Zettaset

WHITE PAPER

The Biggest Financial Services Data Breaches and Their Impacts

The financial services industry has long been prone to cybersecurity breaches and data theft. However, technological advances and massive growth in the past decade have left this sector more vulnerable than ever to data breaches. According to an IBM report on security trends, organizations in this vertical are attacked 65 percent more often than any other industry.[1] Many data breach incidents involve insider leaks and unintended disclosure, but over 21 percent of data breaches are directly linked to hacking or malware.[2]

The 2016 Financial Industry Cybersecurity Report, conducted and compiled by SecurityScorecard, reports that 75 percent of the top 20 U.S. commercial banks are infected with malware, and that only one of the top 20 banks has a Network Security grade of "A."[3]

Let's take a look at the worst data breaches in the financial industry to date and their impact on both the target organization and the industry itself:

5. Heartland

In 2008, this New Jersey-based payment processing company was hit by a cyber attack that, at the time, was hailed as the largest data breach ever to affect an American company. Leveraging malware planted on Heartland's network, hackers gained access to over 134 million credit and debit cards and compromised more than 650 financial services companies.[4]

In the wake of the breach, Heartland was deemed no longer compliant with the Payment Card Industry Data Security Standard (PCI DSS), a requirement that allows organizations to process card payments. Since they were unable to be revalidated until May 2009, Heartland suffered lost revenue and in June reported a loss of $32 million associated with the intrusion.[5]

Two years after the incident, American hacker Albert Gonzalez was sentenced to 20 years in prison for his role in the Heartland data breach. Heartland eventually paid a total of $145 million to credit card companies to settle breach-related claims, and announced an end-to-end encryption security strategy going forward.

4. The Massive American Business Hack

The "Massive American Business Hack" gets its name from a series of data breaches in which cybercriminals targeted banks and companies. This event makes the list because of the sheer amount of time hackers were able to fly under the radar. Between 2005 and 2012, a span of nearly 8 years, a hacking group from Russia and Ukraine breached 800,000 American bank accounts and accessed information on over 160 million credit and debit card numbers.[6]

---

1 https://www.scmagazine.com/financial-services-sector-most-attacked-in-2016-ibm/article/653706/
2 https://documents.trendmicro.com/assets/wp/wp-analyzing-breaches-by-industry.pdf
3 https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf
4 http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/2.html?iid=EL
5 https://www.sec.gov/Archives/edgar/data/1144354/000119312509169191/d10q.htm
6 http://www.nydailynews.com/news/national/russians-ukrainian-charged-largest-hacking-spree-u-s-history-article-1.1408948

They then sold the sensitive information online and used it to withdraw money themselves. In total, organizations including Citibank, Nasdaq, and PNC Bank lost over $300 million as a result of the breach, with over $9 million coming from counterfeit ATM card withdrawals.[7] [8]

3. Court Ventures/Experian

Court Ventures experienced an atypical hack that compromised the personal data of over 200 million Americans in 2012. A Vietnamese hacker named Hieu Minh Ngo took advantage of a business acquisition by powerhouse credit bureau Experian by posing as a private investigator for Court Ventures in order to access Experian's data keys.[9] He then sold the stolen information (which included Social Security numbers, dates of birth, phone numbers, addresses, and more) on Superget.info as part of an identity theft service.

The data breach was investigated by the U.S. Senate Committee on Commerce, Science and Transportation, and Hieu Minh Ngo pleaded guilty to the attack. Personal records sold as a result of this breach led to $65 million in fraudulent income tax returns, which directly affected almost 14 thousand U.S. citizens.[10]

2. JPMorgan Chase

The 2014 JPMorgan Chase data breach targeted the well-known American bank, resulting in the exposure of names, email and postal addresses, and phone numbers of 83 million customers. Two out of every three U.S. households and over seven million small businesses were affected.[11] Social Security numbers and account login information were not compromised, but hackers could potentially use decrypted data in phishing attacks.[12]

The attack began when hackers stole a bank employee's credentials and took advantage of a network server that hadn't yet been upgraded to a dual password scheme. An extensive FBI investigation found a "massive criminal empire" run by Gery Shalon, an Israeli citizen, responsible for the breach.[13]

The fallout from the JPMorgan Chase hack was far-reaching. The bank faced a probe by the attorneys general of 19 states, spent months reassuring wary customers that no money had been taken, and announced it would spend upwards of $250 million each year in security improvement measures.[14]

---

7 http://insights.wired.com/profiles/blogs/8-infamous-data-breaches-that-help-build-our-collective-data
8 https://www.justice.gov/opa/pr/russian-national-admits-role-largest-known-data-breach-conspiracy-ever-prosecuted
9 http://vnetinc.com/blog/200-million-peoples-identities-compromised-in-one-scam/ https://krebsonsecurity.com/2015/07/experian-hit-with-class-action-over-id-theft-service/#more-31682
10 https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0
11 https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach
12 http://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges/index.html
13 http://www.insurancejournal.com/news/national/2015/01/15/354131.htm
14 http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

1. Equifax

In what is being described as the most devastating data breach to date, nearly half of the U.S. population had sensitive data exposed in a May 2017 hack. The target? Equifax, one of the largest credit reporting agencies in the United States and, ironically, an institute charged with guarding against identity theft. The data breach gave hackers access to information such as Social Security numbers, driver's licenses, credit cards, and addresses. Over 209,000 credit card numbers were exposed in the breach.

The identity of the attackers and their country of origin currently remains a mystery, though Equifax brought in an outside security consulting firm to assess the damage and determine the source. In late September 2017 press release, the credit bureau stated while much is still unknown about the breach, a recognized flaw in a web application tool granted hackers initial access.

Equifax is being criticized for mishandling the security breach. They discovered unauthorized access in late July, a full two months after hackers first breached the system[15], but waited nearly two months before notifying the public.[16] To make matters worse, three of the company's top executives sold $1.8 million in Equifax shares in the days following their discovery before the public was even notified.[17] Less than a month after the announcement, the FBI began investigating the situation and the company announced its chief information officer and chief security officer were "retiring".[18]

As of October 3, 2017, Equifax's stock remained over 25 percent lower than its pre-crisis price, a figure that represents a nearly $5 billion loss of market value.[19] The company has offered one year of free credit monitoring and identity theft protection to all consumers. However, at the time of this publication, neither the true cost of the breach nor its wider implications are fully known.

What the Financial Industry Can Learn

Consumer confidence in the security competence of financial institutions is at an all-time low. If the industry fails to prioritize cybersecurity, they will continue to be a target of data breaches. A proven way to prevent attacks is for financial organizations to re-examine their existing cybersecurity policies and implement a powerful data encryption solution to mitigate malicious attacks and prevent unauthorized access to data.

Try XCrypt™ Full Disk Today

[15] https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros
[16] https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack
[17] https://investor.equifax.com/news-and-events/news/2017/09-26-2017-140531280
[18] https://www.usatoday.com/story/money/2017/09/26/equifax-ceo-retiring-amid-cyberbreach-fallout/703173001/

465 Fairchild Drive, Suite 234, Mountain View, CA 94043
www.zettaset.com // +1.650.314.7920 // Fax: +1.650.314.7950 // sales@zettaset.com

About Zettaset

A leader in data protection, Zettaset's XCrypt™ line of encryption products are optimized for unmatched performance and infinite scalability to address the demanding data protection requirements of today's high-volume compute, storage, and cloud environments.