ENGAGE SMARTER

bold360 by LogMeIn

PCI DSS Compliance

Establish compliant payment processing through chat.

PCI DSS (Payment Card Industry Data Security Standard) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data and applies to all entities involved in payment card processing including merchants, processors, acquirers, issuers, and service providers.

"The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents."[1]

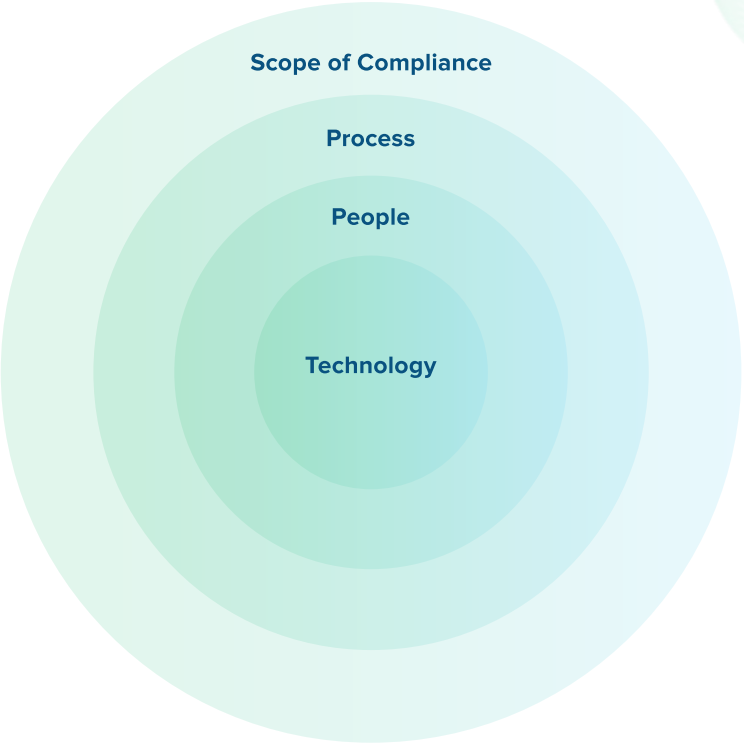
Key Features

The Bold360 solution is compliant with the core principles of PCI DSS and offers two distinct implementations:

The Redirect Method sends cards details directly from the visitor to the payment processor through a secure, encrypted connection and is supported by most payment processors. This is the recommended implementation.

The Chat Window SDK method integrates with payment processing platforms, so the payment processing information appears in a separate, but attached, chat window.

PCI DSS is built around six core principles and twelve main requirements:



The components of PCI compliance include people, process and technologies that store, manage, or transmit sensitive data.

1. Network security

- Installation and maintenance of a firewall configuration to protect cardholder data.
- Not using vendor-supplied defaults for system passwords and other security parameters.

2. Protecting cardholder data

- Protection of stored cardholder data.
- Encrypted transmission of cardholder data across open, public networks.

3. Maintenance of a vulnerability management program

- Application and maintenance of anti-virus software.
- Development and maintenance of secure systems and applications.

4. Implementation of strong access control measures

- Restrict access to cardholder data by business need-to-know .
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.

5. Regularly monitoring and testing networks

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

6. Maintenance of and information security policy

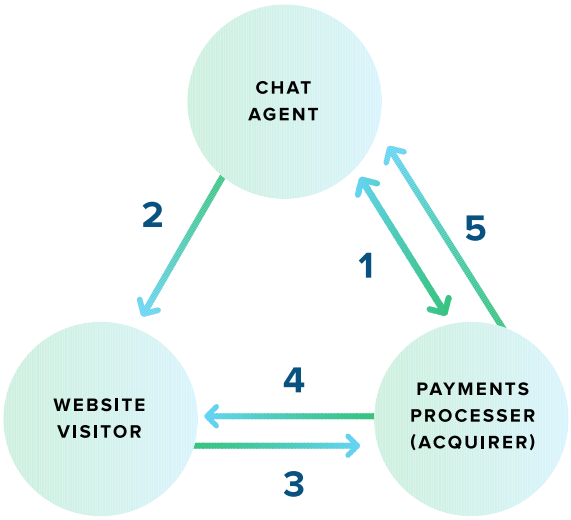
- Maintain a policy that addresses information security.

Bold360 in a PCI-DSS Environment

Bold360 by LogMeIn is a market-leading live chat and customer engagement solution that helps companies engage with their customers in the right way, at the right time to build loyalty, boost sales and improve operational efficiencies. PCI DSS compliance encompasses both people and processes, certifying that card payment information is always secure.

Bold360 software is compliant with the core principles of PCI DSS, but cannot dictate people and processes used by companies using the

software to take card payments from website visitors. While the process flow is identical, Bold360 recommends two distinct methods for PCI DSS compliance.



Redirect Method Process Flow

Where customer service agents are required to take payments over chat, Bold360 recommends using the redirect method. This approach is PCI compliant and is supported by most payment processors. Card details are sent directly from the visitor to the payment processor over a secure encrypted connection thus ensuring that card details are protected from the agent and back-office systems.

1. The agent obtains a one-time unique URL for this transaction using the back-office system and the redirect functionality of the acquirer's system.
2. The agent sends this URL to the website visitor over Bold360.
3. The visitor clicks on the URL which opens a payment card authorization window and enters their payment card details in this window.
4. The acquirer verifies the card payment and sends a payment confirmation message back to the card holder within the payment window.
5. The acquirer sends a transaction completed message back to the agent via the back-office system.

Chat Window SDK Process Flow

Otherwise, utilizing the Chat Window SDK, Bold360 can integrate with a payment processing platform (acquirer) to ensure that sensitive card information is never compromised. The payment processing platform appears in a separate, but attached, chat window and verifies the transaction to the agent handling the chat. This method provides a more consistent customer experience without redirecting the customer to a separate page.

1. Locate appropriate Chat Window SDK to incorporate PCI code (same as code that would appear on your shopping cart checkout page) into your chat windows.
2. When customer is ready for payment, agent uses a pre-defined canned message that triggers a new payment frame chat window.
3. Visitor can enter payment information into new chat window and continue conversation with agent.
4. Agent and visitor are notified the payment is complete (dependent upon user's integration with the payment processor).

Each of these methods maintains compliance and provides a smooth and secure payment experience for your customers. The Bold360 solution supports the implementation of either of these methods to help you establish and maintain security for you and your customers.

1. https://www.pcisecuritystandards.org/security_standards/