

Enabling PCI compliant call tracking

Keep cardholder data information secure

CallRail helps businesses and marketers not only close the attribution gap by tracking [inbound phone calls](#) and [forms](#) from the marketing sources that drove them, but also provides insightful data into how each call is handled. But with providing actionable insights into conversations comes a great responsibility, especially for any business that processes payments and card data.

While payments and transactions online and over the phone increase, so do the phone conversations containing sensitive customer data that present potential security risks for both businesses and their customers.

That's why it is more important than ever before to ensure the personal identifiable information you handle is managed securely and responsibly.

How CallRail helps you enable PCI compliance for phone calls

PCI is the shortened acronym for The Payment Card Industry Data Security Standard ([PCIDSS](#)), a security standard that affects anyone handling any amount of customer credit card data; that includes the software companies, web developer, processors, sponsoring banks, and the merchants.

At CallRail, we take you and your customers' cardholder data seriously.

CallRail's PII redaction feature was built to help businesses uphold security standards and protect their customer's personal and financial data as well as reduce liability when payment information is exchanged during a phone call that is [recorded](#) or [transcribed](#).

Card [redacted] and the **card number** .

and the. [redacted] to [redacted] to repeat that [redacted]

[redacted] credit [redacted] **expiration** for [redacted].

Designed to look for and redact Personal Identifiable Information (PII), CallRail’s redaction feature removes the following sensitive items from your call recordings and transcripts:

- **Secure Information:** Social Security Number, Credit Card Number, Expiration, and CVV
- **Personal information:** Date of birth, Age, Religion, Political Affiliation
- **All Numeric Values:** Any number sequence of two or more numbers

Keep each cardholder's credit card information and other compromising customer data safe.

Keeping you and your customers safe with CallRail

PII/PCI Redaction

All Personal Identifiable Information is automatically redacted from call recordings and call transcripts once [PII Redaction feature is activated](#).

All data encrypted “in transit”

All access to CallRail is encrypted via SSL to protect data from interception on network points between the user and CallRail.

All data encrypted “at rest”

All call records, web visitor sessions, and call routing data are fully encrypted when stored on disk. This data is seamlessly decrypted as-needed for reporting purposes when accessed by the customer. These precautions protect the data even if hard drives fail, or are decommissioned or stolen.

Secure access

Individual users are granted their own login credentials, which can be controlled by an administrator. Login sessions automatically expire after a brief period of inactivity to prevent unauthorized access.

Firewalls and private network gaps

The databases, application servers, and other machines responsible for routing calls through CallRail are isolated and inaccessible via the public internet (except the web application itself, of course). This private network is protected by a pair of redundant hardware firewalls to ensure only expected traffic is allowed.