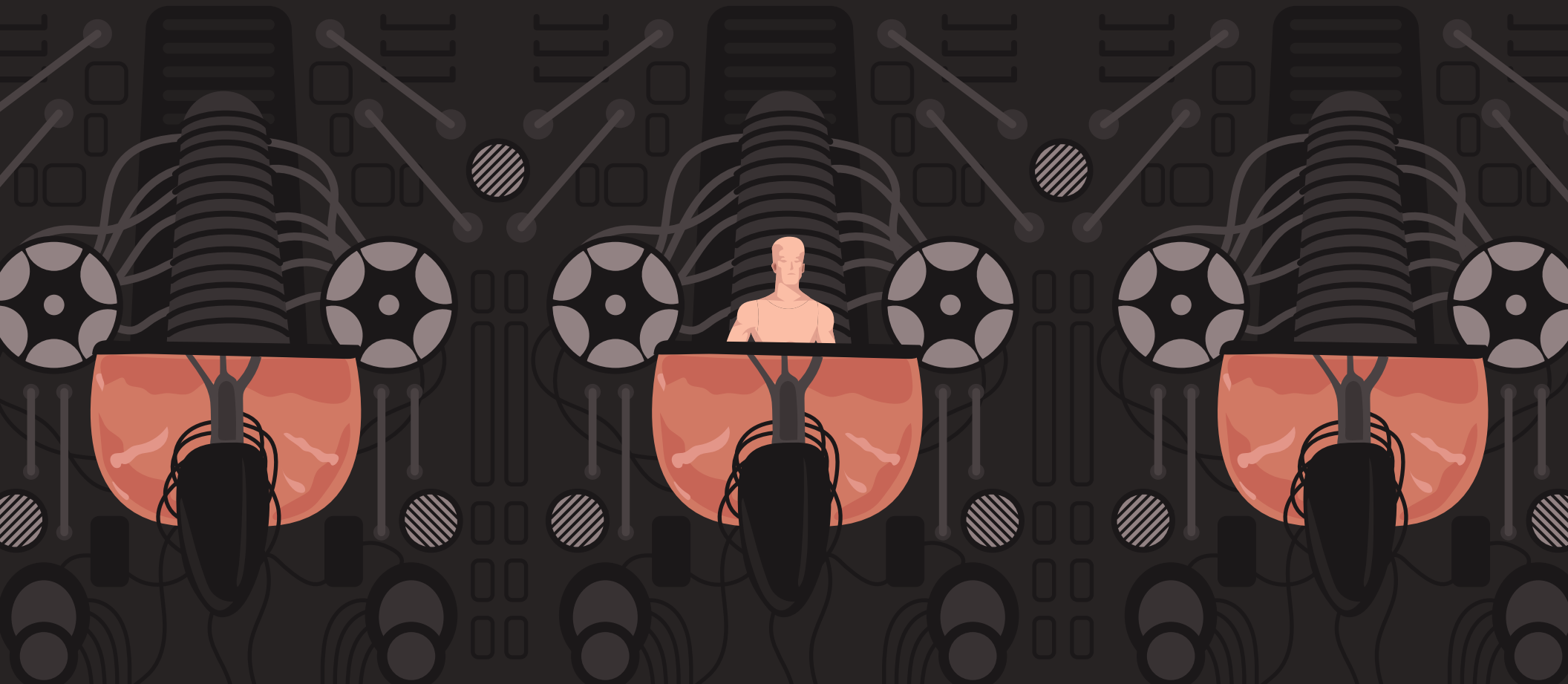

THE FINANCIAL
MATRIX
Bitglass' 2019 Financial Breach Report
bitglass

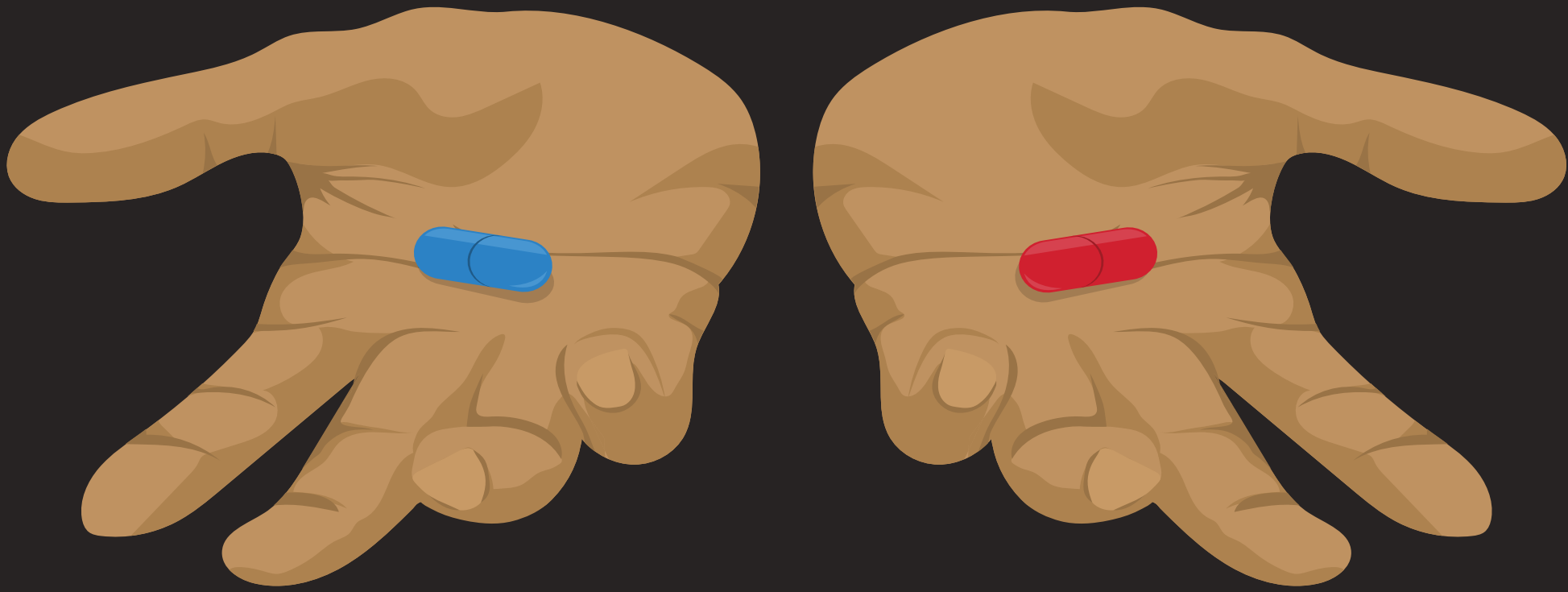
# The Awakening

Firms within the financial services industry must remain vigilant when it comes to cybersecurity. These organizations are entrusted with personally identifiable information (PII) such as home addresses, Social Security numbers, banking details, and more. Securing this information is of vital importance both for these organizations and their customers. Unfortunately, the high value of this type of data makes financial services organizations an attractive target for cybercriminals. With this in mind, Bitglass set out to uncover the state of cybersecurity within the financial services industry, scrutinizing breaches from the past year in order to find out how deep the rabbit hole goes.



# Blue Pill or Red Pill?

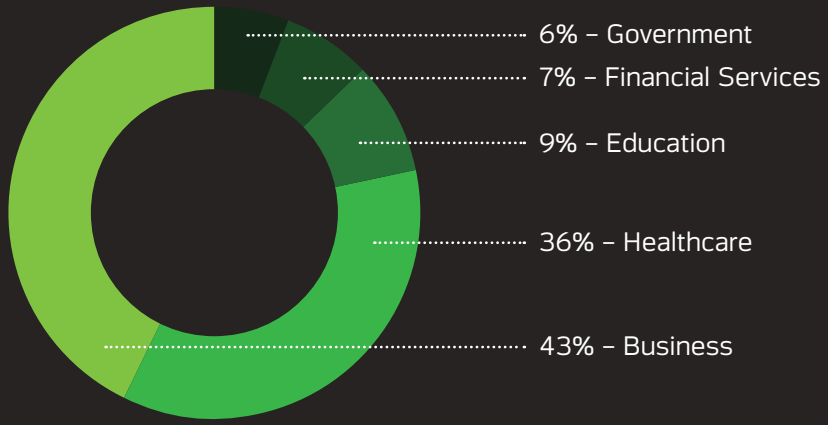
To perform this study, Bitglass compiled data from the Identity Theft Resource Center (ITRC) and the Ponemon Institute. Each year, these organizations conduct studies that provide detailed information about data theft in financial services firms. By analyzing their records in tandem, Bitglass was able to uncover insights about the financial breaches that occurred in 2019.



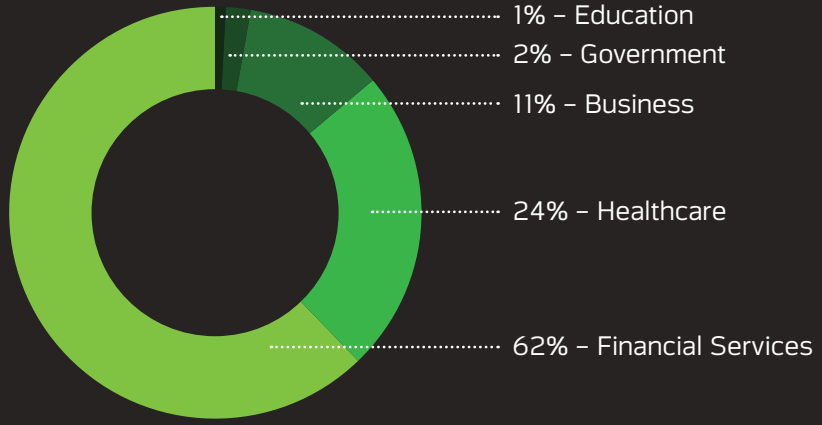
# The Truth, Nothing More

Only **6.5%** of all breaches that occurred this year were suffered by financial services firms. However, **61.7%** of leaked records were exposed by organizations in the financial industry (this is largely due to the Capital One mega breach, which exposed 100,436,121 records). Regardless, while financial services firms are not breached particularly often, their breaches tend to be much larger and more detrimental than those experienced by companies in other industries.

### Percentage of Breaches Per Industry in 2019




### Percentage of Leaked Records Per Industry in 2019

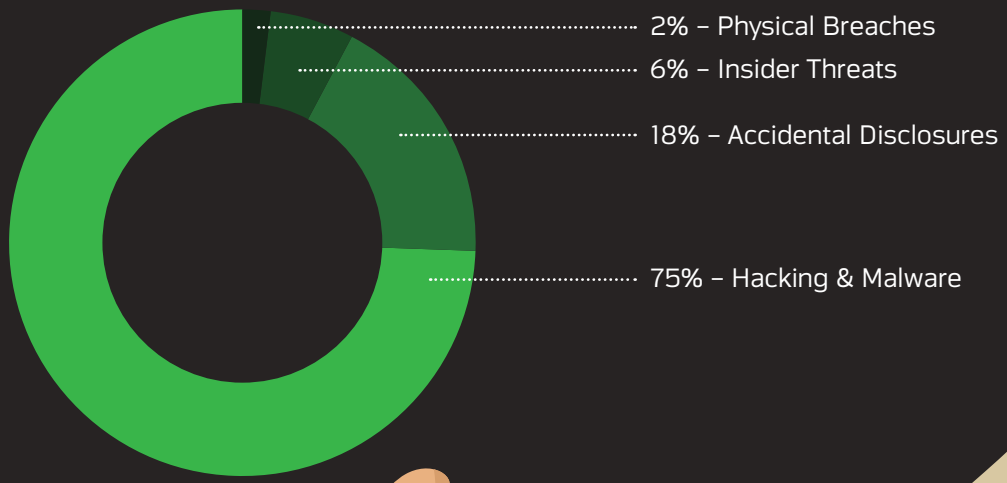



# Learning Kung Fu

As malware continues to evolve, it becomes more difficult to detect and block. Consequently, organizations in the financial services industry must learn to defend against these threats with the proper security tools.

This year, Hacking and Malware remains as the primary cause of data breaches in financial services (up slightly from **73.5%** in 2018). However, Ins ider Threats grew from **2.9%** in 2018 to **5.5%** today, while Accidental Disclosures increased from **14.7%** to **18.2%**. Unfortunately, for organizations that struggle with implementing proper security measures, rising cloud adoption will also lead to a rise in these threats.

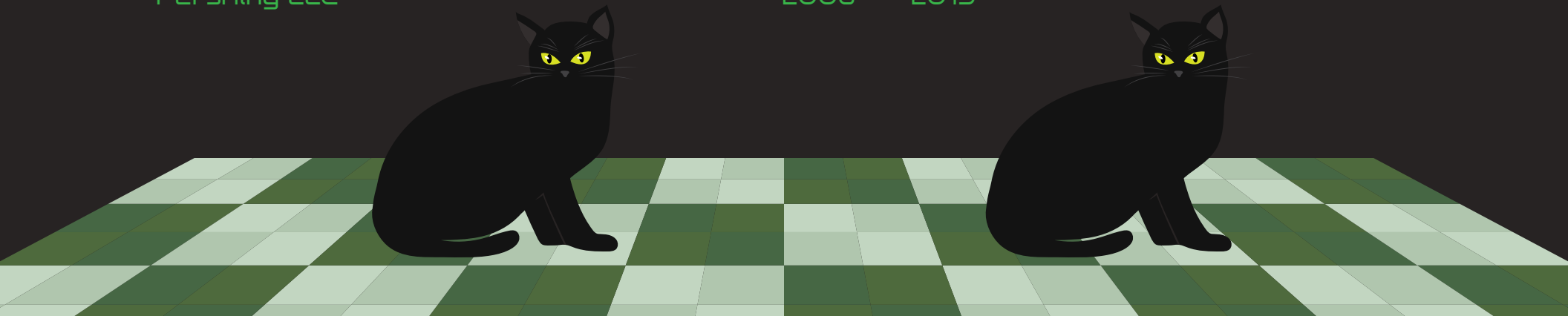
### Breach Types within Finanical Services



# The True Meaning of Déjà Vu

With global cloud adoption reaching **86%** and bring your own device (BYOD) policies finding their way into **85%** of organizations, it can be challenging to maintain proper visibility and control over data—particularly when the appropriate cloud and mobile security solutions are not put in place. Regardless, financial services firms need to be more cognizant of how their data is being used. Unfortunately, some organizations are still learning this lesson and, consequently, are suffering from recurring breaches.

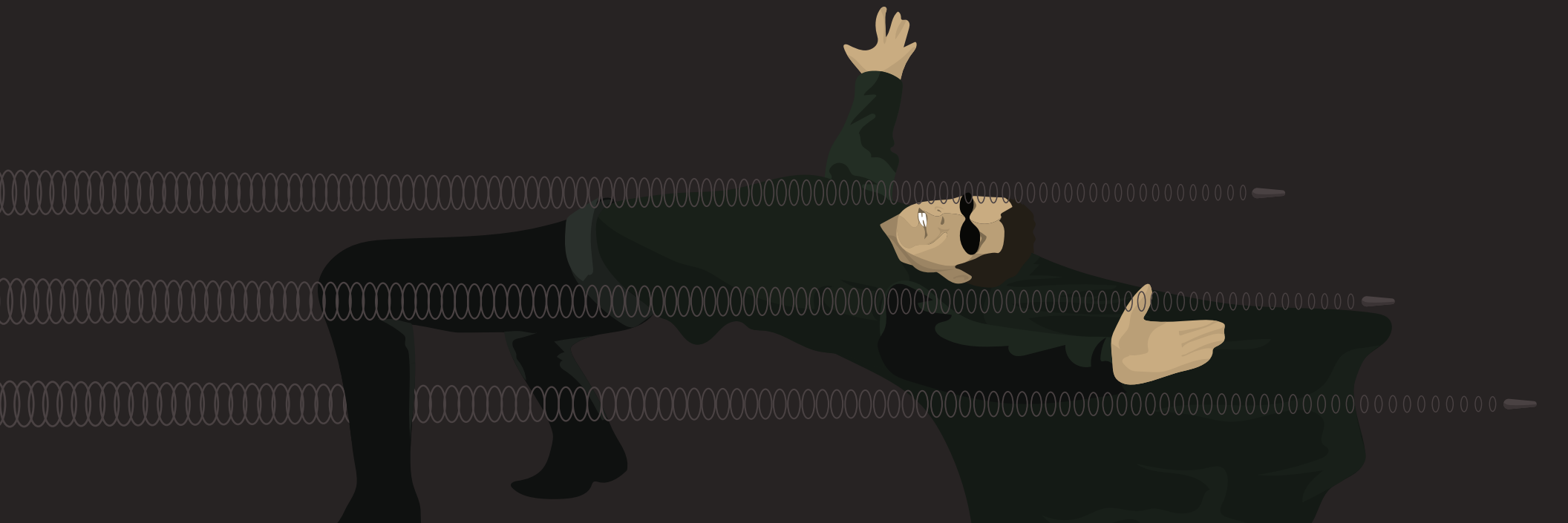
| Repeat Offenders | Years Breached | | | | |
|---|---|---|---|---|---|
| American Express | 2009 | 2012 | 2013 | 2014 | 2019 |
| SunTrust Bank | 2010 | 2011 | 2018 | 2018 | 2019 |
| Capital One | 2012 | 2013 | 2014 | 2019 | |
| Discover | 2006 | 2013 | 2014 | 2019 | |
| Lincoln Financial Group | 2010 | 2011 | 2019 | | |
| Jackson National Life Insurance | 2007 | 2011 | 2019 | | |
| Sage Advisors LLC | 2016 | 2019 | | | |
| Pershing LLC | 2006 | 2019 | | | |



# Bullet Time

Here we take a closer look at the top three breaches of financial services firms in 2019.

- In March 2019, there was a breach of sensitive data at Capital One Financial Corporation. According to Capital One, approximately 106 million individuals from the United States and Canada were affected, making it the third largest breach recorded in U.S. history.
- Centerstone Insurance and Financial Services was recently the target of a phishing campaign that lasted for four months. Throughout the campaign, the threat actor gained access to numerous employee email accounts and exfiltrated the data of 111,589 consumers.
- In May 2019, Nassau Educators Federal Credit Union learned that it was the victim of a phishing campaign. Ultimately, 86,773 records were surrendered, exposing individuals' Social Security numbers, debit and credit card numbers, and government identification numbers.

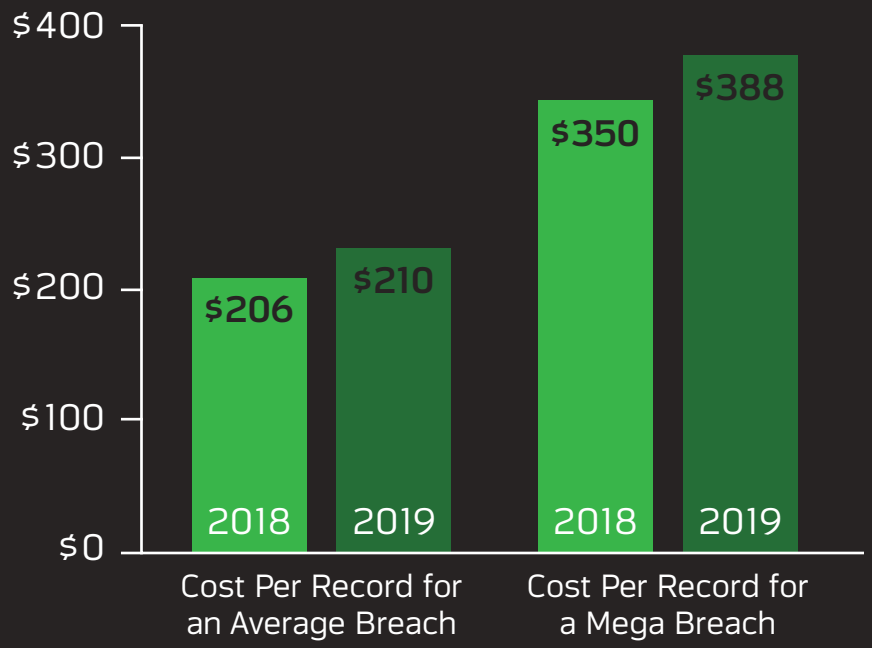


# Lessons from an Oracle

The cost per breached record in financial services has been increasing over the last few years—for regular breaches as well as mega breaches.* However, the cost per breached record for mega breaches is much greater than that of average breaches.

Additionally, Ponemon notes that the cost per breached record within financial services exceeds that of all other industries except healthcare (which was $429). Technology came in third place at $183, while the public sector came in last at $78.

**The Average Cost Per Compromised Record (Finanical Services)**




*Mega breaches are those that affected approximately 100M+ individuals

# Wrap-Up

Due to careless users, malicious insiders, evolving malware, advanced phishing schemes, and much more, financial services firms face a wide variety of threats. As such, they must make sure that they adopt a proactive approach to data protection and are properly equipped with the latest security technologies. Only then can they defend against threat agents in the cyber world.

bitglass

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com

## About Bitglass

Bitglass, the Next-Gen Cloud Security company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.