early 2019.

2. 2014: The Home Depot (56 Million Cards)

This 2014 attack on the do-it-yourself retailers was perpetrated through a "unique, custom-built malware" according to the Wall Street Journal. Fortune magazine reported that Home Depot (HD) ended up paying $25 million to banks, $134.5 million to card companies like Visa and MasterCard and $19.5 million to affected customers.

3. 2009: Heartland Systems (160 Million Cards)

A lone hacker broke into the systems of the payment processing company in 2009 and was later caught and jailed. In 2013, five people, including this hacker, were indicted for attacking a number of retailers, financial institutions and payment processing firms and stealing personal identification and credit/debit card data. The total mentioned in that indictment was 160 million cards. Other companies affected included Nasdaq, 7-Eleven, Carrefour, JC Penney, Hannaford, Wet Seal, Commidea, Dexia, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard.

4. 2006: TJX Companies (94 Million Cards)

The company that own retailers like TJMaxx and Marshall's (TJX) was a target of a cyber-attack in 2006, reported the Associated Press. While data for both Visa (V) and MasterCard (MA) credit cards was stolen, the AP reported that for Visa alone, the fraud related losses could be to the tune of $68 million to $83 million, spread across 13 countries. Consumer Affairs reported that the company ended up paying $41 million to Visa, $24 million to MasterCard and another $9.75 million in consumer protection settlement to 41 states.

5. 1984: TRW/Sears (90 Million Cards)

Almost 37 years ago, the New York Times reported that the password for a leading credit union TRW was stolen from a Sears (SHLD) store on the West Coast. That password unlocked the credit histories and personal information that could subsequently be used to obtain credit card numbers.