Chargent
by AppFrontier

Salesforce PCI GUIDE.

Reduce Your PCI Scope in Salesforce

For 83% of companies, experiencing a data breach is not a matter of if, but when - and the costs can be significant (IBM, Cost of a Data Breach 2022 Report).

In addition to the financial impact of fines and remediation costs, the most significant consequence of a data breach is the damage to customer trust. Your customers have shared sensitive information with you, and they expect that you will take data protection seriously - or they won't do business with your organization.

In this guide, you'll learn more about the requirements of PCI compliance, discover how advanced features in Salesforce and Chargent can help lower your PCI scope, and find resources to help you get started in validating your organization's PCI compliance.

What is PCI Compliance?

In order to better protect consumers, and reduce the risk of fraud and data breaches, Visa, Mastercard, American Express, Discover, and JCB collaborated to establish the Payment Card Industry Security Standards Council (PCI SSC) and set a minimum standard for data security.

Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards for all merchants that process, store or transmit cardholder data and/or sensitive authentication data, and it is applicable to any organization that accepts or processes payment cards.

PCI compliance is not a one-time event, but an ongoing process of adhering to security policies, procedures, software design, network architecture, and other security measures designed to make sure your customer's data is being kept secure.

These standards are not government regulations or laws, but guidelines for protecting cardholder data. Enforcement of PCI compliance is managed by individual payment companies and can include monthly fines, with escalating penalties based on payment volume.

Requirements of PCI Compliance

The PCI DSS provides a detailed, 12 requirements structure for securing cardholder data that is stored, processed, and/ or transmitted by merchants and other organizations.

Build and Maintain a Secure Network and Systems

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. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to 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 all personnel

Salesforce and PCI Compliance

While the appropriate use of Salesforce and Chargent offers a key foundation for achieving PCI compliance, ultimately your organization is responsible for all other security processes and handling of credit card data that you collect.

For Salesforce customers, Salesforce's PCI certification as a data storage service provider simplifies your PCI scope. Because Chargent never stores data outside of Salesforce, Salesforce's PCI certification covers your data while it is at rest in the Salesforce database.

Can I achieve PCI compliance by using Salesforce and Chargent?

Using Salesforce or the Chargent application can save time and effort in validating PCI compliance; however, this does not transfer **PCI compliance** to your organization. Your organization may need to achieve and maintain its own PCI compliance depending on your use cases.

Salesforce Security Features

Salesforce is designed to be highly secure while delivering the flexibility required to tailor your security design to meet the needs of your organization. Salesforce offers a number of security features that Salesforce System Administrators can configure to support their organization's PCI controls.

For complete details, we recommend reviewing Salesforce's **Security Implementation Guide**.

Chargent Key Features for PCI Compliance

Salesforce offers advanced security features to help you meet the requirements of PCI compliance. In addition, Chargent includes a number of capabilities to further reduce PCI scope. Read more in our **Chargent PCI Implementation Guide**.

Encrypted Custom Fields

For PCI Compliance, the Primary Account Number (PAN) may only be stored in Encrypted Custom Fields (ECF) in Salesforce. The PAN should not be stored in clear text fields, attached files, or any other location.

We recommend that all Chargent customers leverage **tokenization** to lower their PCI scope. However, if you have a use case that requires you to store account numbers, that can be accomplished securely with ECFs.

Salesforce PCI Compliance Tip:

Some payment data should never be stored in Salesforce, even in an Encrypted Field. If you store any of the data listed below, your use of Salesforce will be non-compliant with PCI.

- Full magnetic stripe/chip
- PINs/PIN blocks
- CAV2/CVC2/CVV/CID (3 or 4 digit card security code)

Credit Card Handling Field

Each Chargent Payment Gateway record includes a field called Credit Card Handling, which allows you to choose if, or how, credit card data is stored in different scenarios. This allows you to choose the appropriate option to fit your business processes while managing PCI risk.

Chargent Gateway Object

Permissions for the Chargent Gateway are customizable and if you only have one active gateway you can remove the Gateway field from page layouts, as the single active gateway will automatically be chosen for any transactions.

Chargent Payment Console

Chargent's Payment Console feature allows you to submit payments directly from Salesforce to your payment gateway. Transactions and tokens are created without ever saving or storing cardholder account number information in Salesforce.

Tokenization

Tokenization is a process by which a piece of sensitive information, such as a credit card number, is replaced by a surrogate value known as a token. Chargent recommends that all customers leverage tokenization to protect card data, adhere to data security best practices, and reduce PCI scope.

Chargent PCI Compliance Frequently Asked Questions

What are Chargent's data retention policies?

Chargent is not responsible for Salesforce data or retention policies: it is up to each Chargent customer to determine and configure when data should be removed from their Salesforce organization.

What are Chargent's access control mechanisms?
The Chargent team will not require any access to your company's Salesforce organization.

Access to the Chargent application for your company's Salesforce users is configured inside Salesforce. We recommend consulting with your Salesforce administrator to maintain your company's access policies.

How is Chargent managed once it is deployed?
The Chargent app is managed as part of your Salesforce system, like any Salesforce app that your company uses today. All **configurations and maintenance** will be completed by your company's administrator, your company's developers, or any consultants you hire. The AppFrontier support team is available to answer questions related to the setup and use of Chargent.

Why is Chargent not listed on PCI-DSS or PA-DSS sites?
Qualified Service Assessors have reviewed the AppFrontier architecture and determined that current PCI standards do not include advanced models like Salesforce AppExchange deployed applications, but that it is the responsibility of the customer to deploy and manage the Chargent software in compliance with applicable PCI DSS requirements. As a result, Chargent customers treat Chargent as a bespoke application when including Chargent in their PCI scope.

Additional Resources

- **PCI Security Standards Council**
- **PCI DSS Self-Assessment Questionnaire (SAQ)**
- **Payment Card Industry (PCI) Data Security Standard**
- **Salesforce Security Implementation Guide**
- **Salesforce Security, Privacy and Architecture Documentation**

Looking for additional guidance?

WE’RE ALWAYS HERE TO HELP!

Sales@AppFrontier.com

Chargent
by AppFrontier