# A Special Report on Data Breach Penalties

## Written by InfoWatch Analytics Center

**InfoWatch Analytics Center**
https://www.infowatch.com/analytics

# Table of Contents

## Summary

InfoWatch Analytics Center analyzed penalties for violations that caused leaks of personal information and payment details from both government organizations and businesses on a global scale. The research covered cases when breached enterprises were either penalized by information security, financial regulation, and/or other authorities, or subject to decisions by federal or local prosecutor's offices.

The researchers became interested in this matter, as the society, businesses, and government are now more and more concerned about confidential data protection in the face of the increasing legal liability for data protection violations in many countries. The authors believe that this research, while not being comprehensive, gives an insight into the toughening of financial sanctions against companies that allowed cybersecurity violations to happen.

# Research Findings

## Total penalties for personal and payment data leaks went up seven-fold

In 2018, the number of recorded penalties for leaks of personal data and payment details increased by 46.2% YoY, with their total amount growing more than seven-fold to exceed $320 million (Figure 1).

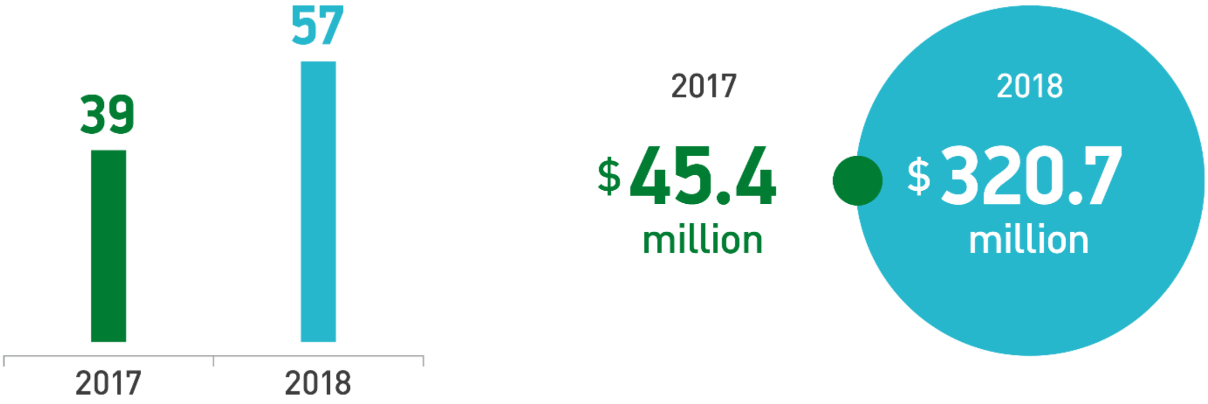


*Figure 1. The number and the total amount of data breach penalties, 2017-2018*

The year 2018 saw almost a five-fold increase in the average penalty amount up to $5.72 million.

## Major penalties of 2018

- ✓ Uber has to pay $148 million for the leak that happened back in 2016 and compromised personal data of more than 57 million customers and drivers. Uber failed to disclose this leak for over a year and preferred to pay the hackers instead of notifying regulators. In September 2018, the settlement was reached that spans all 50 US states and the District of Columbia and is the biggest data-breach payout in history. Moreover, the company was also fined by Dutch and UK authorities and now has to pay €600,000 ($685,000) and £385,000 ($490,000), respectively, for the same incident.
- ✓ As a result of the settlement reached in a court of San Jose, California, in October 2018, Yahoo agreed to pay $50 million in damages to 200 million people in the US and Israel whose email addresses and other personal information were stolen as part of the biggest security breach in history that happened in 2013-2014 and hit a total of over three billion accounts. Oath, the Verizon subsidiary that now oversees Yahoo, will pay for one half of the settlement cost, with the other half paid by Altaba Inc., a company that was set up to hold Yahoo's investments in Asian companies and other assets after the sale. In April, Altaba already paid a $35 million fine imposed by the US Securities and Exchange Commission for Yahoo's delay in disclosing the breach to investors.

- ✓ The UK Financial Conduct Authority (FCA) fined Tesco Personal Finance plc (Tesco Bank) £16.4M ($20.9M) for failing to exercise due skill, care, and diligence in protecting its personal current account holders against a cyber attack that took place in November 2016 and netted the attackers £2.26M.
- ✓ Aetna, a health insurance company, agreed to pay $17 million to settle a federal class-action lawsuit after it mailed out large-windowed envelopes that, even when unopened, showed patients' prescriptions and even their HIV status. Overall, the lawsuit's 13,000+ plaintiffs spanned 27 US states and Washington, DC.
- ✓ Anthem, Inc., a US health insurance plan provider, is to pay $16 million to the US Department of Health and Human Services and Office for Civil Rights (OCR) after the incident that hit the company in 2015 and exposed health information of almost 79 million people, including names, social security numbers, addresses, and dates of birth. Moreover, Anthem is to make huge payouts in several class-action lawsuits.
- ✓ Italy's Competition Authority slapped the largest social network Facebook with two fines that total 10 million euros ($11.4M). The first fine was issued for the social network persuading people to register for accounts on the platform without informing them during the signup process that their data would be collected and used for commercial purposes, while the second fine relates to passing user data onto third parties. Thus, Facebook is still picking up the pieces of the data breach after political consulting firm Cambridge Analytica gained unauthorized access to up to 87 million users' data. As previously reported, the Facebook data of over 200,000 users in Italy may have been shared with Cambridge Analytica as well.
- ✓ University of Texas MD Anderson Cancer Center must pay $4.3 million in a civil penalty to the federal Office of Civil Rights for violations of the Health Insurance Portability and Accountability Act. The case stems from three incidents in 2012 and 2013 when an employee's laptop was stolen at a residence, and two unencrypted drives went missing, which led to the possible compromise of health records of 35,000 people. The administrative law judge of the US Department of Health and Human Services found MD Anderson's slow implementation of security measures "shocking."

## US and UK together account for 50% of imposed penalties

The year 2018 saw a slight increase in the number of countries where regulators fined companies for data breaches. Almost half of all fines were issued in the US and the UK (Figure 2).

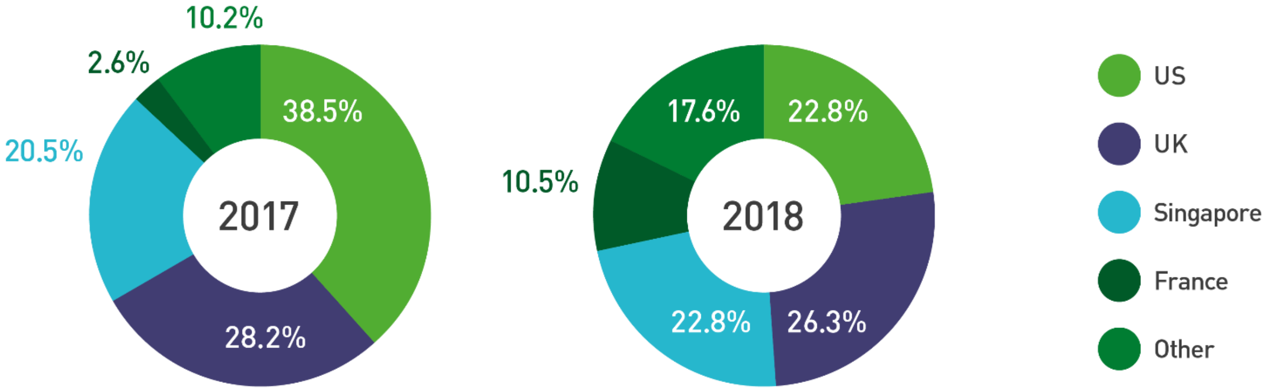


*Figure 2. Penalties by country, 2017-2018*

In 2018, French authorities became much stricter, with a total of six fines imposed (vs. only one in 2017). Among Asian countries, Singapore has an established practice of penalizing for data breaches.

Q4 2018 brought the first penalties for violations of the EU General Data Protection Regulation (GDPR). Thus, Portugal's data protection supervisory authority levied fines totaling 400,000 euros ($458,000) against hospital Centro Hospitalar Barreiro Montijo for major violations of the GDPR regarding indiscriminate access to patients' clinical information and poor service security. The Austrian Data Protection Authority fined a company €4,800 ($5,500) for an improperly set up CCTV camera, while Germany's first fine under the GDPR in the amount of €20,000 (close to $23,000) was imposed on Knuddels GmbH & Co. KG, operator of the chat community Knuddels.de, for losing 1.8 million user data records (including a file with unencrypted user passwords) as the result of a cyberattack.

Russian media did not report any penalties imposed on businesses in the period under review, as Russian regulators usually just issue warnings in such cases. In November 2018, the Russian Ministry of Digital Development, Communications, and Mass Media initiated a bill to amend the Administrative Offences Code in such a way as to oblige legal entities in breach of personal data protection to pay a penalty of 10,000 to 30,000 rubles ($154 to $462 accordingly). Naturally, such fines can hardly scare black market players that actively deal in stolen personal data.

## 25% of penalties were imposed on hi-tech companies, with the largest average amounts paid in the US

In 2018, penalty breakdown by industry changed a lot, with the dropping shares of government organizations (including municipal ones) and healthcare institutions and more and more banks and hi-tech businesses being penalized (Figure 3).

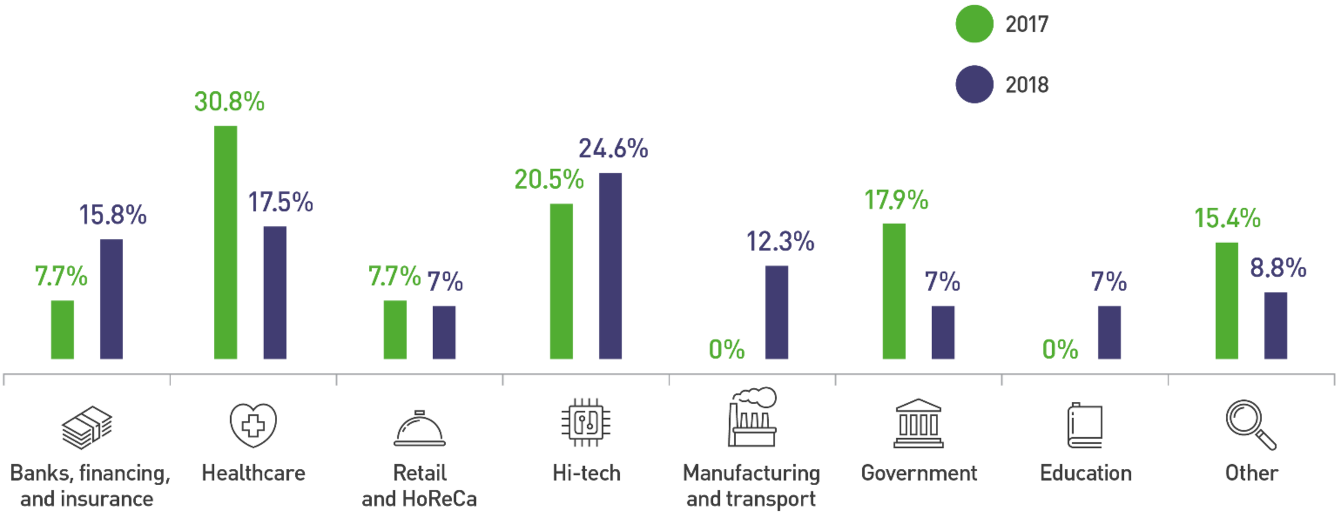


*Figure 3. Penalties by industry, 2017-2018*

Unlike in 2017, the ‘Industry Map’ now includes educational institutions, as well as the manufacturing and transportation sectors where quite a few penalties were imposed.

As noted earlier, the year 2018 saw a five-fold increase in the average fine amount. Here are figures of some countries. The US reached 8.3 times higher average fine amount, or $23.3M (Figure 4), with monetary penalties, in general, going up by 4.3 times, even without a mega fine imposed on Uber.

The UK accounted for more than a 14x increase in such average payout from $0.12M to $1.69M, while, without a large penalty imposed on Tesco Bank, this growth was 2.6x only. Singapore regulatory bodies are in no hurry to tighten their sanctions, with businesses being typically charged as little as $10,000 (1/3 increase YoY), while other countries, if taken together, doubled the average penalty amount to exceed $1M.

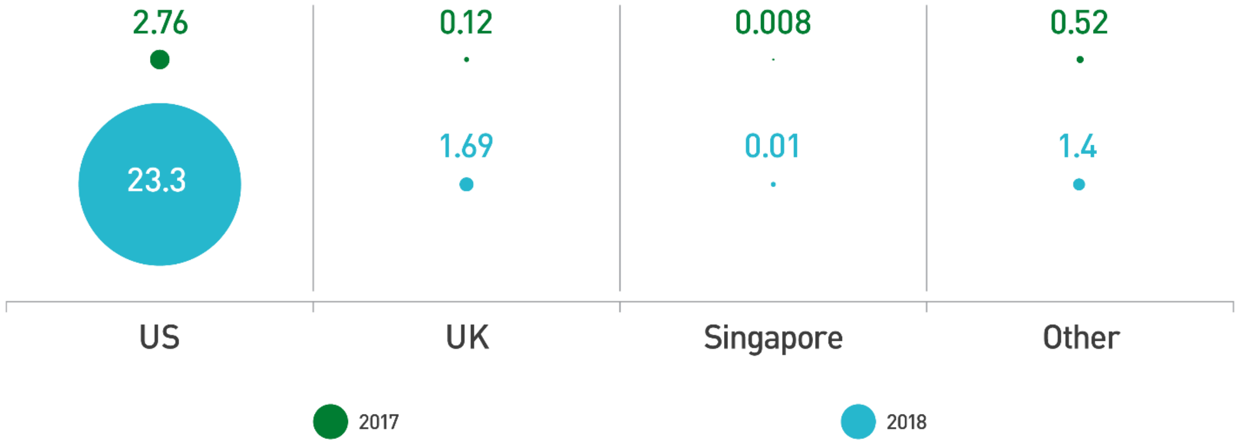


*Figure 4. Average penalty in several countries, million US dollars, 2017-2018*

# Conclusion

The researchers became convinced that regulators in some countries started to apply sanctions against more and more companies that failed to prevent leaks of personal data and payment details. One in every five penalties reached $1M or more, with seven payouts exceeding $10M and one reaching $100+ million. It looks like information protection regulations are getting stricter than ever, and the number of fines amounting to tens or even hundreds of millions of dollars will grow dramatically in 2019.

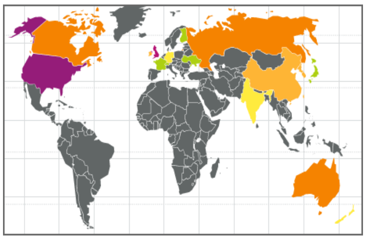
Being in effect since May 25, 2018, the GDPR is to play a key role in this process, as enterprises that violate the GDPR may be fined up to 4% of their turnover. As a result, it is entirely possible that large businesses will be charged billions for high-profile incidents in the future.

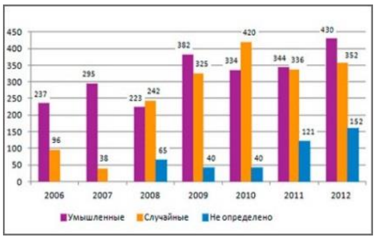
Such regulatory mechanisms push companies to give a lot of thought to protecting their information assets, as any confidential data breach can now potentially result in huge financial losses, i.e. large penalties. Moreover, this situation gives corporate security officers a good opportunity to argue for increasing corporate cybersecurity budgets.

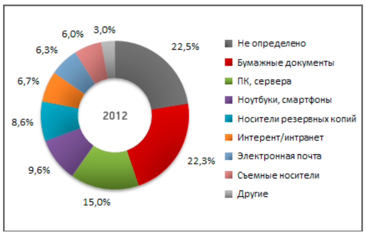
# Data Breach Monitoring on the InfoWatch Website

InfoWatch Analytics Center regularly posts data leakage reports on its website, as well as the most notorious incidents commented by InfoWatch experts.

In addition, the website contains data leakage statistics for past years, available in the form of dynamic diagrams.







Follow the leakage news, new reports, analytical and popular articles via our channels:

- Email
- Facebook
- Twitter

**InfoWatch Analytics Center**
https://www.infowatch.com/analytics

# Glossary

**Information security incidents** *in this research mean cases of compromising confidential information as a result of data leaks and/or destructive actions by employees.*

**Data leak** *means losing control over information due to external intrusion (attack), access abuse, or unauthorized access.*

**Destructive actions by employees** *mean personnel actions that resulted in the compromising of confidential information, including the use of confidential information for personal needs associated with fraud; illegal access to information (abuse of access rights).*

**Confidential information** *in this context means information which can be accessed by a limited number of expressly identified persons subject to its non-disclosure to third parties without the consent of an information owner. In this report, the term "confidential information" also includes personal data.*

**Intentional/Accidental Leaks.** *Intentional leaks mean an information leakage when a user, who works with information, could foresee negative implications of his or her actions, knew about their illegal nature, was warned about liability, and acted for personal gain or benefit. This results in a risk of losing control over information and/or committing a confidentiality breach. In this case, it does not matter whether such user's actions actually led to negative consequences or corporate losses.*

*Accidental leaks mean information leakages when a user neither foresees negative implications of his/her actions, nor acts for personal benefit. In this case, it does not matter whether such user's actions actually led to negative consequences or corporate losses. The terms "intentional/malicious" and "unintentional/accidental" are equal and used as synonyms herein.*

**Attack vector** *means a classification criterion of intruder's actions behind data leakage, including intruders who attack company's web assets and IT infrastructure from the outside to compromise data, and insiders who obtain unauthorized access to classified resources and misuse confidential information, etc.*

**Data channel** *means a scenario which results in the loss of control over information and a breach of its confidentiality. Currently, we identify eight separate leak channels:*

- ✓ *Theft/loss of equipment (server, data storage, laptop, desktop), with information being compromised during maintenance or due to the loss of such equipment*
- ✓ *Mobile devices where data leakage occurs because of unauthorized use or theft of a mobile device (smartphone, tablet) when used as part of BYOD paradigm*
- ✓ *Removable media loss/theft (CDs, flash drives)*
- ✓ *A network where data is leaked via a browser (sending data to personal email, filling in browser forms); unauthorized use of intranet resources, FTPs, and cloud services; and unauthorized information posting on a website*
- ✓ *Email, with data being leaked via corporate email*
- ✓ *Paper documents which can cause a data leakage if stored or utilized improperly (with confidential information printed, stolen, or taken out)*
- ✓ *Instant messengers (data leakage via voice, chat, and video communications)*
- ✓ *'Non-defined' is a category used when incident details appearing in mass media do not allow for the leak channel identification.*