**Cybersecurity Incident Tracker   
(Updated 8.8.19)**

Contents

[Overview 2](#_Toc16166239)

[Key Findings and Recommendations 3](#_Toc16166240)

[Adobe 4](#_Toc16166242)

[Target 8](#_Toc16166243)

[eBay 10](#_Toc16166244)

[JP Morgan Chase 12](#_Toc16166245)

[Sony 14](#_Toc16166246)

[LinkedIn 16](#_Toc16166247)

[MySpace 19](#_Toc16166248)

[Verizon 21](#_Toc16166249)

[Equifax 24](#_Toc16166250)

[Uber 27](#_Toc16166251)

[Under Armour – MyFitnessPal 31](#_Toc16166252)

[Facebook 33](#_Toc16166253)

[Ticketfly 35](#_Toc16166254)

[T-Mobile 37](#_Toc16166255)

[Chegg 39](#_Toc16166256)

[Marriott 41](#_Toc16166257)

[Quora 43](#_Toc16166258)

[Dow Jones 45](#_Toc16166259)

[Facebook 48](#_Toc16166260)

[Oregon Department of Human Services (DHS) 51](#_Toc16166261)

[Federal Emergency Management Agency (FEMA) 54](#_Toc16166262)

[Georgia Institute of Technology 56](#_Toc16166263)

[Bodybuilding.com 58](#_Toc16166264)

[WhatsApp 62](#_Toc16166265)

[Instagram 64](#_Toc16166266)

[First American Financial Corp. 66](#_Toc16166267)

[Quest Diagnostics 71](#_Toc16166268)

[LabCorp 73](#_Toc16166269)

# **Overview**

As technology continues to evolve into an increasingly inextricable part of life, with it comes a multitude of risks. What once began as a risk to vulnerable industries, such as finance and healthcare, is now an omnipresent threat to any organization. While hackers have existed in the cyberspace since its conception, their methods advance with each development in technology, becoming more complicated and dangerous with each passing breach.

More personal privacy is signed away as society continues to digitalize, and the more sensitive the data, the more is at stake. Compromised data can cause problems for individuals, corporations, and even governments and countries. For example, data breached from a government entity can put confidential information in the hands of an enemy state.

On average, a data breach will cost an organization $3.9 million, with the average of each lost or stolen record containing sensitive information costing $148 ([IBM](https://www.ibm.com/security/data-breach)). The main trends identified in some of the biggest cyberattacks in recent years included phishing, spyware and unsecured third-party servers. Some of the largest data breaches to data suffered because of these types of attacks.

While some of these issues are avoidable, they often are overlooked or forgotten. Luckily for humanity, the defenses for data privacy are also adapting to cyberattacks, however, they still occur at alarm rates, and organizations must be prepared to deal with the consequences of a digitalized world.

In utopia, data breaches would be nonexistent, however, with the rise of its occurrences, it seems to be that experiencing a data breach is not an “if”, but a “when.”

# **Key Findings**

* Organizations are never safe from cyberattacks because methods are constantly evolving
* While financial, educational and medical institutions are the most susceptible to cyberattacks, every organization is a potential target
* When it comes to cybersecurity defense, employees can be your greatest asset or your weakest link based on the level of their cyber knowledge
* Many breaches could have been easily avoided if vulnerabilities had been detected before being exploited by attackers
* Late notification is oftentimes the greatest criticism a company faces after a breach; however, it is sometimes unavoidable due to forensic investigations simultaneously occurring
* Companies that disclose breaches and are transparent with their key audiences were less likely to suffer substantial reputational loss
* Because companies enduring cyber crises are heavily criticized by the media and stakeholders following a breach, it is critical to release well-executed public responses

# **Recommendations**

* The level of a cybersecurity crisis rises with the sensitivity of the data that was leaked, so it is vital to safeguard this information with additional security measures
  + Store customers’ personal health and financial information separately from basic personal information
  + Encrypting data, hashing passwords, using two-step verification and other methods exist to properly secure data
* Complete routine security scans and regularly monitor servers to ensure vulnerabilities are discovered by internal members or approved external vendors before it is taken advantage of by malicious actors
* Provide employee training to improve cyber knowledge and to prevent phishing attacks from successfully infiltrating company networks
  + Phishing attacks are the most popular and the most successful form of cyberattack against an organization because it requires little effort for employees to unknowingly hand over their information
* Create crisis scenarios to be prepared for potential situations
* Having established policies and procedures and structured plans prevents additional chaos that comes with a cybersecurity incident, both internal and external
* Evaluate the scope and scale of an incident and who was affected in order to determine which audiences will receive notification first
* Always have a subject matter expert available to monitor the narrative and adjust messaging to address concerns as relevant
* Provide adequate resources and customer service for stakeholders and key audiences
  + Add customer service call lines or live chats to allow stakeholders to receive answers to their questions in an easy and efficient manner
  + Offer updates across company social channels as well as affiliates’ social channels
* Begin rebuilding trust with stakeholders as soon as possible
  + Launching a fierce public relations counterattack helps protect the company’s reputation and prevents stakeholders from further losing trust

# **Adobe**

**Disclosure Date:** October 2013

**Situation Overview:**

Hackers infiltrated the computer system of Adobe, gaining access to credit card information and other personal data from 38 million customers. The security breach, which Adobe called a part of a “sophisticated attack,” also allowed hackers to obtain encrypted passwords and other personal information from customers. Hackers also illegally took copies of the source code of some of the company’s widely used products, which are run on personal computers and businesses servers around the world. Although there was no indication that the attackers obtained unencrypted credit card numbers, as a precaution the company said it had notified customers and credit card companies about the breach and reset customer passwords to prevent further unauthorized access.

**Disclosure Materials:**

* Who disclosed the breach? Media – Krebs on Security
* Press release:

[Adobe To Announce Source Code, Customer Data Breach (Krebs on Security)](https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/)

Adobe Systems Inc. is expected to announce today that hackers broke into its network and stole source code for an as-yet undetermined number of software titles, including its ColdFusion Web application platform, and possibly its Acrobat family of products. The company said hackers also accessed nearly three million customer credit card records, and stole login data for an undetermined number of Adobe user accounts.

KrebsOnSecurity first became aware of the source code leak roughly one week ago, when this author — working in conjunction with fellow researcher Alex Holden, CISO of Hold Security LLC — discovered a massive 40 GB source code trove stashed on a server used by the same cyber criminals believed to have hacked into major data aggregators earlier this year, including LexisNexis, Dun & Bradstreet and Kroll. The hacking team’s server contained huge repositories of uncompiled and compiled code that appeared to be source code for ColdFusion and Adobe Acrobat.

Shortly after that discovery, KrebsOnSecurity shared several screen shots of the code repositories with Adobe. Today, Adobe responded with confirmation that it has been working on an investigation into a potentially broad-ranging breach into its networks since Sept. 17, 2013.

In an interview with this publication earlier today, Adobe confirmed that the company believes that hackers accessed a source code repository sometime in mid-August 2013, after breaking into a portion of Adobe’s network that handled credit card transactions for customers. Adobe believes the attackers stole credit card and other data on approximately 2.9 million customers, and that the bad guys also accessed an as-yet-undetermined number of user names and passwords that customers use to access various parts of the Adobe customer network.

Adobe said the credit card numbers were encrypted and that the company does not believe decrypted credit card numbers left its network. Nevertheless, the company said that later today it will begin the process of notifying affected customers — which include many Revel and Creative Cloud account users — via email that they need to reset their passwords.

In an interview prior to sending out a news alert on the company’s findings, Adobe’s Chief Security Officer Brad Arkin said the information shared by this publication “helped steer our investigation in a new direction.” Arkin said the company has undertaken a rigorous review of the ColdFusion code shipped since the code archive was compromised, and that it is confident that the source code for ColdFusion code that shipped following the incident “maintained its integrity.”

“We are in the early days of what we expect will be an extremely long and thorough response to this incident,” Arkin said. The company is expected to publish an official statement this afternoon outlining the broad points of its investigation so far.

Arkin said Adobe is still in the process of determining what source code for other products may have been accessed by the attackers, and conceded that Adobe Acrobat may have been among the products the bad guys touched. Indeed, one of the screen shots this publication shared with Adobe indicates that the attackers also had access to Acrobat code, including what appears to be code for as-yet unreleased Acrobat components (see screen grab above).

“We’re still at the brainstorming phase to come up with ways to provide higher level of assurance for the integrity of our products, and that’s going to be a key part of our response,” Arkin said. He noted that the company was in the process of looking for anomalous check-in activity on its code repositories and for other things that might seem out of place.

“We are looking at malware analysis and exploring the different digital assets we have. Right now the investigation is really into the trail of breadcrumbs of where the bad guys touched.”

The revelations come just two days after KrebsOnSecurity published a story indicating that the same attackers apparently responsible for this breach were also involved in the intrusions into the networks of the National White Collar Crime Center (NW3C), a congressionally-funded non-profit organization that provides training, investigative support and research to agencies and entities involved in the prevention, investigation and prosecution of cybercrime. As noted in that story, the attackers appear to have initiated the intrusion into the NW3C using a set of attack tools that leveraged security vulnerabilities in Adobe’s ColdFusion Web application server.

While Adobe many months ago issued security updates to plug all of the ColdFusion vulnerabilities used by the attackers, many networks apparently run outdated versions of the software, leaving them vulnerable to compromise. This indeed may have also been the vector that attackers used to infiltrate Adobe’s own networks; Arkin said the company has not yet determined whether the servers that were breached were running ColdFusion, but acknowledged that the attackers appear to have gotten their foot in the door through “some type of out-of-date” software.

Stay tuned for further updates on this rapidly-moving story.

# # #

**Media Details:**

* Since this security breach was one of the largest (to date) in history, the Adobe 2013 data breach received an overwhelming amount of media coverage from top-tier publications, including international, national and local media outlets. The coverage lasted for months on end, and spiked as Adobe discovered that there were more victims of the data breach than originally announced. Adobe was ridiculed by many publications for having “shoddy” security practices, which ultimately lead to the breach. Outlets claimed that Adobe made “basic” mistakes which allowed hackers to ransack its customer database. However, besides the outlets that highlighted Adobe’s security practices, most reporting was fact-based and neutral.
* [Adobe to hire security auditor to prevent repeat of password SNAFU (The Register)](https://www.theregister.co.uk/2015/06/09/adobe_to_hire_security_auditor_to_prevent_repeat_of_password_snafu/)

**Key Communications Takeaways:**

* **Adapt to the ever-changing cybersecurity landscape.** When the 2013 Adobe breach happened, the company did not have any Chief Security Officer or equivalent position. Brad Arkin, Adobe’s current CSO, was only a senior director at Adobe in 2013, which was the company’s highest security title at the time. Following the breach, Adobe created the CSO role and worked to integrate all of the different “pockets of security teams”, which were tasked with clarifying priorities and uncovering organizational blind spots. Had this position/team been implemented sooner, Adobe could have potentially avoided one of the biggest data breaches in history. Reports also stated that Adobe knew its security practices at the time were poor since it used the same encryption key for all passwords. It had not deployed a new encryption system nor decommissioned the old backup server by the time of the breach.
* **Timely notification to the public will reduce scrutiny.** Krebs on Security reported on the Adobe data breach before Adobe did. Having a media publication report on a cyber incident before the company itself can tarnish the relationship between the public and the company. Adobe failed to demonstrate that it had consumers’ best interests in mind by withholding news of the breach from the public.

***Note:*** *While there are no federal laws for data privacy and data breach disclosure, all 50 states, Washington, DC, Puerto Rico and the US Virgin Islands all have specific laws requiring government notification within 72 hours of a breach’s discovery and public disclosure anywhere from 30-60 days of its discovery. These laws were not established until 2017, and in 2018 for Alabama and South Dakota.*

# **Target**

**Disclosure Date:** December 2013

**Situation Overview:**

In one of the biggest data breaches to hit a U.S. retailer, Target had reported that hackers stole data from up to 40 million credit and debit cards of shoppers who had visited its stores during the 2013 holiday season. Less than a month later, Target discovered that an additional 70 million records of personal information was stolen. The information stolen included customer names, mailing addresses, phone numbers and email addresses, credit or debit card numbers, the card’s expiration date and CVV. Target said that much of this data is "partial in nature," but it will nonetheless provide one year of free credit monitoring and identity theft protection to all guests who shopped at its U.S. stores.

**Disclosure Materials:**

* Who disclosed the breach? Media ([Krebs on Security](https://www.forbes.com/sites/sungardas/2014/01/17/five-lessons-for-every-business-from-targets-data-breach/#15b2eff56563))
* Disclosure materials:

[Sources: Target Investigating Data Breach (Krebs on Security)](https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/)

Nationwide retail giant Target is investigating a data breach potentially involving millions of customer credit and debit card records, multiple reliable sources tell KrebsOnSecurity. The sources said the breach appears to have begun on or around Black Friday 2013 — by far the busiest shopping day the year.

Update, Dec. 19: 8:20 a.m. ET: Target released a statement this morning confirming a breach, saying that 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013.

*Original story;*

According to sources at two different top 10 credit card issuers, the breach extends to nearly all Target locations nationwide, and involves the theft of data stored on the magnetic stripe of cards used at the stores.

Minneapolis, Minn. based Target Brands Inc. has not responded to multiple requests for comment. Representatives from MasterCard and Visa also could not be immediately reached for comment.

Both sources said the breach was initially thought to have extended from just after Thanksgiving 2013 to Dec. 6. But over the past few days, investigators have unearthed evidence that the breach extended at least an additional week — possibly as far as Dec. 15. According to sources, the breach affected an unknown number of Target customers who shopped at the company’s bricks-and-mortar stores during that timeframe.

“The breach window is definitely expanding,” said one anti-fraud analyst at a top ten U.S. bank card issuer who asked to remain anonymous. “We can’t say for sure that all stores were impacted, but we do see customers all over the U.S. that were victimized.”

There are no indications at this time that the breach affected customers who shopped at Target’s online stores. The type of data stolen — also known as “track data” — allows crooks to create counterfeit cards by encoding the information onto any card with a magnetic stripe. If the thieves also were able to intercept PIN data for debit transactions, they would theoretically be able to reproduce stolen debit cards and use them to withdraw cash from ATMs.

It’s not clear how many cards thieves may have stolen in the breach. But the sources I spoke with from two major card issuers said they have so far been notified by one of the credit card associations regarding more than one million of cards total from both issuers that were thought to have been compromised in the breach. A third source at a data breach investigation firm said it appears that “when all is said and done, this one will put its mark up there with some of the largest retail breaches to date.”

Some of the largest retailer breaches to date may help explain what happened in this case. In 2007, retailer TJX announced that its systems had been breached by hackers. The company later learned that thieves had used the store’s wireless networks to access systems at its Massachusetts headquarters that were used to store data related to payment card, check and return transactions at stores across the country, and that crooks had made off with data from more than 45 million customer credit and debit cards.

In 2009, credit card processor Heartland Payment Systems disclosed that thieves had broken into is internal card processing network, and installed malicious software that allowed them to steal track data on more than 130 million cards.

This is likely to be a fast-moving story. Stay tuned for updates as they become available.

# # #

**Media Details:**

* Target’s 2013 data breach consisted of significant media coverage reported by local, national and international news outlets for several months. The media coverage was fact-based and largely negative in tone, and is still mentioned years later as one of the worst breaches in corporate history. The company was criticized for failing to tell customers about the breach in a timely manner, as well as having poor customer service following the announcement. However, Target was applauded for its apology video by CEO Gregg Steinhafel, as well as for offering a store-wide discount to customers and offering a year of free credit monitoring to affected customers.
* [Target strives to patch its image after huge data security breach (StarTribune)](http://www.startribune.com/target-strives-to-patch-its-image-after-huge-data-security-breach/237207491/)

**Key Communications Takeaways:**

* **Communicate the problem as soon as possible.** John Biggs of Tech Crunch said, “The company moved quite slowly on this breach.” That’s because a report on the breach had emerged a week earlier on Krebs on Security. Target was criticized by many outlets for knowing about the crisis far before announcing the breach to its customers.
* **Be ready to respond to your customers.** Even once Target began to “fess up” to the breach, their communications with customers were far from adequate, reported Andria Cheng for the [Wall Street Journal's MarketWatch](http://blogs.marketwatch.com/behindthestorefront/2013/12/20/targets-pr-nightmare-customer-service-gridlock/). Customer services lines for the company's own Target Redcard credit cards were in gridlock, a website banner informing customers of the breach was too small to see, and the retailer's social media channels were flooded with angry customers.
* **Rebuild trust.** According to an article by [StarTribune](http://www.startribune.com/target-strives-to-patch-its-image-after-huge-data-security-breach/237207491/), Target “launched a fierce public relations counterattack, with daily news briefings and a flurry of photos and statements designed to show the company aggressively responding to arguably the worst crisis in its 50-year-plus history." This included a video apology from CEO Gregg Steinhafel who offered a store-wide discount and assured customers they were the top priority as the retailer addressed the problem, as well as offering a year of free credit monitoring to affected customers.

# **eBay**

**Disclosure Date:** May 2014

**Situation Overview:**

eBay reported a cyberattack in May 2014 that had exposed names, addresses, dates of birth and encrypted passwords of its 145 million users. The company said hackers got into the company network using the credentials of three corporate employees, and had complete inside access for 229 days, during which time they were able to make their way to the user database.

It asked its customers to change their passwords, but said financial information, such as credit card numbers, was stored separately and was not compromised.

**Disclosure Materials:**

* Who disclosed the breach? eBay Inc.
* Press release:

[eBay Inc. to Ask Users to Change Passwords](https://www.ebayinc.com/stories/news/ebay-inc-ask-ebay-users-change-passwords/)

eBay Inc. (Nasdaq: EBAY) said beginning later today it will be asking eBay users to change their passwords because of a cyberattack that compromised a database containing encrypted passwords and other non-financial data. After conducting extensive tests on its networks, the company said it has no evidence of the compromise resulting in unauthorized activity for eBay users, and no evidence of any unauthorized access to financial or credit card information, which is stored separately in encrypted formats. However, changing passwords is a best practice and will help enhance security for eBay users.

Information security and customer data protection are of paramount importance to eBay Inc., and eBay regrets any inconvenience or concern that this password reset may cause our customers. We know our customers trust us with their information, and we take seriously our commitment to maintaining a safe, secure and trusted global marketplace.

Cyberattackers compromised a small number of employee log-in credentials, allowing unauthorized access to eBay's corporate network, the company said. Working with law enforcement and leading security experts, the company is aggressively investigating the matter and applying the best forensics tools and practices to protect customers.

The database, which was compromised between late February and early March, included eBay customers’ name, encrypted password, email address, physical address, phone number and date of birth. However, the database did not contain financial information or other confidential personal information. The company said that the compromised employee log-in credentials were first detected about two weeks ago. Extensive forensics subsequently identified the compromised eBay database, resulting in the company’s announcement today.

The company said it has seen no indication of increased fraudulent account activity on eBay. The company also said it has no evidence of unauthorized access or compromises to personal or financial information for PayPal users. PayPal data is stored separately on a secure network, and all PayPal financial information is encrypted.

Beginning later today, eBay users will be notified via email, site communications and other marketing channels to change their password. In addition to asking users to change their eBay password, the company said it also is encouraging any eBay user who utilized the same password on other sites to change those passwords, too. The same password should never be used across multiple sites or accounts.

# # #

**Media Details:**

* The eBay breach was covered by top-tier media outlets such as USA Today, Forbes, CNBC, Business Insider and Reuters. While widely reported, coverage lasted about a week, before dying down. The coverage was focused on the email that eBay sent to its customers, urging them to change their passwords. Additionally, coverage focused on how the hackers were able to access data suing the credentials of three corporate employees. Further, coverage highlighted that credit card information was not compromised, since that data is stored on a separate server.
* [eBay data breach: What you need to do now (CBS News)](https://www.cbsnews.com/news/massive-data-breach-at-ebay-change-your-password-now/)

**Key Communications Takeaways:**

* **In the wake of a data breach, it’s imperative that a company responds to customers in a swift and efficient manner.** There were some eBay customers that took to social media to complain that the email notification from eBay providing them with instructions to reset their passwords took hours, and even days, to arrive. When notifying customers and stakeholders of a data breach of this extent, it’s important to ensure communication is done efficiently to prevent further backlash.
* **When communicating to stakeholders on a cyber incident, it is important to be as specific as possible.** eBay received criticism for not providing enough details on the nature of the breach, including when or how the breach was detected, how long data was compromised for, and what is being done to prevent a similar incident from happening again.

* **Because elected officials are quick to engage on high-profile data security incidents when they have an impact on their constituents, companies must be prepared to respond to increased scrutiny and media coverage.** In the wake of the data breach, New York’s attorney general called on eBay to provide free credit monitoring services to users, but the company had no plans to compensate customers or offer free credit monitoring.

**JP Morgan Chase  
  
Disclosure Date:** October 2014

**Situation Overview:**

JPMorgan revealed that 76 million households and seven million small businesses had their private data compromised in a cyberattack. User contact information — names, addresses, phone numbers and email addresses — and internal JPMorgan Chase information relating to such users had been compromised. There was no evidence that account information for such affected customers – account numbers, passwords, user IDs, dates of birth or Social Security numbers – was compromised during the attack. The data breach is considered one of the most serious intrusions into an American corporation's information system and one of the largest data breaches in history.

**Disclosure Materials:**

* Who disclosed the breach? JP Morgan Chase (The original [SEC filing](https://investor.shareholder.com/jpmorganchase/secfiling.cfm?filingID=1193125-14-362173) is no longer available)
* Disclosure materials:

[JP Morgan reveals data breach affected 76 million households (USA Today)](https://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/)

SAN FRANCISCO — The cyberattack on JPMorgan Chase & Co., first announced in July, compromised information from 76 million households and 7 million small businesses, the company revealed Thursday in a filing with the Securities and Exchange Commission.

Contact information, including name, address, phone number and e-mail address, as well as internal JPMorgan Chase information about the users, was compromised, the filing said. However the bank said no customer money appears to have been stolen.

JPMorgan said "there is no evidence that account information for such affected customers — account numbers, passwords, user IDs, dates of birth or Social Security numbers — was compromised during this attack."

The attack is one of the largest corporate breaches thus far reported.

More chillingly, a report Thursday in The New York Times said that the hackers were able to gain "the highest level of administrative privilege" on more than 90 of the bank's servers, according to people the newspaper spoke with who were familiar with the forensic investigation of the breach.

That means they "had root" on the servers of one of the largest banks in the world — they "could transfer funds, disclose information, close accounts, and basically do whatever they want to the data," said Jeff Williams, chief technology officer with Contrast Security in Palo Alto, Calif.

In its SEC filing, JPMorgan said as of Oct. 2 it had not "seen any unusual customer fraud related to this incident."

"This is a truly remarkable attack, but not just in its scope — hackers successfully penetrated one of the most secure organizations on this planet and they stole absolutely nothing of value — no money, no Social Security numbers, no passwords," said John Gunn, with Vasco Data Security International in Chicago.

"Persistence like that, with no stolen money, is due to a future planned operation — or that the objective was to identify data that was material in some other aspect," said J.J. Thompson of Rook Security in Indianapolis.

"This could be to track down a person of interest by observing financial transaction locations, to plans future large scale disruption when they know their competitor plans to wire funds to close a deal, or any other odd scenario you could see on (the TV show) 'Blacklist,'" he said.

Whether there really was an attack or not, consumers should beware of "piggyback attacks" in which criminals launch social engineering attacks making use of customer anxiety after reports of a big-name breach.

"The usual advice applies: If you get an e-mail or a call from a JP Morgan rep, feel free to thank them for contacting you and hang up. Customers should always initiate that contact by looking at their credit card or statement for the contact number; you simply can't trust that an incoming call or e-mail is legitimate and not a phishing attempt," said Tod Beardsley, engineering manager with security firm Rapid7.

# # #

**Media Details:**

* Media coverage surrounding the JPMorgan Chase cyber breach was significant, with coverage from top-tier outlets such as Associated Press, The New York Times, Reuters, and The Wall Street Journal, as well as coverage from top trade publications. The first round of coverage in October of 2014 was focused on the news that the data of 76 million households and 7 million small businesses had been compromised. In December of 2014, it was revealed that the data breach was a result of JPMorgan Chase failing to provide a two-factor authentication for one of its servers, leading to a second round of media coverage. Since JPMorgan Chase holds such highly privileged and confidential information and is regarded as one of the world’s leading financial institutions, this breach was heavily covered by media.
* [JPMorgan Chase Hacking Affects 76 Million Households (The New York Times)](https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/)
* [Neglected Server Provided Entry for JPMorgan Hackers (The New York Times)](https://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/)

**Key Communications Takeaways:**

* **Companies that operate in the financial sector need to be well-equipped to deal with cyber breaches.** Because of the nature of the work that JPMorgan Chase does and the type of information they have access to, they are more likely to be highly scrutinized than other companies. It is imperative that any major financial institution has a rigid and structured plan in place on how to detect and respond to cyber breaches.
* **Be transparent about what is being done to ensure a breach won’t happen again in the future.** In the aftermath of the attack, JPMorgan set up a “business control group” of about a dozen technology and cybersecurity executives to assess the fallout and to prevent hackers from breaching its network in the future. Subsequent media coverage reported on the creation of this new group, showing what the company is doing to move forward
* **Because elected officials are quick to engage on high-profile data security incidents, companies must be prepared to respond to increased scrutiny.** President Obama and national security officials took an interest in the JPMorgan Chase data breach. When dealing with matters that could have an impact on national security, it’s important for companies to be well-equipped to respond effectively.

# **Sony**

**Disclosure Date:** December 2014

**Situation Overview:**

In late November 2014, Sony Pictures Entertainment was hacked by a group calling itself the Guardians of Peace. The hackers, who are widely believed to be working in at least some capacity with North Korea, stole huge amounts of information off of Sony's network. They leaked the information to journalists, who wrote about confidential topics Sony employees had said to each other. Then the hackers, via the website Pastebin, threatened to commit acts of terrorism against movie theaters, demanding that Sony cancel the planned release of *The Interview*, a comedy about two Americans who assassinate North Korean leader Kim Jong Un. Initially, Sony reacted by shelving the movie. Critics, including President Obama, warned that capitulating in the face of terrorist threats would set a bad precedent. Then the studio reversed itself, releasing the movie in select theaters and online.

**Disclosure Materials:**

* Who disclosed the breach? Sony Pictures Entertainment
* Press release:

[Cyber Attack Notification and AllClear ID Services (Sony)](https://www.prnewswire.com/news-releases/cyber-attack-notification-and-allclear-id-services-300010217.html)

As is being widely reported in the press, Sony Pictures Entertainment (SPE) experienced a significant system disruption on Monday, November 24, 2014. SPE has determined that the cause of the disruption was a brazen cyber attack. After identifying the disruption, SPE took prompt action to contain the cyber attack, engaged recognized security consultants and contacted law enforcement.

SPE learned on December 1, 2014, that the security of certain personally identifiable information about its current and former employees, and their dependents, that participated in SPE health plans and other benefits, and certain production employees potentially may have been compromised. Although SPE is in the process of investigating the scope of the cyber attack, SPE believes that the following types of personally identifiable information that such individuals provided to SPE potentially may have been obtained by unauthorized individuals: (i) name, (ii) address, (iii) social security number, driver's license number, passport number, and/or other government identifier, (iv) bank account information, (v) credit card information for corporate travel and expense, (vi) username and passwords, (vii) compensation and (viii) other employment related information. In addition, unauthorized individuals may have obtained (ix) HIPAA protected health information, such as name, social security number, claims appeals information submitted to SPE (including diagnosis), date of birth, home address, and member ID number to the extent that the potentially impacted individuals participated in SPE health plans, and (x) health/medical information provided to SPE outside of SPE health plans.

Also on December 1, 2014, SPE began the process of notifying employees that it would be providing identity theft protection services to them and to their dependents. SPE has continued to reach out to potentially impacted individuals with notification about this situation, to offer identity protection services and to provide them with information about how to protect themselves from identity theft and other potential loss. SPE is encouraging potentially impacted employees and former employees to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information, as neither SPE nor anyone acting on its behalf would contact them in any way, including by email, asking for credit card number, social security number/government identifier or other personally identifiable information. Individuals asked for this information can be confident SPE is not the entity asking. To protect against possible identity theft or other financial loss, SPE encourages potentially impacted employees and former employees to remain vigilant, review account statements, monitor credit reports to the extent available, change passwords and to enroll promptly in the identity theft protection services made available to them by SPE.

The purpose of this press release is to take further steps to make sure that potentially impacted individuals receive this information.

Potentially affected individuals can review the full text of individual notifications and/or obtain information about AllClear ID identity protection services that may be available to them at sonypictures.com or by calling the SPE Information and Support Hotline. The U.S. toll free number is: (866) 361-8961; the international number is: +1 (262) 222-0434.

# # #

**Media Details:**

* Media coverage on the Sony Pictures hack lasted multiple weeks, with the lens of coverage shifting as more information was released. The media first reported that Sony Pictures had been hacked on November 24, 2014 – the same day that the first significant system distribution occurred. Then, media coverage shifted to focus on the link between the hack and North Korea’s potential involvement. Next, media coverage shifted to focus on the leaked emails between Sony executives, with multiple outlets releasing the actual correspondence. The Sony Pictures hack was covered by numerous international, top-tier, local, and trade outlets, and is still being referenced years later as one of the largest cybersecurity breaches of the modern-era.
* [Inside the Sony Hack (Slate)](http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html)

**Key Communications Takeaways:**

* **Lack of a defined strategy is detrimental to a company’s response and therefore, advanced scenario planning is critical.** Sony’s lack of a well-refined or structured plan to address a potential cyber-related incident led to a chaotic environment for employees and stakeholders. The company’s communications approach seemed to lack prior preparation and a sustainable strategy. The company was quickly forced into a reactive media strategy – triaging news reports about a series of response missteps – and seemed unable to keep up with the influx of public and media attention.
* **Because elected officials are quick to engage on high-profile data security incidents when they have an impact on their constituents, companies must be prepared to respond to increased scrutiny and media coverage.** Because of the sensitive nature of the information released, as well as the allegations that the breach could have been initiated by North Korean actors, elected officials were quick to engage in the conversation.
* **While attribution is important, it sometimes doesn’t matter.** In the wake of the breach, Sony Pictures was focused on finding the culprit of the hack and quick to point a finger at North Korean involvement. While finding the culprit of the breach is important, communicating to stakeholders about what is being done in the wake of the breach is equally as important. In some cases, accountability is equally as important as attribution.

# 

# **LinkedIn**

**Disclosure Date:** May 2016

**Situation Overview:**

In 2012, a hacker stole 6.5 million encrypted passwords from LinkedIn and posted them to a Russian crime forum. In 2016, a Russian hacker who goes by “Peace,” sold 117 million email and password combinations on a dark web marketplace. The going rate for the loot was five Bitcoins, or about $2,300. Motherboard said it received a portion of the data—about one million credentials—from Leaked Source, a paid search engine for hacked data that claims to have acquired a total of 167 million of the leaked login credentials. The news outlet verified that at least one of the hacked accounts is legitimate by confirming details with one of the victims. A person who represented Leaked Source, which has been analyzing the stolen data, said in an email that 160 million of the compromised accounts had unique email addresses, while the remaining 7 million only included numerical user ids and passwords. The spokesperson said that the site’s administrators did not have access to the 6.5 million credentials initially released in 2012, meaning they were unable to check whether they are included as part of the latest set.

**Disclosure Materials:**

* Who disclosed the breach? Media ([Mother Board](https://motherboard.vice.com/en_us/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password))
* Disclosure materials:

[Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords (Mother Board)](https://motherboard.vice.com/en_us/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password)

A hacker is trying to sell the account information, including emails and passwords, of 117 million LinkedIn users.

The hacker, who goes by the name "Peace," told Motherboard that the data was stolen during the LinkedIn breach of 2012. At the time, only around 6.5 million encrypted passwords were posted online, and LinkedIn never clarified how many users were affected by that breach.

Turns out it was much worse than anybody thought.

Peace is selling the data on the dark web illegal marketplace The Real Deal for 5 bitcoin (around $2,200). The paid hacked data search engine LeakedSource also claims to have obtained the data. Both Peace and the one of the people behind LeakedSource said that there are 167 million accounts in the hacked database. Of those, around 117 million have both emails and encrypted passwords.

"It is only coming to the surface now. People may not have taken it very seriously back then as it was not spread," one of the people behind LeakedSource told me. "To my knowledge the database was kept within a small group of Russians."

LeakedSource provided Motherboard with a sample of almost one million credentials, which included email addresses, hashed passwords, and the corresponding hacked passwords. The passwords were originally encrypted or hashed with the SHA1 algorithm, with no "salt," which is a series of random digits attached to the end of hashes to make them harder to be cracked.

One of the operators of LeakedSource told Motherboard in an online chat that so far they have cracked "90% of the passwords in 72 hours."

Troy Hunt, a security researcher who maintains the breach notification site "Have I Been Pwned?," reached out to some of the victims of the data breach. Two of them confirmed to Hunt that they indeed were users of LinkedIn and that the password he shared with them was the one they were using at the time of the breach. Motherboard was able to confirm a third victim.

One of the victims told Motherboard that the password in the sample was their current one, though he changed it as soon as Hunt reached out no notify him of the breach.

"Having a password out there feels like someone being able to let themselves in to your private space whenever they like, without you knowing," the victim, who asked to remain anonymous, said in an email.

When reached for comment on Tuesday, LinkedIn spokesperson Hani Durzy told Motherboard that the company's security team was looking into the incident, but that at the time they couldn't confirm whether the data was legitimate. Durzy, however, also admitted that the 6.5 million hashes that were posted online in 2012 were not necessarily all of the passwords stolen.

"We don't know how much was taken," Durzy told me in a phone call.

The lesson: For LinkedIn, the lesson is the same as four years ago: don't store passwords in an insecure way. As for LinkedIn users, if you didn't already change your password four years ago, change it again, especially if you use it on other services (and please stop reusing passwords).

"The prevalence of password reuse means we'll see that unlock other accounts too," Hunt told me.

Another lesson is that even old hacked data can sometimes be valuable, given that some of these passwords might still be valid.

UPDATE, May 18, 12:32 p.m. ET: LinkedIn confirmed on Wednesday that the new data is legitimate.

"Yesterday, we became aware of an additional set of data that had just been released that claims to be email and hashed password combinations of more than 100 million LinkedIn members from that same theft in 2012," the company's chief information security officer Cory Scott wrote in a blog post. "We are taking immediate steps to invalidate the passwords of the accounts impacted, and we will contact those members to reset their passwords. We have no indication that this is as a result of a new security breach."

Scott also encouraged users to use two-factor authentication and use strong passwords.

# # #

**Media Details:**

* The LinkedIn breach received coverage from significant news outlets in the US, including Fortune, Forbes, CNN and The Wall Street Journal. Most of the coverage surrounding the breach was neutral and fact-based, while some outlets speculated why this breach is so bad, most citing the 2012 breach the company had suffered four years prior. LinkedIn was commended for its frequent updates as well as its comprehensive landing page.
* [LinkedIn 2012 Data Breach May Have Hit Over 100 Million (The Wall Street Journal)](https://www.wsj.com/articles/linkedin-2012-data-breach-may-have-hit-over-100-million-1463675653)

**Key Communications Takeaways:**

* **Take action immediately.** Upon learning about the breached data from 2012 being used again, LinkedIn took steps to invalidate the passwords of the impacted accounts and contacted those members to reset their passwords. In addition, LinkedIn provided extra steps users can take to keep their accounts as safe as possible.
* **Make information easily accessible**. LinkedIn was quick to establish a landing page with comprehensive information about the leak, suggestions for users and updates as they arrived. This allowed users to obtain facts easily and in one place.

# **MySpace**

**Disclosure Date:** May 31, 2016

**Situation Overview:**

Time Inc., which owns Myspace, said names and passwords from more than 360 million Myspace accounts were compromised. The data was limited to usernames, passwords and email addresses from the platform prior to June 11, 2013, when the site was relaunched with stronger account security. The website notified impacted users and worked with law enforcement to investigate the breach. It also invalidated affected users’ passwords. “We believe the data breach is attributed to Russian cyberhacker ‘Peace.’ This same individual is responsible for other recent criminal attacks, such as those on LinkedIn and Tumblr, and has claimed on the paid hacker search engine LeakedSource that the data is from a past breach. This is an ongoing investigation, and we will share more information as it becomes available,” Myspace said in a [blog post](https://myspace.com/pages/blog).

**Disclosure Materials:**

* Who disclosed the breach? Myspace ([Time Inc](https://www.businesswire.com/news/home/20160531005770/en/Time-Confirms-Breach-Myspace).)
* Press release:

[Time Inc. Confirms Breach of Myspace (Business Wire)](https://www.businesswire.com/news/home/20160531005770/en/Time-Confirms-Breach-Myspace)

NEW YORK--(BUSINESS WIRE)--Time Inc. (NYSE:TIME) today confirmed reports that Myspace, a Time Inc. company and social networking site, has been the victim of a hacking incident. Shortly before the Memorial Day weekend, the Myspace technical security team became aware that stolen Myspace user login data was being made available in an online hacker forum. The compromised data is limited to a portion of Myspace usernames, passwords and email addresses, from the old Myspace platform prior to June 11, 2013—when the site was relaunched with significant steps to strengthen account security.

The Myspace breach does not affect any of Time Inc.’s systems, subscriber information or other media properties and does not appear to include financial data of any kind.

As Myspace has already reported, it is in the process of notifying all affected users and working proactively with law enforcement authorities to resolve this issue. Myspace has also invalidated the passwords of all known affected users and is monitoring for suspicious activity that might occur on Myspace accounts.

Jeff Bairstow, Time Inc. Executive Vice President and Chief Financial Officer, stated, “We take the security and privacy of customer data and information extremely seriously—especially in an age when malicious hackers are increasingly sophisticated and breaches across all industries have become all too common. Our information security and privacy teams are doing everything we can to support the Myspace team.”

For more information, please visit <https://myspace.com/pages/blog>.

# # #

**Media Details:**

* While some top-tier media outlets, including USA Today, covered the MySpace data breach, most of the coverage came from tech and cyber-focused trade publications. Coverage lasted for a few days and then died down quickly, with subsequent media coverage only including passing mentions of the data breach. The majority of coverage included statements from Time Inc. and MySpace officials.
* [360 million Myspace accounts breached (USA Today)](https://www.usatoday.com/story/tech/2016/05/31/360-million-myspace-accounts-breached/85183200/)

**Key Communications Takeaways:**

* **Timely and accurate notification to the public will reduce public scrutiny.** Time Inc. was quick to issue a statement on the incident, which helped them establish a sense of trust and credibility in the weeks following. As a result, the majority of media coverage included the initial and subsequent statements from company officials.
* **Being as detailed and transparent as possible when disclosing a cyber incident will ensure shareholder trust.** When announcing the cyber incident, Time Inc. announced who was responsible for the attack – Russian cyber hacker, “Peace.” Additionally, Time Inc. was transparent that they had been working closely with law enforcement agencies to identify the perpetrator, allowing them to create a sense of trust and legitimacy.

# **Verizon**

**Disclosure Date:** July 2017

**Situation Overview:**

The personal data of 6 million Verizon customers was leaked online. The security issue, uncovered by research from cybersecurity firm UpGuard, was caused by a misconfigured security setting on a cloud server due to "human error." At first, it was believed that the error made customer phone numbers, names, and some PIN codes publicly available online. However, it was later discovered that the PINs that were made available during the breach weren’t actually linked to customer accounts but rather were numbers used to authenticate customers at call centers. No loss or theft of customer information occurred. UpGuard initially said the error could impact up to 14 million accounts. Chris Vickery, a researcher at UpGuard, discovered the Verizon data was exposed by NICE Systems, an Israel-based company Verizon was working with to facilitate customer service calls. The data was collected over a six-month time span. Vickery alerted Verizon to the leak on June 13. The security hole was closed on June 22. The incident stemmed from NICE security measures that were not set up properly. The company made a security setting public, instead of private, on an Amazon S3 storage server – a common technology used by businesses to keep data in the cloud.

**Disclosure Materials:**

* Who disclosed the breach? Media ([ZDNet](https://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/))
* Disclosure materials:

[Millions of Verizon customer records exposed in security lapse (ZDNet)](https://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/)

An Israeli technology company has exposed millions of Verizon customer records, ZDNet has learned.

As many as 14 million records of subscribers who called the phone giant's customer services in the past six months were found on an unprotected Amazon S3 storage server controlled by an employee of Nice Systems, a Ra'anana, Israel-based company. The data was downloadable by anyone with the easy-to-guess web address.

Nice, which counts 85 of the Fortune 100 as customers, plays in two main enterprise software markets: customer engagement and financial crime and compliance including tools that prevent fraud and money laundering. Nice's 2016 revenue was $1.01 billion, up from $926.9 million in the previous year. The financial services sector is Nice's biggest industry in terms of customers, with telecom companies such as Verizon a key vertical. The company has more than 25,000 customers in about 150 countries.

Privacy watchdogs have linked the company to several government intelligence agencies, and it's known to work closely with surveillance and phone cracking firms Hacking Team and Cellebrite. In regulatory filings with the Securities and Exchange Commission, Nice noted that it can't control what customers do with its software. "Our products may also be intentionally misused or abused by clients who use our products," said Nice in its annual report.

Chris Vickery, director of cyber risk research at security firm UpGuard, who found the data, privately told Verizon of the exposure shortly after it was discovered in late-June.

It took over a week before the data was eventually secured.

The customer records were contained in log files that were generated when Verizon customers in the last six months called customer service. These interactions are recorded, obtained, and analyzed by Nice, which says it can "realize intent, and extract and leverage insights to deliver impact in real time." Verizon uses that data to verify account holders and to improve customer service.

Each record included a customer's name, a cell phone number, and their account PIN -- which if obtained would grant anyone access to a subscriber's account, according to a Verizon call center representative, who spoke on the condition of anonymity as they were not authorized to speak to the press.

Several security experts briefed on the exposure prior to publication warned of phone hijacking and account takeovers, which could allow hackers to break into a person's email and social media accounts protected even by two-factor authentication.

Verizon has over 108 million post-paid wireless customers.

Six folders for each month from January through to June contained several daily log files, apparently recording customer calls from different US regions, based on the location of the company's datacenters, including Florida and Sacramento. Each record also contained hundreds of fields of additional data, including a customer's home address, email addresses, what kind of additional Verizon services a subscriber has, the current balance of their account, and if a subscriber has a Verizon federal government account, to name a few. One field also appeared to record a customer's "frustration score," by detecting if certain keywords are spoken by a customer during a call.

Although the logs referenced customer voice recordings, there were no audio files found on the server.

Some of the records were "masked" in what appears to be a redaction effort to prevent an unauthorized disclosure of private information. But most of the customer records are in part or entirely visible.

Ted Lieu, a Democratic congressman and computer science major, said the exposure was "highly troubling."

"I'm going to be asking the Judiciary Committee to hold a hearing on this issue because Congress needs to find out the scale and scope of what happened and to make sure it doesn't happen again," he told ZDNet.

Lieu, also a Verizon customer, said: "I would like to know if my data was breached."

Verizon said it was investigating how its customer data was improperly stored on the Amazon Web Services (AWS) server as "part of an authorized and ongoing project" to improve its customer service.

"Verizon provided the vendor with certain data to perform this work and authorized the vendor to set up AWS storage as part of this project," said a spokesperson. "Unfortunately, the vendor's employee incorrectly set their AWS storage to allow external access."

One account from a senior Verizon employee with knowledge of the situation said that the company was unaware that the data was being exfiltrated or exported, and Verizon had no control over the server.

The phone giant said that the "overwhelming majority of information in the data set has no external value."

"There is some personal information in the data set," said the spokesperson, "but as indicated earlier, there is no indication that the information has been compromised."

Verizon also would not say how it "masked" data, citing security concerns.

Nice said it too was investigating the exposure. A spokesperson said that none of its systems or products were breached and "no other Nice customer data was involved."

Vickery said, however, that there was evidence that data from Orange, a European telecoms provider was for a time also stored on the exposed server, according to Vickery, suggesting the data exposure may not be limited to Verizon. (Orange did not respond to a request for comment.)

A Nice spokesperson later said that the data was "part of a demo system," and did not comment further.

It remains unclear who else at Nice had access to the server, or if the data was downloaded by anyone else.

Verizon said that it had requested information on who had access to the storage. A spokesperson said Monday that an investigation determined "no other external party accessed the data." When pressed, the company would not say how it came to that conclusion.

# # #

**Media Details:**

* This data breach was heavily reported on for one week by top-tier media outlets, including international, national and local publications. The only negative coverage surrounding Verizon’s data breach was the cyber response team’s delayed response to the data exposure. This “breakdown in communications” delayed Verizon from closing millions of publicly exposed user files, which is what a few media outlets focused on when reporting about the incident. Besides that factor, media coverage was fact-based and largely neutral in tone.
* [Verizon Takes Heat for Delayed Response to Data Exposure (Channel Partners)](https://www.channelpartnersonline.com/2017/07/19/verizon-takes-heat-for-delayed-response-to-data-exposure/)

**Key Communications Takeaways:**

* **Always have an alert incident response team.** The man who discovered the leak, Chris Vickery, said that he called a Verizon employee on the cyber team and left a voice mail saying that he had found a serious leak and needed to discuss it. After never hearing a response, he went back to check on the leak a week later and found that it had not been closed. He then emailed Verizon’s cyber emergency team about the leak, warning that the data should be closed off and noting that he had flagged them about it a week prior. Had there been an incident response team, this situation wouldn’t have been as detrimental.
* **No company thinks it’s going to be them, until it is.** This cyberattack was “opportunistic”, meaning that the attackers gained access to systems through vulnerabilities that have either not been addressed by the company, vulnerabilities due to employee errors, or poor choices of cybersecurity solutions that fail to protect against the latest threats. This conclusion stresses the importance of choosing new tools and technology solutions that are protecting the organization in the evolving era of cyber attacks.

**Equifax  
  
Disclosure Date:** September 2017

**Situation Overview:**

Equifax, one of the three largest consumer credit reporting agencies in the United States, announced in September 2017 that its systems had been breached and the sensitive personal data of 148 million Americans had been compromised. The data breached included names, home addresses, phone numbers, dates of birth, social security numbers, and driver’s license numbers. The credit card numbers of approximately 209,000 consumers were also breached. The Equifax breach is unprecedented in scope and severity. There have been larger security breaches by other companies in the past, but the sensitivity of the personal information held by Equifax and the scale of the problem makes this breach unprecedented.

**Disclosure Materials:**

* Who disclosed the breach? Equifax
* Press release:

[Equifax Announces Cybersecurity Incident Involving Consumer Information (Equifax)](https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628)

ATLANTA, Sept. 7, 2017 /PRNewswire/ -- Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.

Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers - all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.comor contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. – 1:00 a.m. Eastern time.

In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries.

Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

CEO Smith said, "I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will."

# # #

**Media Details:**

* Overall, media coverage surrounding the breach was largely negative. Articles frequently reported missteps by Equifax, including issues with the company’s call center. The breach was covered in hundreds of international, national, regional, specialty and trade publications. Coverage of the breach remained heavy for months, and continued to rise when Equifax discovered that more people were affected by the hack.
* [Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says (Fortune)](http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/)

**Key Communications Takeaways:**

* **Lack of a defined strategy is detrimental to a company’s response and therefore, advanced scenario planning is critical.** After taking almost two months to publicly announce the incident, the company’s communications approach appeared to lack a prior preparation and sustainable strategy along with forward-thinking. The company was quickly forced into a reactive media strategy – triaging news reports about a series of response missteps – and seemed unable to keep up with the influx of public and media attention.
* **Timely and accurate notification to the public will reduce scrutiny.** Equifax’s slow response and public notification tarnished the relationship between the public and the company. Equifax failed to demonstrate that it had consumers’ best interests in mind by not only withholding news of the breach from the public – and its board of directors – but also through its lack of effective and useful consumer resources.
* **Companies in crisis are under a microscope and stakeholders are unforgiving of subsequent missteps, making a well-executed public response is critical to recovery.** A website hosted outside of its Equifax.com domain, an arbitration clause set on the main website to help victims, a wrong website link sent multiple times through Twitter, lack of information on the process and charging victims credit-freeze fees, were among Equifax’s most criticized actions by the media and the public. One mistake after another eroded Equifax’s credibility and the public’s perception that it had control of the situation.

# **Uber**

**Disclosure Date:** November 2017

**Situation Overview:**

Uber faced a data breach in 2016 that affected some 57 million customers, including both riders and drivers, revealing their names, email address and phone numbers. That affected group included 50 million riders and 7 million drivers; around 600,000 driver license numbers for U.S. drivers were also included in the breach. Uber did not report the incident to regulators or to affected customers, but instead paid $100,000 to “hackers” to get rid of the data in order to keep the breach under wraps. No security numbers or trip location information was taken in the attack, and that it doesn’t believe the info that was leaked was ever used, though it doesn’t specify who was responsible.

**Disclosure Materials:**

* Who disclosed the breach? Media ([Bloomberg](https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data))
* Disclosure materials:

[Uber Paid Hackers to Delete Stolen Data on 57 Million People (Bloomberg)](https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data)

Hackers stole the personal data of 57 million customers and drivers from Uber Technologies Inc., a massive breach that the company concealed for more than a year. This week, the ride-hailing firm ousted its chief security officer and one of his deputies for their roles in keeping the hack under wraps, which included a $100,000 payment to the attackers.

Compromised data from the October 2016 attack included names, email addresses and phone numbers of 50 million Uber riders around the world, the company told Bloomberg on Tuesday. The personal information of about 7 million drivers was accessed as well, including some 600,000 U.S. driver’s license numbers. No Social Security numbers, credit card information, trip location details or other data were taken, Uber said.

At the time of the incident, Uber was negotiating with U.S. regulators investigating separate claims of privacy violations. Uber now says it had a legal obligation to report the hack to regulators and to drivers whose license numbers were taken. Instead, the company paid hackers to delete the data and keep the breach quiet. Uber said it believes the information was never used but declined to disclose the identities of the attackers.

“None of this should have happened, and I will not make excuses for it,” Dara Khosrowshahi, who took over as chief executive officer in September, said in an emailed statement. “We are changing the way we do business.”

After Uber’s disclosure Tuesday, New York Attorney General Eric Schneiderman launched an investigation into the hack, his spokeswoman Amy Spitalnick said. The company was also sued for negligence over the breach by a customer seeking class-action status.

Hackers have successfully infiltrated numerous companies in recent years. The Uber breach, while large, is dwarfed by those at Yahoo, MySpace, Target Corp., Anthem Inc. and Equifax Inc. What’s more alarming are the extreme measures Uber took to hide the attack. The breach is the latest scandal Khosrowshahi inherits from his predecessor, Travis Kalanick.

Kalanick, Uber’s co-founder and former CEO, learned of the hack in November 2016, a month after it took place, the company said. Uber had just settled a lawsuit with the New York attorney general over data security disclosures and was in the process of negotiating with the Federal Trade Commission over the handling of consumer data. Kalanick declined to comment on the hack.

Joe Sullivan, the outgoing security chief, spearheaded the response to the hack last year, a spokesman told Bloomberg. Sullivan, a onetime federal prosecutor who joined Uber in 2015 from Facebook Inc., has been at the center of much of the decision-making that has come back to bite Uber this year. Bloomberg reported last month that the board commissioned an investigation into the activities of Sullivan’s security team. This project, conducted by an outside law firm, discovered the hack and the failure to disclose, Uber said.

Here’s how the hack went down: Two attackers accessed a private GitHub coding site used by Uber software engineers and then used login credentials they obtained there to access data stored on an Amazon Web Services account that handled computing tasks for the company. From there, the hackers discovered an archive of rider and driver information. Later, they emailed Uber asking for money, according to the company.

A patchwork of state and federal laws require companies to alert people and government agencies when sensitive data breaches occur. Uber said it was obligated to report the hack of driver’s license information and failed to do so.

“At the time of the incident, we took immediate steps to secure the data and shut down further unauthorized access by the individuals,” Khosrowshahi said. “We also implemented security measures to restrict access to and strengthen controls on our cloud-based storage accounts.”

Uber has earned a reputation for flouting regulations in areas where it has operated since its founding in 2009. The U.S. has opened at least five criminal probes into possible bribes, illicit software, questionable pricing schemes and theft of a competitor’s intellectual property, people familiar with the matters have said. The San Francisco-based company also faces dozens of civil suits.

U.K. regulators including the National Crime Agency are also looking into the scale of the breach. London and other governments have previously taken steps toward banning the service, citing what they say is reckless behavior by Uber.

In January 2016, the New York attorney general fined Uber $20,000 for failing to promptly disclose an earlier data breach in 2014. After last year’s cyberattack, the company was negotiating with the FTC on a privacy settlement even as it haggled with the hackers on containing the breach, Uber said. The company finally agreed to the FTC settlement three months ago, without admitting wrongdoing and before telling the agency about last year’s attack.

The new CEO said his goal is to change Uber’s ways. Uber said it informed New York’s attorney general and the FTC about the October 2016 hack for the first time on Tuesday. Khosrowshahi asked for the resignation of Sullivan and fired Craig Clark, a senior lawyer who reported to Sullivan. The men didn’t immediately respond to requests for comment.

Khosrowshahi said in his emailed statement: “While I can’t erase the past, I can commit on behalf of every Uber employee that we will learn from our mistakes.”

The company said its investigation found that Salle Yoo, the outgoing chief legal officer who has been scrutinized for her responses to other matters, hadn’t been told about the incident. Her replacement, Tony West, will start at Uber on Wednesday and has been briefed on the cyberattack.

Kalanick was ousted as CEO in June under pressure from investors, who said he put the company at legal risk. He remains on the board and recently filled two seats he controlled.

Uber said it has hired Matt Olsen, a former general counsel at the National Security Agency and director of the National Counterterrorism Center, as an adviser. He will help the company restructure its security teams. Uber hired Mandiant, a cybersecurity firm owned by FireEye Inc., to investigate the hack.

The company plans to release a statement to customers saying it has seen “no evidence of fraud or misuse tied to the incident.” Uber said it will provide drivers whose licenses were compromised with free credit protection monitoring and identity theft protection.

# # #

[2016 Data Security Incident (Uber)](https://www.uber.com/newsroom/2016-data-incident/)

As Uber’s CEO, it’s my job to set our course for the future, which begins with building a company that every Uber employee, partner and customer can be proud of. For that to happen, we have to be honest and transparent as we work to repair our past mistakes.

I recently learned that in late 2016 we became aware that two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use. The incident did not breach our corporate systems or infrastructure.

Our outside forensics experts have not seen any indication that trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth were downloaded. However, the individuals were able to download files containing a significant amount of other information, including:

* The names and driver’s license numbers of around 600,000 drivers in the United States. Drivers can learn more here.
* Some personal information of 57 million Uber users around the world, including the drivers described above. This information included names, email addresses and mobile phone numbers. Riders can learn more here.

At the time of the incident, we took immediate steps to secure the data and shut down further unauthorized access by the individuals. We subsequently identified the individuals and obtained assurances that the downloaded data had been destroyed. We also implemented security measures to restrict access to and strengthen controls on our cloud-based storage accounts.

You may be asking why we are just talking about this now, a year later. I had the same question, so I immediately asked for a thorough investigation of what happened and how we handled it. What I learned, particularly around our failure to notify affected individuals or regulators last year, has prompted me to take several actions:

* I’ve asked Matt Olsen, a co-founder of a cybersecurity consulting firm and former general counsel of the National Security Agency and director of the National Counterterrorism Center, to help me think through how best to guide and structure our security teams and processes going forward. Effective today, two of the individuals who led the response to this incident are no longer with the company.
* We are individually notifying the drivers whose driver’s license numbers were downloaded.
* We are providing these drivers with free credit monitoring and identity theft protection.
* We are notifying regulatory authorities.
* While we have not seen evidence of fraud or misuse tied to the incident, we are monitoring the affected accounts and have flagged them for additional fraud protection.

None of this should have happened, and I will not make excuses for it. While I can’t erase the past, I can commit on behalf of every Uber employee that we will learn from our mistakes. We are changing the way we do business, putting integrity at the core of every decision we make and working hard to earn the trust of our customers.

# # #

**Media Details:**

* Overall, media coverage surrounding the Uber data breach was largely negative, focusing on Uber’s attempt to conceal the breach from stakeholders by paying off the hackers. Once Bloomberg broke the story, the news was covered by numerous international, trade, local, and top-tier outlets, including, Reuters, The New York Times, CNBC, and The Wall Street Journal. Subsequent media coverage reported on the multiple lawsuits being filed by individual and government officials against Uber, as well as the firing of multiple Uber executives, including founder and former CEO Travis Kalanick.
* [Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data (The New York Times)](https://www.nytimes.com/2017/11/21/technology/uber-hack.html)

**Key Communications Takeaways:**

* **Attempting to conceal a data breach will lead to a loss of trust from stakeholders.** Uber’s attempt to conceal the data breach from stakeholders led to highly critical media coverage and a loss of trust from customers, investors, regulators and employees.

* **Prompt detection and response are critical.** Uber’s failure to promptly disclose the details of the hack tarnished its relationship with many of its stakeholders. Uber failed to demonstrate that it had its stakeholders’ best interests in mind, while simultaneously breaking the law by failing to disclose the details of the hack.
* **Stakeholders are unforgiving, especially when a company has a history of missteps.** Because Uber had previously faced a number of other issues (sexual harassment allegations, fair wage issues, numerous lawsuits, etc.), stakeholders were less willing to forgive another misstep. As a result, Uber’s decision to not immediately disclose the breach, led to a further loss of trust from key stakeholders, making it harder to regain that trust in the future.

# **Under Armour – MyFitnessPal**

**Disclosure Date:** March 29, 2018

**Situation Overview:**

In late March, Under Armour announced that a data breach affected an estimated 150 million users of its food and nutrition app, MyFitnessPal. Under Armour first became aware of a potential breach on March 25, when the company discovered an unauthorized party had accessed MyFitnessPal user data in February. Under Armour took steps to notify affected users, and proceeded to work with data security firms and law enforcement to assist in its investigation. The affected information included usernames, email addresses, and hashed passwords. Payment information was not affected by the breach.

**Disclosure Materials:**

* Who disclosed the breach? Under Armour
* Press release:

[Under Armour notifies MyFitnessPal users of data security issue (Under Armour)](http://investor.underarmour.com/news-releases/news-release-details/under-armour-notifies-myfitnesspal-users-data-security-issue)

BALTIMORE, March 29, 2018 /PRNewswire/ -- Under Armour, Inc. (NYSE: UA, UAA) today announced that it is notifying users of MyFitnessPal - the company's food and nutrition application and website - about a data security issue. On March 25, the MyFitnessPal team became aware that an unauthorized party acquired data associated with MyFitnessPal user accounts in late February 2018. The company quickly took steps to determine the nature and scope of the issue and to alert the MyFitnessPal community of the incident.

Under Armour is working with leading data security firms to assist in its investigation, and also coordinating with law enforcement authorities. The investigation indicates that the affected information included usernames, email addresses, and hashed passwords - the majority with the hashing function called bcrypt used to secure passwords.

The affected data did not include government-issued identifiers (such as Social Security numbers and driver's license numbers), which the company does not collect from users. Payment card data was also not affected because it is collected and processed separately. The company's investigation is ongoing, but indicates that approximately 150 million user accounts were affected by this issue.

Four days after learning of the issue, the company began notifying the MyFitnessPal community via email and through in-app messaging. The notice contains recommendations for MyFitnessPal users regarding account security steps they can take to help protect their information. The company will be requiring MyFitnessPal users to change their passwords and is urging users to do so immediately.

Additional information about this issue is available at https://content.myfitnesspal.com/security-information/FAQ.html.

# # #

**Media Details:**

* Since the information involved in the breach was not sensitive information, the MyFitnessPal breach did not receive a significant amount of negative media coverage. Although it was covered by top-tier, as well as international, national and local media outlets, the coverage lasted for only a week and was largely fact-based and neutral
* [The Under Armour hack was even worse than it had to be (Wired)](https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/)

**Key Communications Takeaways:**

* **If personally identifiable information is not compromised, stress this to the public.** In this incident, Under Armour was not dealing with sensitive customer information. The intrusion only exposed usernames, email addresses and passwords, indicating that Under Armour’s systems were at least segmented enough to protect PII. Under Armour stressed this its customers which, in turn, made the breach seem less serious in the public eye.
* **Let your customers know about your company’s security measures.** Under Armour told the public that it had used the well-regarded password hashing function "bcrypt" to convert most of the passwords it stored into unintelligible assortments of characters. When implemented properly, this cryptographic process makes it incredibly resource and time-consuming for attackers to attempt to "crack" the passwords and revert them to their useful form—after bcrypt hashing, a strong password can take decades to break, if not longer. As a result, even when hashed passwords leak they are still protected.
* **Be honest.** While Under Armour says it protected "the majority" of the passwords with bcrypt, the remainder weren't nearly so lucky. Instead, in a [Q&A site](https://content.myfitnesspal.com/security-information/FAQ.html) about the breach, Under Armour admitted that some proportion of the exposed passwords were only hashed using a notoriously weak function called SHA-1, which has had known flaws for a decade and was further discredited by research findings last year. "The MyFitnessPal account information that was not protected using bcrypt was protected with SHA-1, a 160-bit hashing function," Under Armour wrote in the Q&A.

**Facebook  
  
Disclosure Date:** September 28, 2018

**Situation Overview:**

Facebook announced in late September that an attack on its computer network had exposed the personal information of nearly 50 million users. The breach was the largest in the company’s 14-year history. The attackers exploited a feature in Facebook’s code to gain access to user accounts and potentially take control of them. Mark Zuckerberg said that the attackers were using Facebook developer APIs to obtain some information, like “name, gender, and hometowns” that’s linked to a user’s profile page.

**Disclosure Materials:**

* Who disclosed the breach? Facebook
* Press release:

[Security Update (Facebook)](https://newsroom.fb.com/news/2018/09/security-update/)

On the afternoon of Tuesday, September 25, our engineering team discovered a security issue affecting almost 50 million accounts. We’re taking this incredibly seriously and wanted to let everyone know what’s happened and the immediate action we’ve taken to protect people’s security.

Our investigation is still in its early stages. But it’s clear that attackers exploited a vulnerability in Facebook’s code that impacted “View As” a feature that lets people see what their own profile looks like to someone else. This allowed them to steal Facebook access tokens which they could then use to take over people’s accounts. Access tokens are the equivalent of digital keys that keep people logged in to Facebook so they don’t need to re-enter their password every time they use the app.

Here is the action we have already taken. First, we’ve fixed the vulnerability and informed law enforcement.

Second, we have reset the access tokens of the almost 50 million accounts we know were affected to protect their security. We’re also taking the precautionary step of resetting access tokens for another 40 million accounts that have been subject to a “View As” look-up in the last year. As a result, around 90 million people will now have to log back in to Facebook, or any of their apps that use Facebook Login. After they have logged back in, people will get a notification at the top of their News Feed explaining what happened.

Third, we’re temporarily turning off the “View As” feature while we conduct a thorough security review.

This attack exploited the complex interaction of multiple issues in our code. It stemmed from a change we made to our video uploading feature in July 2017, which impacted “View As.” The attackers not only needed to find this vulnerability and use it to get an access token, they then had to pivot from that account to others to steal more tokens.

Since we’ve only just started our investigation, we have yet to determine whether these accounts were misused or any information accessed. We also don’t know who’s behind these attacks or where they’re based. We’re working hard to better understand these details — and we will update this post when we have more information, or if the facts change. In addition, if we find more affected accounts, we will immediately reset their access tokens.

People’s privacy and security is incredibly important, and we’re sorry this happened. It’s why we’ve taken immediate action to secure these accounts and let users know what happened. There’s no need for anyone to change their passwords. But people who are having trouble logging back into Facebook — for example because they’ve forgotten their password — should visit our Help Center. And if anyone wants to take the precautionary action of logging out of Facebook, they should visit the “Security and Login” section in settings. It lists the places people are logged into Facebook with a one-click option to log out of them all.

# # #

**Media Details:**

* Since this breach was only months after the Cambridge Analytica scandal, Facebook was already facing scrutiny over how it handles the private information of its users. For this reason, a majority of media outlets concentrated on Facebook’s inability to keep customer information private. The breach was reported on by top-tier outlets, including [Forbes](https://www.forbes.com/sites/kateoflahertyuk/2018/09/29/facebook-data-breach-what-to-do-next/#5e61d21d2de3) and [CNBC](https://www.cnbc.com/2018/10/02/facebooks-muddy-account-breach-response-could-be-the-new-norm.html), as well as international, national and regional publications. In addition to comments on Facebook not being able to keep their users information safe, the company was also ridiculed by Facebook users for not being informed on whose accounts were breached and by whom they were breached.
* [Facebook’s muddy response to last week’s hack may become the new norm (CNBC)](https://www.cnbc.com/2018/10/02/facebooks-muddy-account-breach-response-could-be-the-new-norm.html)

**Key Communications Takeaways:**

* **Communicate to the public that cybersecurity investigations take time.** Facebook was ridiculed for being vague to its customers during the announcement of the cyber breach. The company did not update the public in a timely manner on whose accounts were affected and by whom the accounts were hacked. Due to the General Data Protection Regulation (GDPR) enacted last May in the European Union, fast but incomplete notifications are likely the new norm. For this reason, actively communicate to the public that your company is working to get answers and will update consumers as soon as that information becomes available.
* **Communicate that user privacy and protection is the priority.** During this breach, concerns about Facebook and its management rose as a cascade of privacy incidents hit the company. Additionally, Facebook representatives initially declined to comment on the breach, which leads customers to be uneasy. A simple statement acknowledging the breach and ensuring the public that their privacy is the top priority to the company is better than saying nothing at all.

# **Ticketfly**

**Disclosure Date:** August 8, 2018 by Ticketfly

**Situation Overview:**

A cyberattack towards Ticketfly caused the company to temporarily shut down its website while it consulted with a third-party investigating company. The message “Ticketfly HacKeD By IsHaKdZ. Your Security Down im Not Sorry” [sic] along with an image of Anonymous symbol Guy Fawkes, from V From Vendetta, and a Yandex email address were on the Ticketfly homepage. Approximately 27 million customers’ names, addresses, email addresses and phone numbers were obtained, however users’ financial information was not.

**Disclosure Materials:**

* Who disclosed the breach? Ticketfly
* Media release:

[Ticketfly cyber incident information](https://support.ticketfly.com/s/article/41507) (Ticketfly)

**Details**

In late May 2018, Ticketfly was the target of a malicious cyberattack. This page originally served as a place for Ticketfly to notify clients and fans of details of the investigation as they unfolded, including information about what personal data was accessed as a result of the attack. Now this page contains an overview of what happened. We are sorry this incident occurred.

**What happened**

* On May 30, 2018, we discovered unauthorized access to the Ticketfly platform.
* We take privacy and security very seriously and, upon first learning about this incident, took swift action to secure the data of our clients and fans. This included making the difficult decision to temporarily take all Ticketfly systems offline while consulting with third-party forensic cybersecurity experts and vigorously investigating the incident.
* Our investigation confirmed that financial information, including credit and debit cards, was not accessed. Information, including names, addresses, email addresses and phone numbers, connected to approximately 27 million Ticketfly accounts was accessed. Please note that many people purchase tickets with multiple email accounts, so the number of individuals impacted is likely lower.
* As soon as we had confidence that we could bring the Ticketfly ticketing systems and websites back online safely and securely, we began the work to do so.
* The Ticketfly ticketing system and all websites have now been fully restored.

**What we’ve done**

* We forced a precautionary password reset for all ticket buyers and clients prior to bringing our systems back online.
* We completed a comprehensive review of our security protocols.
* We put in place an application firewall designed to provide an additional layer of security.
* We are in the process of implementing two-factor authentication for our clients.

**FAQs about the cyber incident and accessed data**

*What data was accessed through this cyber incident?*

Information accessed includes names, addresses, email addresses and phone numbers connected to Ticketfly accounts. No credit and debit card information was accessed.

*What about passwords?*

Passwords for Ticketfly ticket buyers were not accessed. As a precautionary measure, we forced a reset for all passwords for both ticket buyers and Ticketfly venue/promoter clients before we brought the system back online the morning of Saturday, June 2, 2018. There is no further action ticket buyers or Ticketfly clients need to take.

For Ticketfly venue/promoter clients (who are all within the US and Canada), we have no evidence that passwords were accessed. It is possible, however, that hashed values of client password credentials could have been accessed. Hashing is a way of scrambling a piece of data, making it generally incomprehensible. As a precautionary measure, in addition to resetting their password on our site, we also recommend that Ticketfly clients reset any other account that uses any of their Ticketfly credentials.

*How did this happen and what more can you share about the incident?*

We understand there is curiosity as to who perpetrated this attack, and how. Unfortunately, we are limited in what specific details we can share. We can convey that our enhanced security measures are intended to help make sure this does not happen again.

*Does the security risk from this intrusion continue to exist?*

We have no reason to believe the security risk from this intrusion currently exists in light of the enhanced security measures described above.

*What about my Ticketfly-powered website?*

All Ticketfly-powered venue and promoter websites are now back online.

# # #

**Media Details:**

* The coverage surrounding the Ticketfly breach came from a few large national sources, but the majority came from smaller niche tech outlets covering the story as it unfolded, including Engadget. The stories covering this breach lasted a few weeks, most likely because the breach disrupted Ticketfly’s business severely, as well as affecting its UK branch.
* [Data breach disrupts concert ticketing service Ticketfly (CBS)](https://www.cbsnews.com/news/ticketfly-eventbrite-data-breach-disruption-today-2018-06-03/)

**Key Communications Takeaways:**

* **Store passwords and other sensitive information separately from other less sensitive information.** While all data breaches are a cause for concern, the Ticketfly breach was not as immediately damaging as others because users’ passwords and other information were not stolen.
* **Don’t pay a hacker’s ransom.** The hacker, IsHaKdZ, claims he found a vulnerability in the Ticketfly website and attempted to report it to the company. He decided to exploit the vulnerability when he did not receive the 1 bitcoin he had asked for “for protection.” While it seems easier and appealing to pay off a hacker immediately, there is always the risk that they do not give you your data or they attack again in the future because they know you will pay.

# **T-Mobile**

**Disclosure Date:** August 20, 2018 by T-Mobile

**Situation Overview:**

T-Mobile experienced a data breach that compromised the personal information of approximately 2 million of its customers. Luckily, no financial information, social security numbers, or passwords were included in the breach. According to T-Mobile, an international group was behind the attack.

**Disclosure Materials:**

* Who disclosed the breach? T-Mobile
* Media release:

[T-Mobile Announcement](https://www.t-mobile.com/customers/6305378821) (T-Mobile)

Dear Customer –

Out of an abundance of caution, we wanted to let you know about an incident that we recently handled that may have impacted some of your personal information.

Our cyber-security team discovered and shut down unauthorized access to certain information, including yours, and we promptly reported it to authorities. None of your financial data (including credit card information) or social security numbers were involved, and no passwords were compromised. However, you should know that some of your personal information may have been exposed, which may have included one or more of the following: name, billing zip code, phone number, email address, account number, account type (prepaid or postpaid), and/or date of birth.

If you have questions about this incident or your account, please contact Customer Care at your convenience. If you are a T-Mobile customer, you can dial 611, use two-way messaging on MyT-Mobile.com, the T-Mobile App, or iMessage through Apple Business Chat. You can also request a call back or schedule a time for your Team of Experts to call you through both the T-Mobile App and MyT-Mobile.com. If you are a T-Mobile For Business or Metro PCS customer, just dial 611 from your mobile phone.

We take the security of your information very seriously and have a number of safeguards in place to protect your personal information from unauthorized access. We truly regret that this incident occurred and are so sorry for any inconvenience this has caused you.

# # #

**Media Details:**

* The coverage for the T-Mobile data breach mostly came from niche tech outlets, as well as articles from sources like USA TODAY. Coverage lasted approximately a week, the most frequent coverage occurring within the first four days of the breach’s occurrence.
* [T-Mobile discloses data breach of consumer information (USA TODAY)](https://www.usatoday.com/story/tech/nation-now/2018/08/24/t-mobile-hit-data-breach-consumer-information/1086512002/)

**Key Communications Takeaways:**

* **Offer various communication options for customers to choose from if they have questions.** T-Mobile alerted its affected customers quickly, and the company also provided multiple ways for customers to reach customer support if they had any questions regarding the breach or their account.
* **Make sure all communications are branded and consistent.** T-Mobile began notifying customers about the breach Friday morning using a text sent to affected accounts, however, this caused some criticism because the short URL used by the company looked like a phishing link. A short link was most likely used due to text-character limits; however, it is important to use credible channels of communication during a time of crisis, especially a data breach.
* **Provide as much information to consumers as possible.** While T-Mobile was quick to patch any vulnerabilities in its system and alert its customers, some key information was missing from the release. Mainly, users were left wondering just how many people were affected by the breach and how this will impact them.

# **Chegg**

**Disclosure Date:** September 25, 2018 by Chegg via SEC filing

**Situation Overview:**

Chegg discovered a data breach from April 29, 2018 months later on September 19, 2018, impacting close to 40 users. The information that may have been obtained in the breach could include a Chegg user’s name, email address, shipping address, Chegg username, and hashed Chegg password, however, hackers did not gain access to Social Security numbers nor financial information.

**Disclosure Materials:**

* Who disclosed the breach? Chegg, Inc.
* Media release:

[FORM 8-K](https://www.sec.gov/Archives/edgar/data/1364954/000136495418000187/cyrus.htm) (Chegg, Inc.)

**Item 7.01. Regulation FD Disclosure.**

In connection with the disclosure of the security incident discussed in Item 8.01 below, on September 25, 2018, Chegg, Inc. (the “Company” or “Chegg”) reaffirmed its previous guidance for the third quarter of 2018 as most recently stated in the press release issued on July 30, 2018 and furnished as an exhibit to a Current Report on Form 8‑K filed that day with the Securities and Exchange Commission (the “SEC”) (the “July Guidance”). Chegg also announced that it currently believes that the security incident discussed in Item 8.01 below will not have a material impact on its financial results for the full year ending December 31, 2018.

The information contained in this Item 7.01 shall not be deemed “filed” for purposes of Section 18 of the Securities Exchange Act of 1934, as amended, or otherwise subject to the liabilities of that section or Sections 11 and 12(a)(2) of the Securities Act of 1933, as amended. The information contained in this Item 2.02 shall not be incorporated by reference into any registration statement or other document filed by Chegg with the SEC, whether made before or after the date of this Current Report on Form 8‑K, regardless of any general incorporation language in such filing, except as shall be expressly set forth by specific reference in such filing.

**Item 8.01 Other Events.**

On September 19, 2018, Chegg learned that on or around April 29, 2018, an unauthorized party gained access to a Company database that hosts user data for chegg.com and certain of the Company’s family of brands such as EasyBib. The Company understands that the information that may have been obtained could include a Chegg user’s name, email address, shipping address, Chegg username, and hashed Chegg password. The investigation into the incident, which is supported by third-party forensics, is ongoing. To date, the Company understands that no social security numbers or financial information such as users’ credit card numbers or bank account information were obtained. The Company expects to start notifying approximately 40 million active and inactive registered users and certain regulatory authorities on September 26, 2018.

Chegg takes the security of its users’ information seriously and will be initiating a password reset process for all user accounts.

**Forward-Looking Statements**

This Current Report on Form 8‑K contains forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. All statements contained in this Current Report on Form 8‑K other than statements of historical fact, including statements regarding when the Company anticipates notifying affected users, are forward-looking statements. The words “believe,” “may,” “will,” “would,” “could,” “estimate,” “continue,” “anticipate,” “intend,” “project,” “endeavor,” “expect,” “plans to,” “if,” “future,” and similar expressions are intended to identify forward-looking statements. Forward-looking statements in this Form 8-K relate to, among other things, the anticipated timing and number of user notifications, the Company’s anticipated security enhancements and remediation efforts, the Company’s reaffirmed guidance for the third quarter of 2018 and belief regarding the impact of the security incident on full year financial results for 2018. We have based these forward-looking statements largely on our current expectations and projections about future events and trends that we believe may affect our financial condition, results of operations, business strategy, short-term and long-term business operations and objectives, and financial needs. These forward-looking statements are subject to a number of risks, uncertainties, and assumptions, including the impact of additional information concerning the security incident, including the scope of the unauthorized access and type of information accessed, costs released to the unauthorized access and related ongoing investigation and any resulting liabilities, the outcome of the ongoing investigation, uncertainty regarding any future civil litigation, governmental investigations and enforcement proceedings, uncertainties regarding the scope and effectiveness of security enhancements and remediation efforts, uncertainties regarding the impact to the Company’s brands and reputation, and uncertainties regarding the impact of the security incident, notification of users, security enhancements and remediation efforts on the Company’s business, financial position and results of operations, in addition to those risks those described in Part II.

# # #

**Media Details:**

* The coverage supporting the Chegg data breach came from a little more than 10 sources and lasted all of two days. While the articles mentioning the breach were mainly covering the event, it was also mentioned in end-of-the-year security recaps and lists closer to the end of the year and into early 2019.
* [Chegg to reset passwords for 40 million users after April 2018 hack (ZD Net)](https://www.zdnet.com/article/chegg-to-reset-passwords-for-40-million-users-after-april-2018-hack/)

**Key Communications Takeaways:**

* **Regularly monitor servers to ensure they are secure.** While Chegg was quick to force its users to reset their passwords, the breach went unnoticed for nearly five months. This gave hackers time to test the passwords the users may have used for other accounts, which causes even more harm. By checking for vulnerabilities and breaches frequently, companies are able to prevent risks from becoming any larger than necessary.
* **Use strong hashing algorithms when encrypting users’ passwords**. Although Chegg did not specify which hashing algorithm was used, it is something worth noting because some algorithms are known for being stronger than others.

# **Marriott**

**Disclosure Date:** November 2018

**Situation Overview:**

On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. Marriott recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that it was from the Starwood guest reservation database. That month, Marriott International announced that cyber thieves had stolen data on approximately 500 million customers. The information copied from the Starwood guest reservation database over time includes information about guests who made a reservation at a Starwood property, including names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest (“SPG”) account information, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences.

**Disclosure Materials:**

* Who disclosed the breach? Marriott International
* Press release:

[Marriott Announces Starwood Guest Reservation Database Security Incident](http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/)

Marriott has taken measures to investigate and address a data security incident involving the Starwood guest reservation database. On November 19, 2018, the investigation determined that there was unauthorized access to the database, which contained guest information relating to reservations at Starwood properties\* on or before September 10, 2018.

On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. The company recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.

The company has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest (“SPG”) account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and sometimes other data such as mailing address, email address, or other information.

Marriott reported this incident to law enforcement and continues to support their investigation. The company has already begun notifying regulatory authorities.

“We deeply regret this incident happened,” said Arne Sorenson, Marriott’s President and Chief Executive Officer. “We fell short of what our guests deserve and what we expect of ourselves. We are doing everything we can to support our guests, and using lessons learned to be better moving forward.”

“Today, Marriott is reaffirming our commitment to our guests around the world. We are working hard to ensure our guests have answers to questions about their personal information, with a dedicated website and call center. We will also continue to support the efforts of law enforcement and to work with leading security experts to improve. Finally, we are devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network,” Mr. Sorenson continued.

# # #

**Media Details:**

* The Marriott International breach received extremely heavy coverage for a month by international, national and regional publications, as well as all top-tier outlets. The media coverage ranged from neutral to negative and was largely fact-based. Referred to as “one of the top 5 worst hacks that directly impacts the general public”, Marriott International was ridiculed for admitting to knowing about this breach in early September, but waiting until late November to notify its guests. However, Marriott was positively acknowledged for updating its customers frequently on breach results as they became readily available. Additionally, Marriott had an easily-navigable and informative landing page on its website that detailed the breach, what was affected, who was impacted, and next steps.
* [Marriott’s breach response is so bad, security experts are filling in the gaps – at their own expense (Tech Crunch)](https://techcrunch.com/2018/12/03/marriott-data-breach-response-risk-phishing/)

**Key Communications Takeaways:**

* **Apologize to your customers when you are in the wrong.** Marriott International had excellent communications from its CEO, Arne Sorenson, with a separate page on its website dedicated to a detailed [statement](http://news.marriott.com/2018/01/statement-from-arne-sorenson-president-and-ceo-marriott-international-inc/) by Sorenson. The statement explained in detail the scope of the incident and stated how important privacy is to the company. In addition, the statement noted that The Marriott accepts full responsibility and is working to regain the trust of its customers.
* **Make sure all internal and external communications are perfect during a cyber breach.** Marriott sent its notification email from “email-marriott.com,” which is registered to a third party firm, CSC, on behalf of the hotel chain giant. But there was little else to suggest the email was at all legitimate — the domain didn’t load or have an identifying HTTPS certificate. In fact, there was no easy way to check that the domain is real, except a buried note on Marriott’s data breach notification site that confirms the domain as legitimate. In addition, this email was easily spoof-able.
* **In the midst of a major cyberbreach, have an easily navigable website.** Marriott’s website had a landing page dedicated to an FAQ during the cyber breach, as well as separate pages for informing the public on breach and investigation updates.

**Quora**  
 **Disclosure Date:** December 3, 2018 by Quora CEO Adam D’Angelo via The Quora Blog

**Situation Overview:**

Quora suffered a breach of 100 users’ email addresses, hashed passwords, and non-public information, including private messages. Quora discovered the breach on November 30, 2018 and began investigating. In the meantime, all users were logged out and forced to reset their password, which were then salted and hashed to prevent attackers from using it.

**Disclosure Materials:**

* Who disclosed the breach? Quora CEO Adam D’Angelo via The Quora Blog
* Media release:

[Quora Security Update](https://blog.quora.com/Quora-Security-Update) (The Quora Blog)

We recently discovered that some user data was compromised as a result of unauthorized access to one of our systems by a malicious third party. We are working rapidly to investigate the situation further and take the appropriate steps to prevent such incidents in the future.

We also want to be as transparent as possible without compromising our security systems or the steps we're taking, and in this post we’ll share what happened, what information was involved, what we're doing, and what you can do.

We're very sorry for any concern or inconvenience this may cause.

What happened

On Friday we discovered that some user data was compromised by a third party who gained unauthorized access to one of our systems. We're still investigating the precise causes and in addition to the work being conducted by our internal security teams, we have retained a leading digital forensics and security firm to assist us. We have also notified law enforcement officials.

While the investigation is still ongoing, we have already taken steps to contain the incident, and our efforts to protect our users and prevent this type of incident from happening in the future are our top priority as a company.

**What information was involved**

For approximately 100 million Quora users, the following information may have been compromised:

* Account information, e.g. name, email address, encrypted password (hashed using bcrypt with a salt that varies for each user), data imported from linked networks when authorized by users
* Public content and actions, e.g. questions, answers, comments, upvotes
* Non-public content and actions, e.g. answer requests, downvotes, direct messages (note that a low percentage of Quora users have sent or received such messages)

Questions and answers that were written anonymously are not affected by this breach as we do not store the identities of people who post anonymous content.

The overwhelming majority of the content accessed was already public on Quora, but the compromise of account and other private information is serious.

**What we are doing**

While our investigation continues, we're taking additional steps to improve our security:

* We’re in the process of notifying users whose data has been compromised.
* Out of an abundance of caution, we are logging out all Quora users who may have been affected, and, if they use a password as their authentication method, we are invalidating their passwords.
* We believe we’ve identified the root cause and taken steps to address the issue, although our investigation is ongoing and we’ll continue to make security improvements.

We will continue to work both internally and with our outside experts to gain a full understanding of what happened and take any further action as needed.

**What you can do**

We’ve included more detailed information about more specific questions you may have in our help center, which you can find here.

If you were affected, we will update you with relevant details via email.

While the passwords were encrypted (hashed using bcrypt with a salt that varies for each user), it is generally a best practice not to reuse the same password across multiple services, and we recommend that people change their passwords if they are doing so.

**Conclusion**

It is our responsibility to make sure things like this don’t happen, and we failed to meet that responsibility. We recognize that in order to maintain user trust, we need to work very hard to make sure this does not happen again. There’s little hope of sharing and growing the world’s knowledge if those doing so cannot feel safe and secure, and cannot trust that their information will remain private. We are continuing to work very hard to remedy the situation, and we hope over time to prove that we are worthy of your trust.

# # #

**Media Details:**

* The coverage surrounding the Quora data breach was short lived, mainly because the compromised information was not as sensitive as compared to other data breaches, which occur nearly daily. Coverage came from sources such as CNN, The New York Times, Fortune, TechCrunch, Engadget, and VICE.
* [Quora, the Q. and A. Site, Says Data Breach Affected 100 Million Users (The New York Times)](https://www.nytimes.com/2018/12/04/technology/quora-hack-data-breach.html)

**Key Communications Takeaways:**

* **Prompt users to act immediately.** Quora was quick to force users to change passwords, as well as recommend changing that password on other sites in case hackers try to use it. Not only does this prevent hackers from using Quora’s users accounts, it protects those same users on other sites from potentially more harmful breaches.
* **Store sensitive information separately.** While the breach affected email addresses, passwords and messages, no personal financial information had been compromised. This information was protected differently, and was safe from cyberattacks.

**Dow Jones  
  
Disclosure Date:** February 27, 2019 by Bob Diachenko via Security Discovery

**Situation Overview:**

On February 22, 2019 Bob Diachenko, an independent security researcher, found a copy of the Dow Jones Watchlist, a database containing 2,418,862 identity records on government officials and politicians from every country in the world, leaked online on a public Elasticsearch cluster. The watchlist, compiled from publicly available information, contained 2,418,862 records on prominent individuals who are considered high financial risks (i.e. capable of embezzlement, money laundering, accepting bribes, etc.)

Diachenko reached out to Dow Jones security incident response team on the same day he discovered the dataset, and the database was removed and replaced with the following statement:

*“This data is entirely derived from publicly available sources. At this time our review suggests this resulted from an authorized third party’s misconfiguration of an AWS server, and the data is no longer available.”*

**Disclosure Materials:**

* Who disclosed the breach? Bob Diachenko, posted to his Security Discovery blog
* Media release:

[Dow Jones Risk Screening Watchlist Exposed Publicly in a Major Data Breach](https://securitydiscovery.com/dow-jones-risk-screening-watchlist-exposed-publicly/)

On Feb 22 2019, I found a copy of the Dow Jones Watchlist dataset, sitting on a public Elasticsearch cluster 4.4GB in size and available for public access to anyone who knew where to look (hint: any public IoT search engine, such as BinaryEdge).

*“Used by eight of the world’s ten largest, global, financial institutions Dow Jones Watchlist is statistically proven to be the most accurate, complete, and up-to-date list of senior PEPs (politically exposed persons), their relatives and close associates”*.

The database I discovered contained an astonishing 2,418,862 records detailing:

* global coverage of senior Politically Expose Persons, their relatives, close associates, and the companies they are linked to.
* national and international government sanction lists and categories
* persons officially linked to, or convicted of, high-profile crime
* profile notes from Dow Jones including citing Federal agencies and law enforcement sources.

In other words, it contained the identities of government officials, politicians and people of political influence in every country of the world. The data is designed to help identify risks when researching an individual and efficient due diligence. Obviously banks use Watchlist data to identify money laundering and illicit payments through key information about a public figure’s identity.

Every record presented one or several lists where an individual was put:

* Politically Exposed Person (PEP)
* Special Interest Person (SIP) or Special Interest Entity (SIE)

*“Doing business with the wrong person just once can result in steep financial penalties for your organization and legal proceedings against key executives. The ensuing scandal can cause irreparable damage to your corporate reputation”*.

– quote from the Dow Jones sales brochure.

After reaching out to Dow Jones security incident response team on the same day when instance was discovered, database has been taken down with the following statement:

***This data is entirely derived from publicly available sources. At this time our review suggests this resulted from an authorized third party’s misconfiguration of an AWS server, and the data is no longer available.***

Publicly revealing the database beyond the aforementioned leak could be reckless: Watchlist database contains sensitive information on citizens regarding their alleged criminal histories and possible terrorist links.

Let’s face it we live in the age of Big Data where we are probably going to be on a list someday, but let’s hope that list is not leaked online or publically available? Big Data and “data mining” in this case allows Watchlist’s users to have a far better understanding of information and research than just a simple Google search can provide.

Dow Jones Watchlist is an online research database which aggregates licensed and publically available news, magazines, blogs etc from across the globe, but they also have a research team who updates these names and connections.

The information is then indexed, tagged and searchable.

What makes this data so much more valuable is the focus on premium and reputable sources. In the age of fake news and social engineering online it is easy to see how valuable this type of information would be to companies, governments, or individuals.

**About author and security researcher:**

Bob Diachenko has over 12 years experience working in corporate/product/internal communications with a strong focus on infosecurity, IT and technology. In the past Bob has worked with top tier media, government agencies, and law enforcement to help secure exposed data. Follow Bob on [Twitter](https://twitter.com/MayhemDayOne) and his blog on [Linkedin](https://www.linkedin.com/in/vdyachenko/), Email: bob@securitydiscovery.com

# # #

**Media Details:**

* The Dow Jones breach was mainly covered by niche technology media outlets such as Engadget, Tech Crunch and SC Magazine. Coverage focused on the breach itself and why, while the information in the dataset were technically public information, having the compiled reports exposed is reckless. Dow Jones spokespeople and other technology executives responded to news outlets regarding the issue.
* [Dow Jones’ watchlist of 2.4 million high-risk individuals has leaked (Tech Crunch)](https://techcrunch.com/2019/02/27/dow-jones-watchlist-leak/)

**Key Communication Takeaways:**

* **If third parties are handling sensitive information, it is important to protect the data with passwords and protocol that reduce the risk of breaches.** “This data breach is particularly egregious for both the lack of very basic protection — a password — and the extremely high degree of sensitivity of the data. There may be people on the list that are innocent, and the risky individuals are now aware they are on the list and can change their tactics to avoid detection in the future,” said Carl Wright, CCO at AttackIQ.
* **Because organizations pay for premium access to datasets, it is important to respect their patronage as a customer and protect the product or services they pay for.** In addition to not better protecting its premium customers’ data, Dow Jones did not mention any plans to compensate customers following the breach.
* **In the wake of a data breach, it is critical for organizations to respond to the incident in an efficient and appropriate manner.** Dow Jones saved itself from additional critiques by removing the data and replacing it with a message immediately after being informed of the leak.

# **Facebook**

**Disclosure Date:** March 21, 2019 by Krebs on Security

**Situation Overview:**

Facebook found that user passwords were being stored in a readable format within its internal data storage systems of as many as 600 million users. These passwords were stored in plain text and able to be accessed by more than 20,000 of the company’s employees in some cases since 2012. Facebook shared information about the incident shortly after it was released by Krebs on Security, and stated that there was no evidence that the data was used maliciously.

**Disclosure Materials:**

* Who disclosed the breach? Krebs on Security
* Media release:

[Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years](https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/) (Krebs on Security)

Hundreds of millions of Facebook users had their account passwords stored in plain text and searchable by thousands of Facebook employees — in some cases going back to 2012, KrebsOnSecurity has learned. Facebook says an ongoing investigation has so far found no indication that employees have abused access to this data.

Facebook is probing a series of security failures in which employees built applications that logged unencrypted password data for Facebook users and stored it in plain text on internal company servers. That’s according to a senior Facebook employee who is familiar with the investigation and who spoke on condition of anonymity because they were not authorized to speak to the press.

The Facebook source said the investigation so far indicates between 200 million and 600 million Facebook users may have had their account passwords stored in plain text and searchable by more than 20,000 Facebook employees. The source said Facebook is still trying to determine how many passwords were exposed and for how long, but so far the inquiry has uncovered archives with plain text user passwords dating back to 2012.

My Facebook insider said access logs showed some 2,000 engineers or developers made approximately nine million internal queries for data elements that contained plain text user passwords.

“The longer we go into this analysis the more comfortable the legal people [at Facebook] are going with the lower bounds” of affected users, the source said. “Right now they’re working on an effort to reduce that number even more by only counting things we have currently in our data warehouse.”

In an interview with KrebsOnSecurity, Facebook software engineer Scott Renfro said the company wasn’t ready to talk about specific numbers — such as the number of Facebook employees who could have accessed the data.

Renfro said the company planned to alert affected Facebook users, but that no password resets would be required.

“We’ve not found any cases so far in our investigations where someone was looking intentionally for passwords, nor have we found signs of misuse of this data,” Renfro said. “In this situation what we’ve found is these passwords were inadvertently logged but that there was no actual risk that’s come from this. We want to make sure we’re reserving those steps and only force a password change in cases where there’s definitely been signs of abuse.”

A written statement from Facebook provided to KrebsOnSecurity says the company expects to notify “hundreds of millions of Facebook Lite users, tens of millions of other Facebook users, and tens of thousands of Instagram users.” Facebook Lite is a version of Facebook designed for low speed connections and low-spec phones.

Both Github and Twitter were forced to admit similar stumbles in recent months, but in both of those cases the plain text user passwords were available to a relatively small number of people within those organizations, and for far shorter periods of time.

Renfro said the issue first came to light in January 2019 when security engineers reviewing some new code noticed passwords were being inadvertently logged in plain text.

“This prompted the team to set up a small task force to make sure we did a broad-based review of anywhere this might be happening,” Renfro said. “We have a bunch of controls in place to try to mitigate these problems, and we’re in the process of investigating long-term infrastructure changes to prevent this going forward. We’re now reviewing any logs we have to see if there has been abuse or other access to that data.”

Facebook’s password woes come amid a tough month for the social network. Last week, The New York Times reported that federal prosecutors are conducting a criminal investigation into data deals Facebook struck with some of the world’s largest tech companies.

Earlier in March, Facebook came under fire from security and privacy experts for using phone numbers provided for security reasons — like two-factor authentication — for other things (like marketing, advertising and making users searchable by their phone numbers across the social network’s different platforms).

**Update, 11:43 a.m.:** Facebook has posted a statement about this incident [here](https://newsroom.fb.com/news/2019/03/keeping-passwords-secure/).

# # #

**Media Details:**

* The coverage surrounding the Facebook data breach came from the top outlets in the United States, as well as some internationally. In addition to covering the story, most of the articles regarding the incident also criticized Facebook for its lack of security as well as its lack of transparency, considering the company waited three months to disclose the breach only after another source had reported it first. This comes just months after another data breach Facebook had suffered from in October 2018 and one week following a report that Facebook is in the midst of a criminal investigation.
* [Facebook staff had access to hundreds of millions of people's passwords (CNN)](https://www.cnn.com/2019/03/21/tech/facebook-password-database/index.html)

**Key Communications Takeaways:**

* **Report incidences to the public first to control the coverage and prevent additional backlash from the media.** Facebook made a grave error by going public with the breach after another outlet had reported the incident first, which caused other news outlets to further criticize the company. Had Facebook reported the incident earlier, the company would have been able to control which information the media received, therefore controlling its image and reputation better. While many factors may have prevented Facebook from releasing a full statement upon learning about the breach, issues can be vaguely disclosed and updated as investigations continue and information becomes available.
* **Learn from the past to avoid making similar mistakes.** No matter how many privacy or data breaches Facebook endures, the company continues to make avoidable mistakes. To avoid this, Facebook needs to take its users’ data seriously and protect it with extreme caution and the utmost care.
* **Regularly monitor data storage systems, both internal and external.** While Facebook found the breach during a routine security screen in January, there were still stored passwords from 2012, meaning past reviews were insufficient. Had this information been accessible to those outside of Facebook, the effects would have been much more damaging.

**Oregon Department of Human Services (DHS)  
  
Disclosure Date:** March 21, 2019 by DHS

**Situation Overview:**

After nine of DHS employees clicked on a phishing link in January, nearly 2 million email records were compromised. These emails may have exposed the names, addresses, dates of birth, Social Security numbers, and other information of as many as 1.6 million DHS clients.

**Disclosure Materials:**

* Who disclosed the breach? Oregon Department of Human Services (DHA)
* Media release:

[Oregon Department of Human Services Notifies Public of Data Breach](https://www.oregon.gov/DHS/DHSNEWS/NewsReleases/Data-Breech-News%20Release-2019-03-21.pdf) (DHS)

(Salem, Ore.) – The Oregon Department of Human Services uncovered a phishing incident that affected e-mail records at the department. Unfortunately, Protected Health Information under the Health Insurance Portability and Accountability Act (HIPAA) was compromised and potentially exposed.

The agency has hired an outside entity, IDExperts, to perform a forensic review to clarify the number and identities of Oregonians whose information was exposed, and the specific kinds of information involved.

The Department of Human Services takes privacy and the confidentiality of client information seriously and has strong information technology security processes in place, which enabled the department to detect and contain the incident. The department cannot confirm that any clients’ personal information was acquired from its email system or used inappropriately. However, it is notifying the public because information was accessible to an unauthorized person or persons.

Although DHS has not confirmed that clients’ personal information was acquired during the incident, DHS considers the incident a breach under Oregon’s Identity Theft Protection Act (ORS 646A.600 to 646A.628). Therefore, this notification is provided in part as a substitute notice of a breach under Oregon’s Identity Theft Protection Act, because the class of affected consumers exceeds 350,000.

The facts are summarized below, along with protective measures the department has taken since discovering the incident and general guidance on protecting personal information.

What happened?

On January 28, 2019 DHS and Enterprise Security Office Cyber Security team confirmed that a breach of regulated information had occurred. Nine individual employees opened a phishing email and clicked on a link that compromised their email mailboxes and allowed access to these employees’ email information. Current information indicates on January 8th, a spear phishing email was sent to DHS employees. Through our process of discovery, we learned that there were nearly 2 million emails in those email mailboxes.

The unauthorized access to the affected email mailboxes was successfully stopped. DHS is in the process of thoroughly reviewing the incident and the information involved. This investigation includes clarifying the number of impacted records that might contain personal information of clients receiving services from DHS.

What information was involved?

Clients’ Protected Health Information under the Health Insurance Portability and Accountability Act (HIPAA) was accessible to an unauthorized person. Client information may include first and last names, addresses, dates of birth, Social Security numbers, case number and other information used to administer DHS programs.

What is the Department of Human Services doing?

The security and confidentiality of personal information is critical to the Department of Human Services. While there is no indication that any personal information was copied from its email system or used inappropriately, the department will be offering identity theft recovery services for impacted individuals. DHS is in the process of determining whose information was affected by this breach. Once confirmed, IDExperts will send individual notices to identified individuals, including notices to clients whose HIPAA-protected information was involved, with instructions on how to register for the service, which includes free credit monitoring.

Need more information?

DHS will provide updates as more information is known.

**IDExperts has established a toll-free information line which will be available Friday (March 22, 2019) at (800) 792-1750 to assist DHS clients with more information. There is also an established website with information.** [**http://ide.myidcare.com/oregon**](http://ide.myidcare.com/oregon)

DHS Concerned DHS clients may contact all three national consumer reporting agencies, including for a copy of a current credit report, at:

Equifax, TransUnion, and Experian Website:   
AnnualCreditReport.com   
Phone 877-322-8228 (Option 1)

Mailing Address:   
Annual Credit Report Request Service   
P.O. Box 105281 Atlanta, GA 30348-5281

Credit freeze: Consumers, including potentially affected DHS clients, have the option to freeze their credit reports for free. Parents may request a freeze of the credit report of a DHS client who is a child under the age of 16. The guardian, conservator, or person holding a valid power of attorney for a DHS client may also request a credit report freeze for that DHS client. Below is each company’s freeze contact information:

Equifax, (800) 349-9960 (Automated, Option 1) or (888) 298-0045 (Live)   
TransUnion, (888) 909-8872 (Option 3)   
Experian, (888) 397-3742 (Option 1 followed by Option 2)

As always, DHS clients are encouraged to report suspected identity theft to law enforcement, including the Oregon Attorney General’s Consumer Protection Division and the Federal Trade Commission.

For information on how to report suspected identity theft and for information about protecting your identity, visit:

The Oregon Attorney General’s Consumer Protection Division, which can be found online at: <https://www.doj.state.or.us/consumer-protection/id-theft-databreaches/data-breaches/>

Federal Trade Commission consumer information on Privacy, Identity & Online Security, which can be found online at: <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>

# # #

**Media Details:**

* Coverage of the incident only lasted a week and included mostly local sources with the occasional niche source, including those with a focus in law or healthcare.
* [Oregon Department of Human Services confirms data breach (Register Guard)](https://www.registerguard.com/news/20190321/oregon-department-of-human-services-confirms-data-breach)

**Key Communications Takeaways:**

* **Inform all afflicted parties of the breach quickly and efficiently.** According to DHS’ media release, on Jan. 28, DHS and Enterprise Security Office Cyber Security team confirmed that a breach of regulated information had occurred Jan. 8. By waiting nearly two months later, clients lost precious time during which their data could have been sold or used by an unauthorized third party. While it may be impossible to answer all questions, it is important to at least inform stakeholders that a breach had occurred and whatever other information is available.
* **Proper employee education and training is essential to preventing phishing attacks.** Had the nine DHS employees been able to recognize the phishing links, the data breach would not have occurred. Phishing links are the easiest offense for hackers because the information they want is given to them by employees instead of using more complicated methods.

# **Federal Emergency Management Agency (FEMA)**

**Disclosure Date:** March 22, 2019 by FEMA

**Situation Overview:**

About 2.3 million victims of the 2017 California Wildfires and Hurricanes Harvey, Irma and Maria had personal information including names and addresses, bank account information and birth dates shared with an unidentified contractor.

FEMA stated that there were no indications that the data had been compromised and that the agency is working with the contractor to delete the unnecessary data from its networks. A memo released by FEMA said that the contractor did not alert FEMA that it had received more information than necessary. Although the contractor was not required to inform FEMA, doing so would have allowed the agency to “remedy this situation earlier and avoid additional privacy incidents.”

**Disclosure Materials:**

* Who disclosed the breach? Federal Emergency Management Agency (FEMA)
* Media release:

[FEMA Press Secretary Lizzie Litzow Statement on Major Privacy Incident](https://www.fema.gov/news-release/2019/03/22/fema-press-secretary-lizzie-litzow-statement-major-privacy-incident) (FEMA)

Release date: March 22, 2019

Release Number: HQ-19-021

WASHINGTON -- FEMA, in coordination with the Department of Homeland Security Office of the Inspector General (DHS OIG), identified an incident involving the sharing of sensitive, personally identifiable information of disaster survivors using the Transitional Sheltering Assistance program. In transferring disaster survivor information to a contractor, FEMA provided more information than was necessary.

Since discovery of this issue, FEMA has taken aggressive measures to correct this error. FEMA is no longer sharing unnecessary data with the contractor and has conducted a detailed review of the contractor’s information system. To date, FEMA has found no indicators to suggest survivor data has been compromised. FEMA has also worked with the contractor to remove the unnecessary data from the system and updated its contract to ensure compliance with Department of Homeland Security (DHS) cybersecurity and information-sharing standards. As an added measure, FEMA instructed contracted staff to complete additional DHS privacy training.

FEMA’s goal remains protecting and strengthening the integrity, effectiveness, and security of our disaster programs that help people before, during, and after disasters.

# # #

**Media Details:**

* The coverage of the FEMA data breach lasted several days with the focus of the articles shifting to the victims of the breach more as the days continued. The media first reported the FEMA data breach on March 22, 2019- the same day FEMA had released a statement informing the public of the incident. The biggest news outlets in the nation covered the story, including The New York Times and The Washington Post.
* [Personal Data of 2.3 Million Disaster Victims Was Released by FEMA, Report Says (The New York Times)](https://www.nytimes.com/2019/03/22/us/fema-data-breach.html)

**Key Communication Takeaways:**

* **Organizations, particularly governmental entities, must be especially careful while managing the data of vulnerable groups.** While enduring a personal crisis, one does not expect to experience another immediately after, especially from the group either helping or protecting them. Establishing guidelines and policies that prevent breaches is essential to properly protecting all stakeholders. The breach would have been minimized had FEMA established a rule that forces contractors to inform the agency when too much information is shared.
* **Sufficient data security protects organizations from additional crises and negative news coverage.** For example, the coverage surrounding FEMA’s response to the 2017 hurricane season after a report released in 2018 found the agency had under-prepared for the storm’s impact had dissolved by the time of the breach, yet was brought up again once the crisis surfaced, adding fuel to the fire.

# **Georgia Institute of Technology**

**Disclosure Date:** April 2, 2019 by Georgia Tech

**Situation Overview:**

Personal information of 1.3 million current and former faculty, students, staff and student applicants of Georgia Institute of Technology were accessed by an outside entity through a central database. The compromised information affected by the breach includes names, addresses, Social Security Numbers and birth dates. This is the university’s second breach in less than a year, when 8,000 students were affected when their information was accidentally emailed to the wrong recipient in 2018.

**Disclosure Materials:**

* Who disclosed the breach? Georgia Institute of Technology
* Media release:

[Unauthorized Access on Georgia Tech Network Exposes Information for 1.3 Million Individuals](https://www.news.gatech.edu/2019/04/02/unauthorized-access-georgia-tech-network-exposes-information-13-million-individuals) (Georgia Tech)

Unauthorized access to a Georgia Institute of Technology web application has exposed personal information for up to 1.3 million individuals, including some current and former faculty, students, staff and student applicants. Georgia Tech information security officials are working to determine the extent of the access and to identify the individuals who may be affected.

A central Georgia Tech database was accessed by an unknown outside entity. Georgia Tech’s cybersecurity team is conducting a thorough forensic investigation to determine precisely what information was extracted from the system, which may include names, addresses, social security numbers and birth dates.

The U.S. Department of Education and University System of Georgia have been notified, and those whose data was exposed will be contacted as soon as possible regarding available credit monitoring services.

In late March, Georgia Tech learned of the illegal access and immediately corrected the impacted application. Georgia Tech is committed to the privacy and security of its personal data and deeply regrets the potential impact on those affected.

# # #

**Media Details:**

* The coverage surrounding the Georgia Tech data breach lasted approximately one week and were mostly from Georgia news outlets, including the Atlanta Journal Constitution and various local news outlets.
* [Data breach exposes up to 1.3M Georgia Tech faculty, students (AJC)](https://www.ajc.com/news/breaking-news/breaking-data-breach-exposes-georgia-tech-faculty-students/zAUUNWy5hoHQ8bNvMxcsWL/)

**Key Communication Takeaways:**

* **Learn from mistakes.** Academic institutions have always been large targets for data breaches, and despite knowing this, they are still ill-prepared for cyberattacks. Considering Georgia Tech had a data breach less than one year ago, the university should have reviewed its cybersecurity measures and secured any potential vulnerabilities to prevent falling victim to another attack.
* **Work quickly to solve the issue.** According to Georgia Tech’s statement, the issue was discovered in late March and was immediately corrected, and is currently under investigation. Immediate action prevents further damage to those affected and to a company’s reputation.

# **Bodybuilding.com**

**Disclosure Date**: April 19, 2019 by Bodybuilding.com

**Situation Overview:**

Bodybuilding.com announced a data breach that potentially impacted its 7 million registered users. The potential stolen information includes names, email addresses, billing/shipping addresses, phone numbers, order history, birth date, and information included in public BodySpace profiles. The company, which boasts 35 million unique visitors monthly, has since forced a password reset and notified its customers of the breach via email and FAQ.

**Disclosure Materials:**

* Who disclosed the breach? Bodybuilding.com
* Media release:

[DATA INCIDENT](https://www.bodybuilding.com/help?notifications&data-incident) (Bodybuilding.com)

Bodybuilding.com recently became aware of a data security incident that may have affected certain customer information in our possession. We have no evidence that personal information was accessed or misused, but we are directly notifying all current and former users and customers out of an abundance of caution. We have included below information about the circumstances as we understand them and the steps we are undertaking to address the situation.

If you have additional questions about the incident, we encourage you to call our dedicated call center at 1-844-386-9553, 8:00 am to 10:00 pm CT Monday through Friday, and 10:00 am to 7:00 pm CT Saturday and Sunday.

We sincerely regret any inconvenience or concern caused by this incident. We are committed to protecting your information and maintaining your trust and confidence.

**FAQs**

**1. What Happened?**

We became aware of a data security incident involving unauthorized access to our systems in February 2019. We engaged one of the leading data security firms to conduct a thorough investigation, which traced the unauthorized activity to a phishing email received in July 2018. On April 12, 2019, we concluded our investigation and could not rule out that personal information may have been accessed. While we have no evidence that personal information was accessed or misused, we are notifying all current and former customers and users about the incident out of an abundance of caution to explain the circumstances as we understand them.

**2. What Actions Are You Taking In Response To This Incident?**

*Updated: April 23, 2019*

Upon discovering the incident, we took steps to understand the nature and scope of the issue, and brought in external forensic consultants that specialize in cyber-attacks. We have engaged with law enforcement and are working with leading security experts to address any vulnerabilities and remediate the incident.

We continue to monitor our systems for unauthorized access, have introduced additional security measures, and will be *prompting Bodybuilding.com customers to reset their passwords on their next log-in. If users have not updated their passwords by June 12, 2019, Bodybuilding.com will be resetting customers' passwords at that time.*

**3. Was Any Credit Card Data Affected?**

The information potentially accessed in this incident does NOT include full credit or debit card numbers, as we do not store those numbers when customers make purchases in our store. If you’ve opted to store your card in your account, we store only the last four digits of your payment card number for reference and use by you for subsequent purchases, but never the entire card number.

**4. What Data Was Involved?**

While we have no evidence that personal information was accessed or misused, information you provided to us which might have been accessed in this incident could include name, email address, billing/shipping addresses, phone number, order history, any communications with Bodybuilding.com, birthdate, and any information included in your BodySpace profile. Note that BodySpace profile information is generally already publicly visible to others, as noted in our applicable Privacy Policy and Terms of Use available here: https://www.bodybuilding.com/help?legal-and-privacy. If you have an online account with us, Bodybuilding.com user names and passwords might have been accessed.

**Importantly, the information potentially accessed in this incident does NOT include full credit or debit card numbers, as we do not store those numbers when customers make purchases in our store.** If you’ve opted to store your card in your account, we store the last four digits of your payment card number for reference and use by you for subsequent purchases, but never the entire card number.

**In addition, if you accessed www.bodybuilding.com via a third-party site like Facebook, we did not have access to your password, and it was not accessible to the unauthorized party.**

**5. Were Customer Or Online User Social Security Numbers Affected By This Incident?**

No, we do not collect Social Security Numbers from customers or online users.

**6. Has The Issue Been Resolved?**

We have worked with an outside security expert to address the vulnerabilities and remediate the incident. We appreciate your business and look forward to continuing to serve your needs.

**7. What Is Bodybuilding.Com Doing To Protect My Information?**

Once we became aware of the incident, we quickly took steps to determine the nature and scope of the issue. We are working with a leading data security firm to assist in our investigation. We have also notified and are coordinating with law enforcement authorities.

* We Are Taking Steps To Protect Our Community, Including The Following:
* We are notifying Bodybuilding.com users to provide information on how they can protect their data.
* We will be requiring Bodybuilding.com users to change their passwords and urge users to do so immediately. Instructions about how to change your password are below.
* We continue to monitor for suspicious activity and to coordinate with law enforcement activities.
* We continue to make enhancements to our systems to detect and prevent unauthorized access to user information.

**8. I Think I Received An Email About This Issue. How Do I Know It Is Really From Bodybuilding.Com?**

Emails were sent to all current and former users and customers regarding this issue. Please note that the email from Bodybuilding.com does not ask you to click on any links or contain attachments and does not request your personal data. If the email you received about this issue prompts you to click on a link, suggests you download an attachment, or asks you for information, the email was not sent by Bodybuilding.com and may be an attempt to steal your personal data. Avoid clicking on links or downloading attachments from such suspicious emails. Any link included in our email to users directs users to insert the Bodybuilding.com FAQs URL into your browser and does not request your personal data.

Emails from Bodybuilding.com will never request your personal information and will always come from the domain @bodybuilding.com.

**9. What Should I Do To Protect My Information?**

We take our obligation to safeguard your personal data very seriously and are alerting you about this issue so you can take steps to help protect your information. We recommend you:

* Change your password for any other account on which you used the same or similar information used for your Bodybuilding.com account.
* Review your accounts for suspicious activity.
* Be cautious of any unsolicited communications that ask for your personal data or refer you to a web page asking for personal data.
* Avoid clicking on links or downloading attachments from suspicious emails.

**10. How Do I Change My Password?**

You can change your password via the following methods:

* If you are currently logged in, you can change the password for your account on the Change Password Page in BodySpace settings (https://www.bodybuilding.com/profile/change-password).
* If you’ve forgotten or misplaced your password, please go to the Reset Password Page and follow the prompts (https://www.bodybuilding.com/profile/forgot-password).

These instructions can always be found on our “Account Inquiries” Help Page in our Help Center at www.bodybuilding.com/help

**11. Where Can I Get More Information?**

We have established a dedicated call center to answer any questions you may have. You can reach the call center at 1-844-386-9553 between 8:00 AM – 10:00 PM CT, Monday through Friday, or 10:00 AM – 7:00 PM CT, Saturday and Sunday,

We sincerely regret any inconvenience or concern caused by this incident. We are committed to protecting your information and maintaining your trust and confidence.

# # #

**Media Details:**

* The coverage surrounding the Bodybuilding.com data breach lasted approximately a week and were mainly articles from niche tech outlets; however, Forbes wrote an article about the breach’s cause- employees- five days after the breach was announced. The breach is still referenced in articles to emphasize the importance of proper cyber awareness training for all employees.
* [Bodybuilding.com Breach: Proof That An Organization's Biggest Cyber Risk Is Its People (Forbes)](https://www.forbes.com/sites/jameshadley/2019/04/24/bodybuilding-com-breach-proof-that-an-organizations-biggest-cyber-risk-is-its-people/#2e82d7ab1bef)

**Key Communications Takeaways:**

* **Address the public’s questions and concerns as efficiently as possible.** Bodybuilding.com released a comprehensive FAQ as part of its official statement on the breach, which saved the company from scrutiny from the press and its users. While it took the company months to disclose the breach, they were the first to do so and had enough data collected to answer any questions users may have.
* **Proper cyber security training for all employees should be an operation standard.** While 87 percent of executives view untrained staff as their greatest cyber risk, cybersecurity training is not treated as a priority. Organizations are only as secure as their least tech-savvy employee, which means regular company-wide training must be implemented to prevent breaches. Training should be engaging so employees can practice avoiding phishing attacks before they arrive and to help them retain information from the training better.

# **WhatsApp**

**Disclosure Date:** May 13, 2019 by Facebook

**Situation Overview:**

WhatsApp, a Facebook subsidiary messaging app, experienced a security flaw that left people vulnerable to spyware designed by the NSO Group, an Israeli government surveillance agency, who denied the claims. Those affected would have been able to be spied on through their phone’s microphone and camera, WhatsApp messages and connected apps. The interesting part of the bug is that it required no user participation- the spyware begins revealing the phone’s encrypted content shortly after users missed the call.

**Disclosure Materials:**

* Who disclosed the breach? Facebook
* Media release:

[CVE-2019-3568](https://www.facebook.com/security/advisories/cve-2019-3568) (Facebook)

Description: A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of SRTCP packets sent to a target phone number.

Affected Versions: The issue affects WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen prior to v2.18.15.

Last Updated: 2019-05-13

# # #

**Media Details:**

* Because of the app’s popularity for global messaging, the WhatsApp data breach received coverage from various international outlets, including those located in the UK, Luxembourg, India and more. In addition, The New York Times, CNN, Reuters and CNBC covered the breach, as well as a recommendation and tutorial from TIME to update the app.
* [WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer’s Phone (The New York Times)](https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html)

**Key Communication Takeaways:**

* **Patch vulnerabilities as quickly as possible to isolate problem and to prevent them from spreading and creating more issues.** WhatsApp engineers were quick to jump on the breach and begin working on a patch to rectify the issue. After, they encouraged users to update their apps as quickly as possible to protect them against targeted exploits designed to compromise information stored on cell phones. By doing so, WhatsApp prevented more data to be taken from its users.
* **Make sure your company has the resources necessary to combat and respond to cybersecurity breaches.** Because WhatsApp is a subsidiary of Facebook, its resources, including engineers, investigators and communicators, are much greater than those of other companies. Using these resources to a company’s advantage reduces bad media coverage or effects on reputation.

# **Instagram**

**Disclosure Date:** May 20, 2019 by TechCrunch

**Situation Overview:**

More than 49 million Instagram influencers, celebrities, and brands had their private contact information exposed after an India-based social media marketing company left the data unprotected on an Amazon Web Services (AWS) database for at least 72 hours. Users’ bio, profile photo, location, verification status, email address and phone number of high-profile accounts were exposed during the breach. This is Instagram’s second leak of 2019, the first being in April, when 540 million Instagram account records were exposed by a different third party using AWS.

**Disclosure Materials:**

* Who disclosed the breach? TechCrunch
* Media release:

[Millions of Instagram influencers had their contact data scraped and exposed](https://techcrunch.com/2019/05/20/instagram-influencer-celebrity-accounts-scraped/) (TechCrunch)

A massive database containing contact information of millions of Instagram influencers, celebrities and brand accounts has been found online.

The database, hosted by Amazon Web Services, was left exposed and without a password allowing anyone to look inside. At the time of writing, the database had over 49 million records — but was growing by the hour.

From a brief review of the data, each record contained public data scraped from influencer Instagram accounts, including their bio, profile picture, the number of followers they have, if they’re verified and their location by city and country, but also contained their personal contact information, such as the Instagram account owner’s email address and phone number.

Security researcher Anurag Sen discovered the database and alerted TechCrunch in an effort to find the owner and get the database secured. We traced the database back to Mumbai-based social media marketing firm Chtrbox, which pays influencers to post sponsored content on their accounts. The records contained data that calculated the worth of each account, based off the number of followers, engagement, reach, likes and shares they had. This was used as a metric to determine how much the company could pay an Instagram celebrity or influencer to post an ad.

TechCrunch found several high-profile influencers in the exposed database, including prominent food bloggers, celebrities and other social media influencers.

We contacted several people at random whose information was found in the database and provided them their phone numbers. Two of the people responded and confirmed their email address and phone number found in the database was used to set up their Instagram accounts. Neither had any involvement with Chtrbox, they said.

Shortly after we reached out, Chtrbox pulled the database offline. Pranay Swarup, the company’s founder and chief executive, did not respond to a request for comment and several questions, including how the company obtained personal Instagram account email addresses and phone numbers. Later in a tweet, Chtrbox disputed the number of people affected and claimed no more than 350,000 influencers were affected. Chtrbox also said database was only open for 72 hours, but the researcher confirmed the database was first detected on Shodan, a search engine for exposed databases and devices, on May 14.

The scraping effort comes two years after Instagram admitted a security bug in its developer API allowed hackers to obtain the email addresses and phone numbers of six million Instagram accounts. The hackers later sold the data for bitcoin.

Months later, Instagram — now with more than a billion users — choked its API to limit the number of requests apps and developers can make on the platform.

Facebook, which owns Instagram, later said it disputed the report.

“We take any allegation of data misuse seriously. Following an initial investigation into the claims made in this story, we found that no private emails or phone numbers of Instagram users were accessed,” said an Instagram spokesperson. “Chtrbox’s database had publicly available information from many sources, one of which was Instagram. Chtrbox also clarified that the database contained information for 350,000 people, not 49 million as has been reported,”

“We’re looking into the issue to understand if the data described – including email and phone numbers – was from Instagram or from other sources,” said an updated statement. “We’re also inquiring with Chtrbox to understand where this data came from and how it became publicly available,” it added.

# # #

**Media Details:**

* The coverage surrounding the Instagram data breach spanned approximately a week and included stories from outlets all over the globe. Nationally, sources like PRWeek, TechCrunch, Business Insider, and various niche tech media outlets covered the breach. Many of the stories posted had edits posted at the bottom correcting some of the articles contents. The most common correction was the fact that some of the emails and phone numbers compromised in the breach were publicly posted on users’ profiles for business purposes.
* [Tech PR pros question ‘Facebook’s trust issues’ after Instagram data security breach (PRWeek)](https://www.prweek.com/article/1585581/tech-pr-pros-question-facebooks-trust-issues-instagram-data-security-breach)

**Key Communication Takeaways:**

* **Always verify your third-party partners are following the correct policies and procedures when dealing with your company’s data.** Facebook and its subsidiaries have made this mistake repeatedly, and in this case, just one month following another breach related to third parties using Amazon Web Service, and one week after WhatsApp’s data breach.
* **When planning to launch a new product or service, it is wise to ensure data privacy measures are secure to prevent bad media coverage before major announcements and releases.** Instagram’s breach poses an issue for Facebook, who had just announced its plan to create its own cryptocurrency. “If consumers aren’t able to trust the social media giant with their email addresses, how can they trust them with their money?” said Hayley Coleby, senior social media director at The PHA Group. “Facebook needs to make a serious U-turn with their policies or they risk losing more investments and users."

# **First American Financial Corp.**

**Disclosure Date:** May 24, 2019 by Krebs on Security

**Situation Overview:**

A massive data leak containing 885 million personal and financial records was found unprotected on the website of First American Financial Corp, a leading title insurer for the U.S. real estate market and Fortune 500 company. The breach exposed consumers’ Social Security numbers, bank account numbers, mortgage and tax records, wire transaction receipts, and driver’s license images from as far back as 2003. The data was unprotected and accessible to anyone who had the URL for over two years.

First American’s spokesperson issued a statement on the issue sometime between May 24 through 29, which is when the site that served the records had been disabled.

**Disclosure Materials:**

* Who disclosed the breach? Krebs on Security
* Media release:

[First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records](https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/) (Krebs on Security)

The Web site for Fortune 500 real estate title insurance giant First American Financial Corp. [NYSE:FAF] leaked hundreds of millions of documents related to mortgage deals going back to 2003, until notified this week by KrebsOnSecurity. The digitized records — including bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers license images — were available without authentication to anyone with a Web browser.

Santa Ana, Calif.-based First American is a leading provider of title insurance and settlement services to the real estate and mortgage industries. It employs some 18,000 people and brought in more than $5.7 billion in 2018.

Earlier this week, KrebsOnSecurity was contacted by a real estate developer in Washington state who said he’d had little luck getting a response from the company about what he found, which was that a portion of its Web site (firstam.com) was leaking tens if not hundreds of millions of records. He said anyone who knew the URL for a valid document at the Web site could view other documents just by modifying a single digit in the link.

And this would potentially include anyone who’s ever been sent a document link via email by First American.

KrebsOnSecurity confirmed the real estate developer’s findings, which indicate that First American’s Web site exposed approximately 885 million files, the earliest dating back more than 16 years. No authentication was required to read the documents.

Many of the exposed files are records of wire transactions with bank account numbers and other information from home or property buyers and sellers. Ben Shoval, the developer who notified KrebsOnSecurity about the data exposure, said that’s because First American is one of the most widely-used companies for real estate title insurance and for closing real estate deals — where both parties to the sale meet in a room and sign stacks of legal documents.

“Closing agencies are supposed to be the only neutral party that doesn’t represent someone else’s interest, and you’re required to have title insurance if you have any kind of mortgage,” Shoval said.

“The title insurance agency collects all kinds of documents from both the buyer and seller, including Social Security numbers, drivers licenses, account statements, and even internal corporate documents if you’re a small business. You give them all kinds of private information and you expect that to stay private.”

Shoval shared a document link he’d been given by First American from a recent transaction, which referenced a record number that was nine digits long and dated April 2019. Modifying the document number in his link by numbers in either direction yielded other peoples’ records before or after the same date and time, indicating the document numbers may have been issued sequentially.

The earliest document number available on the site – 000000075 — referenced a real estate transaction from 2003. From there, the dates on the documents get closer to real time with each forward increment in the record number.

As of the morning of May 24, firstam.com was returning documents up to the present day (885,000,000+), including many PDFs and post-dated forms for upcoming real estate closings. By 2 p.m. ET Friday, the company had disabled the site that served the records. It’s not yet clear how long the site remained in its promiscuous state, but archive.org shows documents available from the site dating back to at least March 2017.

First American wouldn’t comment on the overall number of records potentially exposed via their site, or how long those records were publicly available. But a spokesperson for the company did share the following statement:

“First American has learned of a design defect in an application that made possible unauthorized access to customer data. At First American, security, privacy and confidentiality are of the highest priority and we are committed to protecting our customers’ information. The company took immediate action to address the situation and shut down external access to the application. We are currently evaluating what effect, if any, this had on the security of customer information. We will have no further comment until our internal review is completed.”

I should emphasize that these documents were merely available from First American’s Web site; I do not have any information on whether this fact was known to fraudsters previously, nor do I have any information to suggest the documents were somehow mass-harvested (although a low-and-slow or distributed indexing of this data would not have been difficult for even a novice attacker).

Nevertheless, the information exposed by First American would be a virtual gold mine for phishers and scammers involved in so-called Business Email Compromise (BEC) scams, which often impersonate real estate agents, closing agencies, title and escrow firms in a bid to trick property buyers into wiring funds to fraudsters. According to the FBI, BEC scams are the most costly form of cybercrime today.

Armed with a single link to a First American document, BEC scammers would have an endless supply of very convincing phishing templates to use. A database like this also would give fraudsters a constant feed of new information about upcoming real estate financial transactions — including the email addresses, names and phone numbers of the closing agents and buyers.

As noted in past stories here, these types of data exposures are some of the most common yet preventable. In December 2018, the parent company of Kay Jewelers and Jared Jewelers fixed a weakness in their site that exposed the order information for all of their online customers.

In August 2018, financial industry giant Fiserv Inc. fixed a bug reported by KrebsOnSecurity that exposed personal and financial details of countless customers across hundreds of bank Web sites.

In July 2018, identity theft protection service LifeLock corrected an information disclosure flaw that exposed the email address of millions of subscribers. And in April 2018, PaneraBread.com remedied a weakness exposing millions of customer names, email and physical addresses, birthdays and partial credit card numbers.

# # #

**Media Details:**

* The coverage surrounding the First American Financial Corp was mostly done by niche tech, insurance and real estate outlets, as well as an article from The New York Times, The Los Angeles Times and Bloomberg. Coverage lasted approximately one week and covered the lawsuit that ensued shortly after the incident came to light. Some articles used the breach as an example of what not to do, and included tips on how not to make the same mistake.
* [Title Insurer First American Says App Defect May Have Exposed Customer Data (Insurance Journal)](https://www.insurancejournal.com/news/national/2019/05/28/527554.htm)

**Key Communications Takeaways:**

* **Defense against cyberattacks is a company’s best offensive strategy.** Cyberattacks are like earthquakes: unpredictable. Despite this, buildings have been designed to be more resilient if one occurs. Cybersecurity defenses should work the same way- to prevent the unexpected rather than attempt to recover after it occurs. Having a proactive approach to cybersecurity rather than a reactive approach prevents issues before they have the opportunity to begin.
* **Flexibility and adaptability are the two most important features while preparing against cyberattacks.** Evidence-based approaches that are drawn from IT intelligence offer the best methods for preparation because they are based on real-world activities in the cyber zone.

# 

**Checkers**

**Disclosure Date:** May 29, 2019 by Checkers

**Situation Overview:**

More than 100 Checkers and Rally’s restaurants in 20 states found malware in its point-of-sale systems. The restaurant discovered the attack in April 2019, but found that 15 percent of its location’s systems had been compromised since at least October 2016. The compromised information siphoned customers’ full credit card information, including cardholder names, payment card numbers, card expiration dates and card verification codes.

**Disclosure Materials:**

* Who disclosed the breach? Checkers
* Media release:

[NOTICE OF DATA BREACH (Checkers)](https://www.checkers.com/security-issue/)

To Our Valued Checkers and Rally’s Guests:

We recently became aware of a data security issue involving malware at certain Checkers and Rally’s locations. After discovering the issue, we quickly engaged leading data security experts to conduct an extensive investigation and coordinated with affected restaurants and federal law enforcement authorities to address the matter. We have worked closely with the third-party security experts to contain and remove the malware.

Our guests are our top priority, and we take the protection of their information very seriously. Below is additional information about what happened and what we are doing to further protect our guests’ data.

**What Happened?**

After becoming aware of a potential issue, we retained data security experts to understand its nature and scope. Based on the investigation, we determined that malware was installed on certain point-of-sale systems at some Checkers and Rally’s locations, which appears to have enabled an unauthorized party to obtain the payment card data of some guests.

It is important to understand that not all Checkers and Rally’s restaurants were affected by this issue. A list of the impacted locations and their respective estimated dates of exposure is available here. In addition, not all guests who visited the listed restaurants during the relevant time periods are affected by this issue.

**What Information Was Involved?**

The malware was designed to collect information stored on the magnetic stripe of payment cards, including cardholder name, payment card number, card verification code and expiration date. Based on the investigation, we have no evidence that other cardholder personal information was affected by this issue.

**What We Are Doing?**

As indicated above, after identifying the incident, we promptly launched an extensive investigation and took steps to contain the issue. We also are working with federal law enforcement authorities and coordinating with the payment card companies in their efforts to protect cardholders. We continue to take steps to enhance the security of Checkers and Rally’s systems and prevent this type of issue from happening again.

**What You Can Do**

If you used a payment card at an affected restaurant during a relevant time period, please consider the following recommendations:

* Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately.
* Order a Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.
* Review the Reference Guide and FAQs. The Reference Guide and FAQs provide additional recommendations on the protection of personal information.

**For More Information**

If you have any questions about this issue, please call 1-844-386-9554, Monday through Friday from 8:00 a.m. to 10:00 p.m. CST and Saturday and Sunday from 10:00 a.m. to 7:00 p.m. CST.

We hope this information is useful to you, and we sincerely regret any inconvenience or concern this may cause our guests.

Sincerely,

Adam Noyes  
Checkers Drive-In Restaurants, Inc.  
Chief Administrative Officer & Executive Vice President

# # #

**Media Details:**

* The coverage surrounding the Checkers & Rally’s data breach came from mostly smaller news outlets with a Checkers in its local area or cybersecurity blogs. Coverage only lasted a few days.
* [Checkers & Rallys locations in 20 states had a data breach (Tampa Bay Times)](https://www.tampabay.com/business/checkers-amp-rallys-locations-in-20-states-had-a-data-breach-20190529/)

**Key Communications Takeaways:**

* **Give consumers as many answers as possible.** After the breach was discovered, Checkers was quick to investigate. In addition to posting a media release, Checkers also included an FAQ, an extensive reference guide regarding which chains were affected by the breach and instructions on which steps to take if someone had used their card at one of the chains during the relevant time. Suggestions included placing security freeze on credit files, reporting incidents and getting a free credit report.
* **Continue to update the public when updates become available.** While Checkers had a great response to the breach and informed the afflicted parties well, there was a lack of updates from the company. While it is possible no additional details appeared, it is still advisable to disclose the lack of new information to confirm the breach is officially closed.

# **Quest Diagnostics**

**Disclosure Date:** June 3, 2019 by Quest Diagnostics

**Situation Overview:**

Quest Diagnostics’ billing collections vendor, American Medical Certification Association (AMCA), reported that close to 12 million patients’ financial account data, Social Security numbers, and health information were likely stolen in a breach that ranged from August 1, 2018 to March 30, 2019.

**Disclosure Materials:**

* Who disclosed the breach? Quest Diagnostics
* Media release:

[FORM 8-K](https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm) (Quest Diagnostics)

On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest Diagnostics Incorporated (“Quest Diagnostics”) and Optum360 LLC, Quest Diagnostics’ revenue cycle management provider, of potential unauthorized activity on AMCA’s web payment page. Quest Diagnostics and Optum360 promptly sought information from AMCA about the incident, including what, if any, information was subject to unauthorized access.

Although Quest Diagnostics and Optum360 have not yet received detailed or complete information from AMCA about the incident, AMCA has informed Quest Diagnostics and Optum360 that:

* between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA’s system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself;
* the information on AMCA’s affected system included financial information (e.g., credit card numbers and bank account information), medical information and other personal information (e.g., Social Security Numbers);
* as of May 31, 2019, AMCA believes that the number of Quest Diagnostics patients whose information was contained on AMCA’s affected system was approximately 11.9 million people; and
* AMCA has been in contact with law enforcement regarding the incident.

Quest Diagnostics has not been able to verify the accuracy of the information received from AMCA.

Quest Diagnostics’ laboratory test results were not provided to AMCA and were therefore not impacted by this incident.

In response to this incident, Quest Diagnostics has:

* suspended sending collection requests to AMCA;
* provided notifications to affected health plans and will ensure that notification is provided to regulators and others as required by federal and state law; and
* been working and will continue to work diligently, along with Optum360, AMCA and outside security experts, to investigate the AMCA data security incident and its potential impact on Quest Diagnostics and its patients.

Quest Diagnostics has insurance coverage in place for certain potential liabilities and costs relating to the incident; this insurance is limited in amount and subject to a deductible.

Quest Diagnostics takes this matter very seriously and is committed to the privacy and security of patients’ personal, medical and financial information.

The statements in this Current Report on Form 8-K which are not historical facts, including statements regarding the incident described in this Current Report on Form 8-K, may be forward-looking statements. Readers are cautioned not to place undue reliance on forward-looking statements, which speak only as of the date that they are made and which reflect management’s current knowledge, understanding or beliefs and which involve risks and uncertainties that could cause actual results and outcomes to be materially different. Risks and uncertainties that may affect the future results of Quest Diagnostics include, but are not limited to, the ultimate scope and extent of the incident and patient information compromised, the outcome of any potential regulatory inquiries and/or litigation arising out of or in connection with the incident, the potential damage to Quest Diagnostics reputation from this incident, the outcome of the investigation of the incident, remediation costs and other additional operating or other expenses that may be incurred by Quest Diagnostics as the result of this incident, the impact of the incident on Quest Diagnostics’ revenues, and other factors discussed in Quest Diagnostics’ most recently filed Annual Report on Form 10-K and in any of Quest Diagnostics’ subsequently filed Quarterly Reports on Form 10-Q and Current Reports on Form 8-K, including those discussed in the “Business,” “Risk Factors,” “Cautionary Factors that May Affect Future Results” and “Management’s Discussion and Analysis of Financial Condition and Results of Operations” sections of those reports.

# # #

**Media Details:**

* Because of the sensitivity of the information, many larger news outlets covered the story, including Forbes, New York Post, Fortune, The Washington Post, and more. Coverage lasted longer than anticipated because Lab Corp disclosed a breach in their data the following day. In addition, Quest Diagnostics faced a class action lawsuit over the breach, which extended the timeframe in which the company was covered by the news.
* [Quest Diagnostics Warns Up to 12 Million Patient Records Might Have Been Breached (Fortune)](https://www.tampabay.com/business/checkers-amp-rallys-locations-in-20-states-had-a-data-breach-20190529/)

**Key Communications Takeaways:**

* **Work quickly to ensure the protection and privacy of your publics.** Although the breach had been active for approximately eight months, Quest Diagnostics made sure to investigate the issue as well as cease sending collection requests to AMCA. Quest Diagnostics also followed all government regulations and laws by notifying affected parties and regulators.
* **As a healthcare company, it is especially important to be aggressive with cybersecurity defenses.** “Healthcare companies are especially susceptible to data breaches not only because they aggregate a tremendous amount of important and sensitive data, but also because they tend to be less focused on cyber security protection than other industries," Morgan & Morgan attorney John Yanchunis said in a Forbes article.

# **LabCorp**

**Disclosure Date:** June 4, 2019 by LabCorp

**Situation Overview:**

LabCorp disclosed that 7.7 million of its customers were also impacted by the same hack that had affected Quest Diagnostics just one day after its announcement. The records kept on LabCorp customers were less sensitive, however, only exposing names, addresses, dates of birth, and balance information.

* Who disclosed the breach? LabCorp
* Media release:

[FORM 8-K](https://www.sec.gov/Archives/edgar/data/920148/000119312519165091/d757830d8k.htm) (LabCorp)

In response to questions it has received, LabCorp® (NYSE: LH) announced that it has been notified by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency (AMCA) about unauthorized activity on AMCA’s web payment page (the AMCA Incident). According to AMCA, this activity occurred between August 1, 2018, and March 30, 2019. AMCA is an external collection agency used by LabCorp and other healthcare companies. LabCorp has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system. AMCA’s affected system included information provided by LabCorp. That information could include first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA’s affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance). LabCorp provided no ordered test, laboratory results, or diagnostic information to AMCA. AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp consumers.

AMCA has informed LabCorp that it is in the process of sending notices to approximately 200,000 LabCorp consumers whose credit card or bank account information may have been accessed. AMCA has not yet provided LabCorp a list of the affected LabCorp consumers or more specific information about them.

AMCA has indicated that it is continuing to investigate this incident and has taken steps to increase the security of its systems, processes, and data. LabCorp takes data security very seriously, including the security of data handled by vendors. AMCA has informed LabCorp that it intends to provide the approximately 200,000 affected LabCorp consumers with more specific information about the AMCA Incident, in addition to offering them identity protection and credit monitoring services for 24 months. LabCorp is working closely with AMCA to obtain more information and to take additional steps as may be appropriate once more is known about the AMCA Incident.

In response to initial notification of the AMCA Incident, LabCorp ceased sending new collection requests to AMCA and stopped AMCA from continuing to work on any pending collection requests involving LabCorp consumers.

# # #

**Media Details:**

* Coverage surrounding the LabCorp data breach was heavy, mainly because Quest Diagnostics had just announced its breach one day earlier than LabCorp. Coverage came from some of the biggest news outlets in the nation, including The Washington Post, USA TODAY, CMM, and The Wall Street Journal. Coverage for LabCorp (and Quest Diagnostics) continues as they are referenced in newer articles relating to cybersecurity in the ever-vulnerable healthcare industry.
* [LabCorp Patient Data Affected in Breach of Collection Firm’s Systems (The Wall Street Journal)](https://www.wsj.com/articles/labcorp-patient-data-affected-in-breach-of-collection-firms-systems-11559693005)

**Key Communications Takeaways:**

* **Continue investigations to ensure customers’ data is safe from malicious actors.** Following the data breach, LabCorp monitored the dark web for signs of its customers’ personal data. Luckily for LabCorp, the data held in AMCA’s database was not nearly as sensitive as Quest Diagnostics, so even if the data had been used, the consequences would not have been as critical.
* **Conduct research on the businesses you decide to partner with before signing any agreements.** Both Quest Diagnostics and LabCorp are partnered with AMCA, which also does business under the name Retrieval-Masters Creditors Bureau. According to Krebs, this company received an “F” rating from the Better Business Bureau, with 60 complaints closed against in recent years.