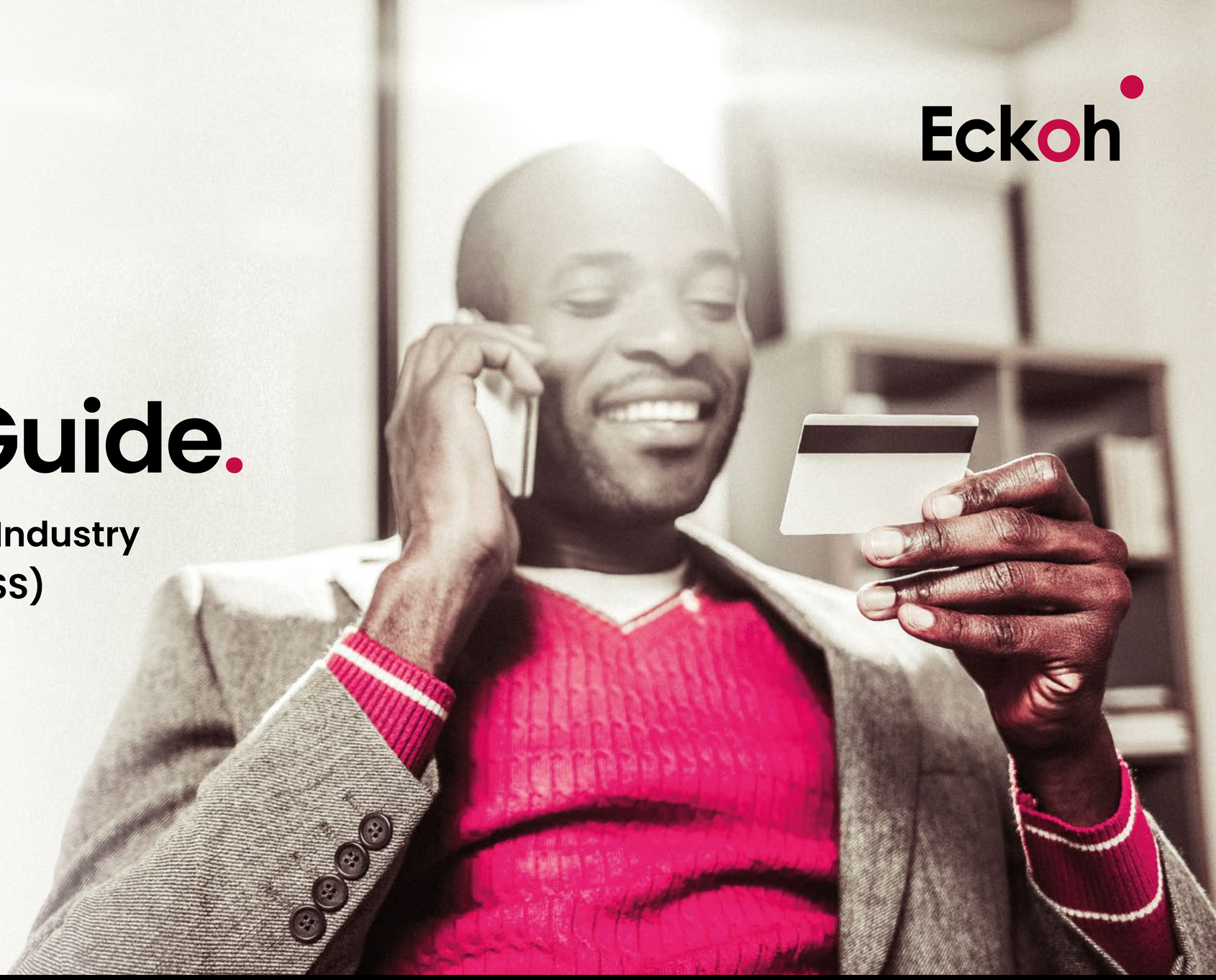
# PCI DSS Reference Guide.

## Navigating the Payment Card Industry Data Security Standard (PCI DSS)



# We are Eckoh.

Leading organizations **trust** Eckoh's data payment security solutions.

Since 2009, Eckoh has **transformed** contact centers across a range of sectors to be **efficient**, **secure** and **PCI DSS compliant.**

PCI Security Standards Council™

PARTICIPATING ORGANIZATION

With a long 20-year legacy of creating award-winning, efficient customer engagement automation solutions for contact centers, Eckoh is also a master in designing the most future-facing, flexible and robust payment security solutions for this market. Adjusting to changes in regulations, operating models, and customer behavior, we can make rapid and agile modifications to business processes without disruption to existing systems.

We constantly audit, research and innovate so that you can stay ahead of the competition, applying the latest techniques in first-class security technology within our customer engagement tools.

# What's in store?

**2.**
**Who does PCI compliance apply to?**

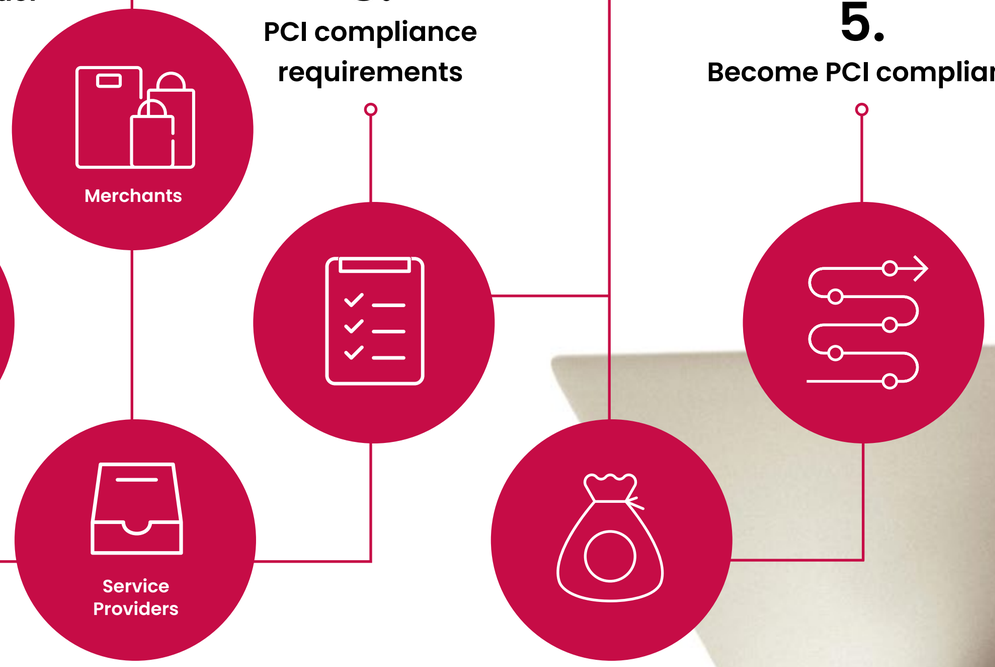
**4.**
**The cost of non-compliance**

**Click on the icons below** to jump to the page.

**1.**
**Protecting cardholder data** in contact centers

**3.**
**PCI compliance requirements**

**5.**
**Become PCI compliant**




# 1. Protecting cardholder data.

The Payment Card Industry Data Security Standard (PCI DSS) is a set by American Express, Discover Financial Services, JCB International, MasterCard and Visa.

The purpose of these security standards is to protect cardholder data from fraud, theft and data breaches. Although PCI DSS requirements are not law like the California Consumer Privacy Act, non-compliance is not an option and companies agree to follow these rules if they process, store or transmit cardholder data.

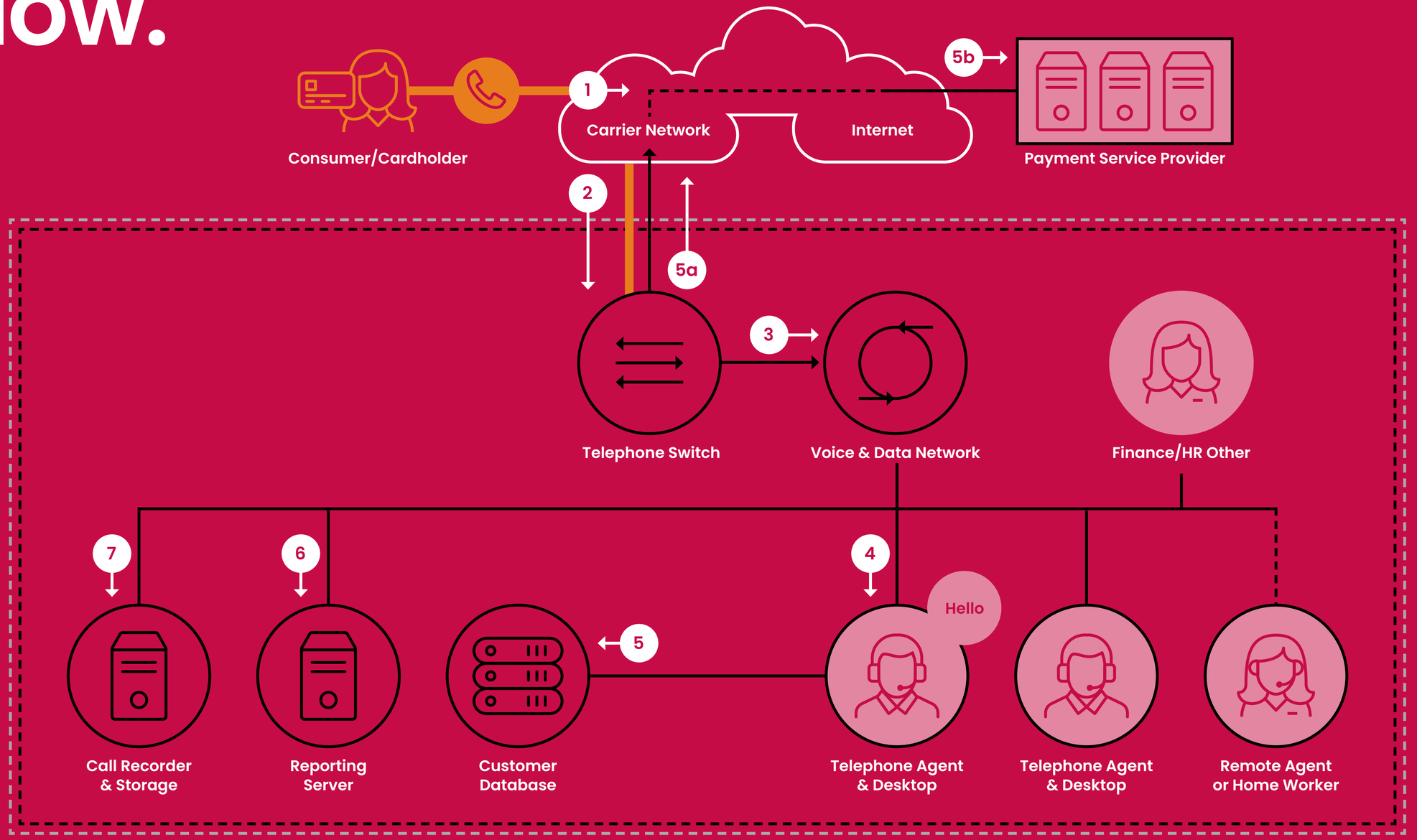
In 2018, The PCI Security Standards Council **(PCI SSC)** released supplemental information about securing payments in a card-not-present environment such as contact centers. This guidance is based on the three pillars of people, process and technology and the unique risks in sensitive cardholder data being transmitted in card-not-present transactions. For example, a customer providing their credit card number, expiration date and security code with a live agent in a contact center exposes cardholder data to the customer's phone carrier network, call recordings, servers, agent desktops, the agent and so much more.

Because of this increased attack surface and more companies moving to cloud solutions, the PCI SSC deems it critical to make telephone-based payments, especially those made over Voice over Internet Protocol **(VoIP),** in-scope for PCI DSS requirements. In short, any network or system that stores, transmits or processes cardholder data, that network/system is in-scope for PCI DSS compliance and needs to ensure cardholder data security.

# Call flow.

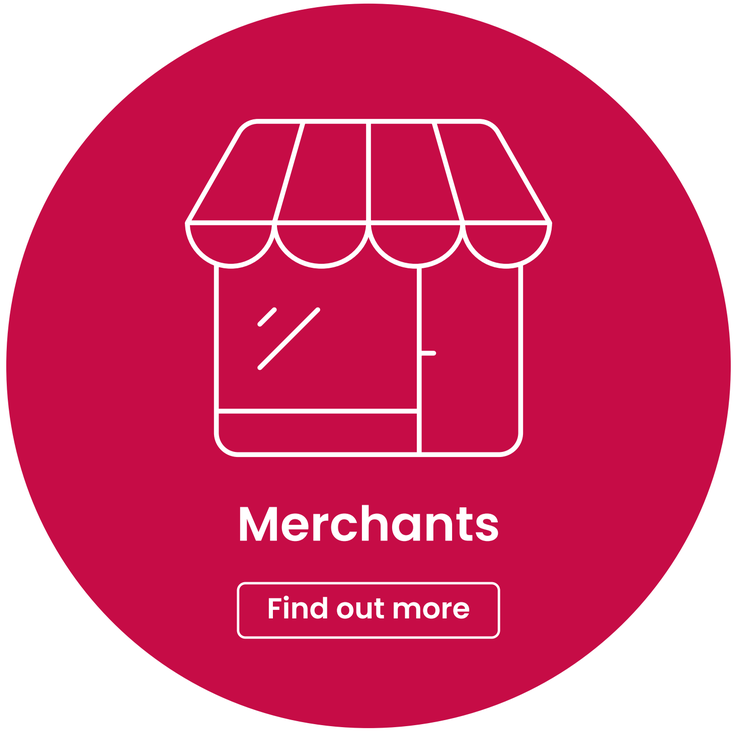
## Legend

- Out of PCI DSS Scope
- In PCI DSS Scope
- Service Provider
- Entity



# 2. Who does compliance apply to?

There are two very distinct categories for PCI DSS compliance:



**Merchants**

Find out more

**Service Providers**

Find out more

# 2. Merchants.



As far as the PCI Data Security Standard is concerned, a merchant is any organization that accepts transactions from the five major card brands: American Express, Discover Financial Services, JCB International, MasterCard and Visa.

| Category | Criteria | Requirement |
|---|---|---|
| **Level 1** | Processes more than six million card transactions on an annual basis or has suffered a hack or an attack that resulted in an Account Data Compromise Event. | Annual PCI DSS assessment resulting in the completion of a Report of Compliance **(ROC).** |
| **Level 2** | Processes one to six million card transactions on an annual basis. | Annual Self-Assessment Questionnaire **(SAQ).** |
| **Level 3** | Processes 20,000 to one million card transactions on an annual basis. | Annual Self-Assessment Questionnaire **(SAQ).** |
| **Level 4** | All other merchants. | Annual Self-Assessment Questionnaire **(SAQ).** |

Each card company does have minor differences in their definition for levels in regards to transaction numbers. Some payment providers, partners and clients may require you to level up in order to meet their specific security needs.

# 2. Service Providers.

Service providers are defined by the PCI Security Standards Council as any business entity that is not a payment brand that is directly involved with the storing, transmission or processing of payment card data.

| Category | Criteria | Requirement |
|---|---|---|
| **Level 1** | Store, transmit or process more than 300,000 card transactions on an annual basis. | • Annual ROC by a Qualified Security Assessor (**QSA**).<br>• Quarterly Network scan by an Approved Scanning Vendor (**ASV**)<br>• Penetration Test<br>• Internal Scan<br>• Attestation of Compliance Form (**AOC**) |
| **Level 2** | Store, transmit or process less than 300,000 card transactions on an annual basis. | • Annual Self-Assessment Questionnaire D (**SAQ-D**)<br>• Quarterly network scan by **ASV**<br>• Penetration Test<br>• Internal Scan<br>• **AOC** Form |

# 3. Compliance requirements.

Within the below 12 requirements are hundreds of sub-requirements that go well beyond the initial measures. Some can be extremely difficult to meet and partnering with experts can help.

**Build and Maintain a Secure Network**

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

**Protect Cardholder Data**

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

**Maintain a Vulnerability Management Program**

5. Use and regularly update anti-virus software of programs.
6. Develop and maintain secure systems and applications.

**Implement Strong Access Control Measures**

7. Restrict access to credit card data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to stored cardholder data.

**Regularly Monitor and Test Networks**

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

**Maintain an Information Security Policy**

12. Maintain a policy that addresses information security for employees and contractors.

# 4. Cost of non-compliance.

Although PCI DSS is not law, there is a cost for non-compliance if you're doing business with the five card companies that oversee PCI. The most common four areas of cost are as follows:

**One to three months**

Between $5,000 per month for low-volume merchants and $10,000 dollars per month for high-volume merchants.

**Four to six months**

Between $25,000 per month for low-volume merchants and $50,000 for high-volume merchants.

**Longer than seven months**

$50,000 per month for low-volume merchants to $100,000 per month for high-volume merchants.

**Data breach**

Between $50-$90 per customer affected by the data breach, depending on the merchant's monthly transaction volume.

Additionally, payment processors will also fine a merchant.

# Cost of a Data Breach.

There are also hidden costs for not adhering to PCI compliance.

Some are more challenging to put figures to such as how non-compliance affects cybersecurity insurance, but here shows some key statistics from the 2021 IBM Cost of a Data Breach Report.

**The average cost of a data breach for a US company is $9.05 million** (Higher than the worldwide average of $4.24 million.)

Where **remote working** is involved with a data breach, the costs average $1.07 million more.

**Healthcare continues to be the highest cost industry** averaging $9.23 million.

**Churn after a data breach averages 38% of a company's customer base** averaging $1.59 million in additional financial loss.

It takes an average of **287 days** to identify and contain a breach.

# 5. Become PCI compliant.

## Assess

Identify which level of compliance your organization qualifies for.

Analyze your current IT systems and business processes that involve payment data storing, transmitting or processing.

Identify any vulnerabilities such as pause-and-resume, remote workers or cardholder data being transmitted across your telephone or network.

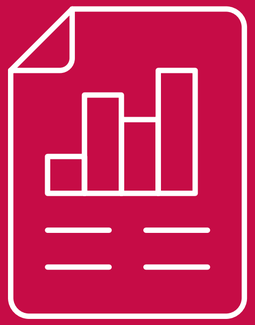
## Remediate

Eliminate the vulnerabilities by partnering with vendors that remove the risk of storing, transmitting or processing cardholder data. The best approach is to never let this sensitive data touch or traverse across any part of your environment or come in contact with any agents.

Put processes in place that reduce your risk level and prepare your organization for responding to a data breach.


## Repeat

PCI Compliance is an ongoing process. It's best to ensure any vendors you do work with in this area are not just experts, but also proactively innovate for any future changes to PCI DSS.



## Report

Complete the necessary reporting for your merchant level.

# Glossary of terms.

**Key terminology**

| | |
|---|---|
| **PCI DSS** | Payment Card Industry Data Security Standard |
| **PCI SSC** | Payment Card Industry Security Standards Council |
| **SAQ** | Self-Assessment Questionnaire |
| **VoIP** | Voice over Internet Protocol |
| **ROC** | Report of Compliance |
| **QSA** | Qualified Security Assessor |
| **ASV** | Approved Scanning Vendor |
| **AOC** | Attestation of Compliance |

**Listed here are the SAQ levels appropriate for contact center environments taking card-not-present payments:**

**SAQ-A**

Merchants accepting card-not-present payments, such as over the phone or via ecommerce, that have fully outsourced all PCI DSS functions for storing, transmitting or processing cardholder data. If the merchant is qualified for SAQ-A, no electronic storage, transmission or processing can touch their systems or premises.

**SAQ-D**

If the merchant does not meet SAQ-A requirements, they are required to complete an Attestation of Compliance. SAQ-D is the most comprehensive questionnaire and includes provisions for all of the PCI DSS requirements.

# We're ready. Are you?



This Guide to Safe Payments is to inform and educate merchants and other entities involved in payment card processing.

For more information about the **PCI SSC** and the standards we manage, please visit **www.pcisecuritystandards.org**.

The intent of this document is to provide supplemental information, which does not replace or supersede PCI Standards or their supporting documents.

**Get in touch**

**www.eckoh.com**

Eckoh