2017 Data Breaches

E-Sports Entertainment Association (ESEA)

January 8, 2017: On December 30, 2016, ESEA, one of the largest video gaming communities, issued a warning to players after discovering a breach. At the time, it wasn't known what was stolen and how many people were affected. However, in January, LeakedSource revealed that 1,503,707 ESEA records had been added to its database and that leaked records included a great deal of private information: registration date, city, state, last login, username, first and last name, bcrypt hash, email address, date of birth, zip code, phone number, website URL, Steam ID, Xbox ID, and PSN ID.

Xbox 360 ISO and PSP ISO

February 1, 2017: Security expert Troy Hunt, of the website *Have I Been Pwned?*, revealed that Xbox 360 ISO and PSP ISO had been hacked in September 2015. The websites, both forums which host illegal video game download files, housed sensitive user information that was taken. 1.2 million Xbox 360 ISO users and 1.3 million PSP ISO users were affected and may have had their e-mail addresses, IP addresses, usernames, and passwords stolen in the breach. At this time, it's not clear who is responsible, but forum users were encouraged to change their passwords immediately.

InterContinental Hotels Group (IHG)

February 7, 2017: IHG, the company that owns popular hotel chains like Crowne Plaza, Holiday Inn, Candlewood Suites, and Kimpton Hotels, announced a data breach that affected 12 of its properties. Malware was found on servers which processed payments made at on-site restaurants and bars; travelers that used cards at the front desk did not have information taken. The malware was active from August 2016 to December 2016 and stolen data includes cardholder names, card numbers, expiration dates, and internal verification codes. Some targeted locations include Sevens Bar & Grill at Crowne Plaza San Jose-Silicon Valley, the Bristol Bar & Grille at the Holiday Inn in San Francisco's Fisherman's Wharf, InterContinental San Francisco, Aruba's Holiday Inn Resort, and InterContinental Los Angeles Century City.

Arby's

February 17, 2017: The national fast food chain acknowledged a data breach after being pressed by the website KrebsOnSecurity. The company admitted that they had been notified in mid-January about a possible breach in select restaurants, but the FBI asked them not to go public yet. Malware was placed on payment systems inside certain Arby's corporate stores, which make up about one-third of all Arby's in the nation. There are about 1,000 corporate Arby's restaurants, and while not all were affected, it's not clear yet how many were. The company says that the malware has been removed, but the scope of the breach is not yet known. Arby's did not say when the breach occurred, but one credit union believes it may have been between October 25, 2016 and January 19, 2017.

River City Media

March 6, 2017: A group of spammers, operating under the name River City Media, unknowingly released their private data into cyberspace after failing to properly configure their backups. The leak known as Spammergateincluded Hipchat logs, domain registration records, accounting details, infrastructure planning, production notes, scripts, business affiliations, and more. The biggest discovery, however, was a database of 1.4 billion email accounts, IP addresses, full names, and some physical addresses. Thankfully, the "good guys" found the information—in this situation, it was Chris Vickery, a security researcher for MacKeeper—and reported everything to the proper authorities.

At this time, it's unclear what's going to happen to River City Media. While law enforcement is involved, groups like River City Media often have all sorts of aliases and affiliate programs—no one can be sure they will all be wiped out.

Verifone

March 7, 2017: KrebsOnSecurity revealed that Verifone, the largest maker of point-of-sale credit card terminals used in the U.S., discovered a breach of its internal network in January 2017. When asked, Verifone said the breach didn't affect its payment services network and was only within the corporate network. The company claims they responded to the breach immediately and "the potential for misuse of information is limited." Sources say there's evidence that a Russian hacking group is responsible for the breach, and that the intruders may have been inside Verifone's network since mid-2016, but nothing has been confirmed.

Dun & Bradstreet

March 15, 2017: Dun & Bradstreet, a huge business services company, found its marketing database with over 33 million corporate contacts shared across the web in March 2017. The firm claims its systems were not breached, but that it has sold the 52GB database to thousands of companies across the country; it's unclear which of those businesses suffered the breach that exposed the records. Millions of employees from organizations like the U.S. Department of Defense, the U.S. Postal Service, AT&T, Wal-Mart, and CVS Health had information leaked, and the database may have included full names, work email addresses, phone numbers, and other business-related data.

Saks Fifth Avenue

March 19, 2017: BuzzFeed broke the news that customer information was available in plain text via a specific link on the Saks Fifth Avenue website. The information for tens of thousands of customers was visible on a page where customers could join a wait list for products they were interested in. While payment details were not exposed, it was possible to see email addresses, phone numbers, product codes, and IP addresses. When BuzzFeed contacted Hudson Bay Company, the Canada-based organization that owns Saks Fifth Avenue, the pages containing customer information were taken down. At this time, it's not clear how this happened, how customers may have been affected, and who was responsible.

UNC Health Care

March 20, 2017: 1,300 letters were sent to prenatal patients who had received care in the University of North Carolina Health Care System about a potential data breach they may have been affected by. UNC Health Care revealed that women who had completed pregnancy home risk screening forms at prenatal appointments between 2014 and 2017 at the Women's Clinic at N.C. Women's Hospital and UNC Maternal-Fetal Medicine at Rex may have mistakenly had their personal information transmitted to local county health departments. Breached information included full names, addresses, races, ethnicities, Social Security numbers, and a variety of health-related information. The county health departments are subject to federal and state privacy laws and must protect all information they received; it was also requested that they electronically purge electronic information about non-Medicaid patients.

America's JobLink

March 21, 2017: America's JobLink, a web-based system that connects job seekers and employers, revealed its systems were breached by a hacker who exploited a misconfiguration in the application code. The criminal was able to gain access to the personal information of 4.8 million job seekers, including full names, birth dates, and Social Security numbers.

Activity was uncovered in the ten states that use the America's JobLink system: Alabama, Arkansas, Arizona, Delaware, Idaho, Illinois, Kansas, Maine, Oklahoma, and Vermont. The code misconfiguration was discovered and eliminated on March 14, 2017, so anyone who had an account with America's JobLink before March 14, 2017 may have been affected and had their personal information compromised.

FAFSA: IRS Data Retrieval Tool

April 6, 2017: The IRS revealed that up to 100,000 taxpayers may have had their personal information stolen in a scheme involving the IRS Data Retrieval Tool, which is used to complete the Free Application for Federal Student Aid (FAFSA). In March 2017, federal officials observed a potential data breach and took the tool down. The IRS said it shut down the Data Retrieval Tool because identity thieves that had obtained some personal information outside of the tax system were possibly using the tool to steal additional data.

Currently, the agency suspects that less than 8,000 fraudulent returns were filed, processed, and returns issued, costing $30 million. 52,000 returns were stopped by IRS filters and 14,000 illegal refund claims were halted as well.

InterContinental Hotels Group (IHG)

April 19, 2017: When IHG first announced a data breach in February 2017, it was believed that only 12 of its properties had been affected. It's been revealed, however, that the initial 12 has jumped to 1,200. IHG said the dozen hotels initially named were only the ones they run directly and at the time, they did not know the full scope of the breach; the other hotels are IHG-branded franchise properties. The malware had infected hotel servers, but was eradicated in all locations by the end of March.

Chipotle

April 25, 2017: Chipotle posted a "Notice of Data Security Incident" on its website to let customers know about unauthorized activity it detected on the network that supports in-restaurant payment processes. It believes payment card transactions that occurred from March 24, 2017 through April 18, 2017 may have been affected. The investigation is still ongoing and at the time the notice was published, the company did not have any additional information; it just said that it believes it has stopped the unauthorized activity and it's too early to give more details.

Sabre Hospitality Solutions

May 2, 2017: Sabre Hospitality Solutions, a tech company that provides reservation system services for more than 36,000 properties, revealed a breach that allowed hotel customer payment information to be compromised. The company shared the information in its quarterly filing report and did not say when the breach happened or which locations may have been affected. The unauthorized access has been shut off and the company does not believe any other Sabre systems have been compromised.

Gmail

May 3, 2017: Gmail users were targeted in a sophisticated phishing scam that was seeking to gain access to accounts through a third-party app. The emails were made to look like they were from a user's trusted contact and notified the individual that they wanted to share a Google Doc with them. Once clicked, the link led to Google's real security page where the person was prompted to allow a fake Google Docs app to manage his or her email account. Google put a stop to the scam in about one hour and the company says they estimate about 1 million users may have been affected.

Bronx Lebanon Hospital Center

May 10, 2017: Thousands of HIPAA-protected medical records were exposed in a data breach due to a misconfigured Rsync backup server hosted by a third party, iHealth. At least 7,000 patients who visited the Bronx Lebanon Hospital Center in New York between 2014 and 2017 may have had extremely personal information compromised. Leaked information has been reported to include names, home addresses, religious affiliations, addiction histories, mental health and medical diagnoses, HIV statuses, and sexual assault and domestic violence reports. Once the breach was detected, the hospital and iHealth took immediate steps to protect the exposed data.

Brooks Brothers

May 12, 2017: If you shopped at a Brooks Brothers retail store or outlet in the last year and used a credit or debit card, you may have had your card data stolen. Brooks Brothers revealed a breach that affected some of their stores between April 4, 2016, and March 1, 2017; the retailer has not revealed which exact locations were targeted yet. A forensic investigation showed an unauthorized individual installed malicious software on some payment processing systems that was capable of collecting payment card information. Brooks Brothers said the issue has been resolved but did not provide any other details upon announcing the breach.

DocuSign

May 17, 2017: Customers and users of the electronic signature provider DoguSign were targeted recently by malware phishing attacks. DocuSign says that hackers breached one of its systems, but they only obtained email addresses and no other personal information. The hackers used the email addresses to conduct a malicious email campaign in which DocuSign-branded messages were sent that prompted recipients to click and download a Microsoft Word document that contained malware. If you received a suspicious DocuSign email, forward it to spam@docusign.com; moving forward, only access documents directly through the DocuSign website and not by clicking email links.

OneLogin

May 31, 2017: OneLogin, a San Francisco-based company that allows users to manage logins to multiple sites and apps through a cloud-based platform, has reported a troubling data breach. OneLogin provides single sign-on and identity management for about 2,000 companies in 44 countries, over 300 app vendors and more than 70 software-as-a-service providers. A threat actor obtained access to a set of AWS keys and used them to access the AWS API from an intermediate host with another, smaller service provider in the US. The attack began at 2am PST on May 31 and was shut down by 9am. Customer data was compromised during this time, including the ability to decrypt encrypted data. The investigation is ongoing and the full extent of the breach is still unknown.

Kmart

May 31, 2017: Sears Holdings, the parent company of Kmart, revealed that Kmart's store payment systems were infected with malware; Kmart.com and Sears shoppers were not impacted by this breach. The malicious code has been removed, but the company has not shared how long the payment system was under attack and how many stores were affected. No personal identifying information was compromised, but certain credit card numbers may have been. Kmart suffered a very similar data breach back in 2014, that we also told you about at the time.

University of Oklahoma

June 14, 2017: The University of Oklahoma's (OU) student-run newspaper, The Oklahoma Daily, was the first to discover an on-campus data breach connected to the university's document sharing system, Delve. Educational records, dating back to at least 2002, were unintentionally exposed through incorrect privacy settings. The Oklahoma Daily reported that in just 30 of the hundreds of documents made publicly discoverable on Microsoft Office Delve, there were more than 29,000 instances in which students' private information was made public to users within OU's email system. Sensitive information included Social Security numbers, financial aid information, and grades. The file sharing service has been shut down until further notice.

Washington State University

June 15, 2017: A hard drive containing the personal information of approximately one million people was stolenfrom a Washington State University storage unit in Olympia, WA. The hard drive was inside an 85-pound safe, so the university says it has no current reason to believe the individual was able to get inside the safe and steal the data on the hard drive. Information on the hard drive was part of research the university had conducted for school districts, government offices, and other outside agencies; Social Security numbers and health history were among the personal details stolen. The university has sent letters to individuals who may have been affected and will be offering them a free year of credit monitoring.

Deep Root Analytics

June 20, 2017: Last year, the Republican National Committee hired Deep Root Analytics, a data analytics firm, to gather political information about U.S. voters. Chris Vickery, a cyber risk analyst, discovered that the sensitive information Deep Root Analytics obtained–personal data for roughly 198 million American citizens–was stored on an Amazon cloud server without password protection for almost two weeks this month. Exposed information includes names, dates of birth, home addresses, phone numbers, and voter registration details. Deep Root has taken full responsibility, updated the access settings, and put protocols in place to prevent further access.

Blue Cross Blue Shield / Anthem

June 27, 2017: Health insurance company Anthem has agreed to a $115 million settlement in connection with a 2015 data breach that impacted 80 million of their customers across their Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, Unicare, Healthlink, and DeCare brands.

Although Anthem acted quickly, notifying the FBI and working with a cyber security firm as soon as it was made aware of the breach, the breadth of the initial breach and subsequent costly payout just goes to reinforce the need for companies of all sizes to take cyber security issues seriously.

While the settlement still needs to be approved by the courts during a hearing on August 17th, the health insurance giant released a statement, stating "Nevertheless, we are pleased to be putting this litigation behind us, and to be providing additional substantial benefits to individuals whose data was or may have been involved in the cyberattack and who will now be members of the settlement class."

Anthem originally agreed to provide impacted individuals with 2 years of credit monitoring services. They are extending that offer for an additional 2 years, as part of this settlement.

California Association of Realtors

July 10, 2017: A subsidiary of the California Association of Realtors—Real Estate Business Services (REBS)—was the victim of a data breach; it was recently reported to the California Attorney General's Office. The organization's store.car.org online payment system was infected with malware that was active between March 13, 2017, and May 15, 2017. When a user made a payment on the website during that time frame, personal information may have been copied by the malware and transmitted to an unknown third party. Sensitive data that had the potential to be accessed included the user's name, address, credit card number, credit card expiration date, and credit card verification codes. The malware has been removed and the organization is now using PayPal for payments.

Verizon

July 13, 2017: A reported 14 million Verizon subscribers may have been affected by a data breach, and you might be one of them if you have contacted Verizon customer service in the past six months. These records were held on a server that was controlled by Israel based Nice Systems. The data breach was discovered by Chris Vickery, who is with the security firm, UpGuard. He informed Verizon of the data exposure in late-June, and it took more than a week to secure the breached data. The actual data that was obtained were log files that became generated when customers of Verizon contacted the company via phone.

Online Spambot

August 30, 2017: Remember the River City Media breach from March 2017 in which the "bad guys" had information stolen? It's happened again to an online spambot, and the set of stolen data is even larger. Though River City Media's breach was originally believed to impact 1.4 billion people, it "only" ended up being 393 million records; this online spambot breach reportedly involves 711 million records. The spambot had harvested email addresses and some passwords to send spam emails, but forgot to secure the server the data was kept on. Currently, it is unknown how many people have found this database and are using the information for their own nefarious purposes.

TalentPen and TigerSwan

September 2, 2017: Over 9,000 documents containing the personal information of job seekers with Top Secret clearance were publicly available on an unsecured Amazon server for just over six months. UpGuard, a cybersecurity firm, found the public files in a folder labeled "resumes" and reached out to TigerSwan, a private security firm that owned the files. It was discovered that a third-party vendor that TigerSwan had ended their contract with—TalentPen—had failed to take down the files after they were transferred to TigerSwan in February. TalentPen left the files in a bucket site on Amazon Web Services without a password or any type of security until August 24, 2017 when Amazon contacted them about it; at that point, the files were taken down.

Equifax

September 7, 2017: Equifax, one of the three largest credit agencies in the U.S., suffered a breach that may affect 143 million consumers. Due to the sensitivity of data stolen—including Social Security numbers and driver's license numbers—this is being called one of the worst breaches ever. Hackers were able to gain access to the company's system from mid-May to July by exploiting a weak point in website software; the breach was discovered by Equifax on July 29th, 2017 and at that time, they sought assistance from an outside forensics firm. Other compromised data is said to include full names, addresses, dates of birth, credit card numbers, and other personal information.

U.S. Securities and Exchange Commission (SEC)

September 21, 2017: Jay Clayton, Chairman of the SEC, issued a statement about cybersecurity and included details of a 2016 data breach. Clayton wrote that in 2016, a software vulnerability in the test filing component of the SEC's EDGAR system was discovered and patched "promptly." However, in August 2017, the SEC learned that incident "may have provided the basis for illicit gain through trading." The vulnerability allowed access to nonpublic information, but the SEC does not believe there has been any unauthorized access to personally identifiable information.

SVR Tracking

September 21, 2017: SVR Tracking, a San-Diego based service that gives auto dealership and lot owners the ability to locate and recover vehicles, allowed more than half a million customer records to be leaked online. On September 18, Kromtech Security Center found 540,642 records in an unsecured Amazon S3 bucket and notified SVR Tracking of their findings on September 20; SVR secured the bucket within three hours. However, it is unknown how long the information was publicly available online and the data was quite sensitive in nature—it included email addresses, passwords, license plate numbers, VINs, and even the ability to see every single place a vehicle has been in the last 120 days.

Deloitte

September 25, 2017: A breach that affected Deloitte, a multinational professional services firm, in March came to light—and the reason is pretty embarrassing for a company that was once named the "best cybersecurity consultant in the world" by Gartner. The firm did not employ two-factor authentication, so when hackers acquired a single password from an administrator of the firm's email account, they were able to access all areas of the email system. Investigators determined that Deloitte's biggest clients were of interest to the hackers, but Deloitte insists only a small fraction of its clients have been impacted.

Sonic

September 26, 2017: KrebsOnSecurity reported a breach at fast food chain Sonic after discovering a "fire sale" of millions of stolen credit and debit card numbers on the Dark Web. Sonic learned about the breach when its credit card processor notified them of unusual activity on customer payment cards. Sonic has almost 3,600 stores in 45 states, but it is not immediately known which locations were affected—the company is working with law enforcement and investigators to determine the true scope of the breach.

Whole Foods Market

September 28, 2017: Whole Foods Market—recently acquired by Amazon—made a statement regarding the discovery of a recent breach of its payment systems. Individuals who shopped in the company's grocery stores were likely not affected, but it is believed the unauthorized access occurred in Whole Foods locations with taprooms and full table-service restaurants. The company is currently in the middle of an ongoing investigation and has said it will provide additional updates as it learns more. It has also said that Amazon's payment systems are not connected to Whole Foods and no Amazon transactions were impacted by the breach.

Disqus

October 6, 2017: Disqus, a blog comment hosting service, revealed that it was targeted by hackers five years ago. The company had no idea it had been the victim of a data breach in 2012 until the website *Have I Been Pwned?* reached out with exposed user information it had found. In a statement, Disqus says it verified the authenticity of the data and found it was from their 2012 user database, which included information dating back to 2007. User email addresses, user names, sign-up dates, and last-login dates were among the stolen data; hashed passwords using SHA1 with a salt for approximately one-third of users were also public. Disqus does not believe there is any evidence of unauthorized logins, but it has reset the passwords of all affected users.

Yahoo!

October 9, 2017: In December 2016, it was reported that "more than 1 billion user accounts" may have been impacted by the 2013 Yahoo breach. Recent news, however, shows it was indeed more than 1 billion—**much** more. Four months after Verizon acquired Yahoo's core internet assets, it was revealed that **every single customer account** was impacted by that breach; **three billion Yahoo accounts**—including email, Tumblr, Fantasy, and Flickr—were stolen. Even after thorough investigations, it is still unknown who was behind the 2013 Yahoo breach.

Hyatt Hotels

October 12, 2017: After suffering a data breach in December 2015, the Hyatt hotel chain has fallen victim to hackers again. The company discovered unauthorized access to its payment card information for debit and credit cards that were swiped at the front desks of some of its properties. Stolen information includes card numbers, expiration dates, internal verification codes, and cardholder names. At this point, Hyatt believes 41 of its properties in 11 countries were affected between March 18, 2017 and July 2, 2017. Only five properties in the U.S. were targeted: three were in Hawaii, while one was in Puerto Rico, and the other in Guam. Hyatt has provided a list of all affected properties that prior guests can check.

Forever 21

November 14, 2017: Los Angeles-based clothing retailer Forever 21 announced that some of its customers may have been affected by a potential data breach. Upon receiving a tip from a third-party, Forever 21 launched an investigation and found certain point-of-sale (PoS) devices were compromised—likely between March and October of this year. The company said it implemented "encryption and tokenization solutions" in 2015 and that it appears the targeted PoS devices would have had encryption that was not operating. At the time of the announcement the investigation was still occurring, so it is not known how many people may have been impacted by this breach or who is responsible. Forever 21 customers are encouraged to keep an eye on their payment accounts and look for fraudulent charges.

Maine Foster Care

November 14, 2017: Residents of Maine receiving foster care benefits had their personal information exposedon a third-party website outside of the State of Maine system. During a system upgrade on September 21, 2017, a contractor hired by Maine Office of Information Technology accidentally posted the private information, which included names of foster children and legal guardians, addresses, and Social Security numbers. The information was publicly available for approximately four and a half hours that day; once it was discovered, the data was removed from the site. The personal information was accessed once during that time period, but Maine's Chief Information Officer Jim Smith said "there is no indication that there is any intent by a third party to misuse your personal data."

Uber

November 21, 2017: The ride-sharing service giant Uber revealed that in late 2016, it became aware of a data breach that potentially exposed the personal information of 57 million Uber users and drivers. However, the company chose to pay the hackers $100,000 to keep the enormous data breach a secret, instead of immediately alerting those affected by the breach. How did this happen? Hackers did not gain access to Uber's internal systems, but rather GitHub, a service that Uber's engineers use to collaborate on software code. Two hackers downloaded the data stored on GitHub, which included names, email addresses, and phone numbers of Uber users worldwide. With our lives becoming busier by the minute, more and more people are relying on services like Uber to make their lives a bit easier and more convenient. Unfortunately, it's becoming painfully clear that often times, that convenience comes at cost. Who would have thought that a simple ride to the airport could potentially cost you your identity?

Imgur

November 24, 2017: Imgur, the online image-sharing community, had a lot to be thankful for on Thanksgiving—until it received a notification that day about a possible data breach from

2014. Troy Hunt, the owner of the website Have I Been Pwned, reached out to Imgur's COO on November 23, 2017 to let him know that he had received data that seemed to include the emails and passwords of Imgur users. The company investigated, and by the next morning, had discovered 1.7 million users from 2014 had indeed had their email addresses and passwords stolen. Imgur contacted affected users immediately on November 24 and publicly disclosed the breach on their website that day as well.

TIO Networks

December 1, 2017: Due to a vulnerability in their network, TIO Networks, who was recently acquired by PayPal, may have compromised the identities of over 1.6 million customers. The compromised data includes bank account information, payment card information, passwords and usernames for accounts, and Social Security numbers. Although there has been no evidence that any of customer data has been stolen, they are still treating this incident as a data breach. PayPal is offering free credit monitoring services to those impacted by this breach.

eBay

December 10, 2017: Due to a customer privacy leak, the personal information of many eBay customers, including usernames, first and last names, and purchase history, were made available via a Google's Shopping platform.

The breach was due to "an improper feed signal" between the two companies. According to an eBay spokesperson, the companies are trying to find the root cause. The purchase histories that were leaked revealed very sensitive products, such as HIV home test kits, pregnancy test, and drug testing kits. Within a couple days, the users real names were masked with dashes. This is just another example of one of the many ways that your personal information can become compromised, through no fault of your own.

Alteryx

December 19, 2017: Alteryx, a California-based data analytics firm, was found culpable of not protecting the personal information of more than 120 million American households. The company had purchased this data from Experian, a giant credit reporting agency similar to Equifax. What we now know is that the exposed data was openly housed on an Amazon Web Services cloud storage bucket. All that anyone needed to access peoples' private information was the URL, along with an Amazon AWS account. The impact of this breach is yet to be seen, but could very well be substantial based on the information that was available to potential cybercriminals. We will update this post as further details emerge.