PCI Compliance

Anyone involved with the processing, transmission, or storage of card data must comply with the Payment Card Industry Data Security Standards (PCI DSS). This is why ThenMedia uses Stripe's embeddable card-payment system, Stripe Checkout, to enable our clients to accept card payments on their website.

The simplest way to be PCI compliant is to never see (or have access to) card data at all. Stripe makes this easy as they do the heavy lifting to protect customers' card information. By using Stripe Checkout, payment information is securely transmitted directly to Stripe without it passing through our servers.

Stripe has been audited by a PCI-certified auditor and is certified to PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry. To accomplish this, Stripe use the best-in-class security tools and practices to maintain a high level of security at Stripe.

Encryption of sensitive data and communication

All card numbers are encrypted at rest with AES-256. Decryption keys are stored on separate machines. None of Stripe's internal servers and daemons can obtain plaintext card numbers but can request that cards are sent to a service provider on a static allowlist. Stripe's infrastructure for storing, decrypting, and transmitting card numbers runs in a separate hosting environment, and doesn't share any credentials with Stripe's primary services (API, website, etc.).

Using TLS and HTTPS

TLS (Transport Layer Security) refers to the process of securely transmitting data between the client and our server. This was originally performed using the SSL (Secure Sockets Layer) protocol. However, this is outdated and no longer secure, and has been replaced by TLS. The term SSL continues to be used colloquially when referring to TLS and its function to protect transmitted data.

TLS attempts to accomplish the following:

- Encrypt and verify the integrity of traffic between the client and our server
- Verify that the client is communicating with the correct server. In practice, this usually means verifying that the owner of the domain and the owner of the server are the same entity. This helps prevent man-in-the-middle attacks. Without it, there's no guarantee that you're encrypting traffic to the right recipient.

All ThenMedia sites are served securely using TLS. This includes ThenMedia Cloud and even websites which don't include Stripe Payments.

Stripe Payment Flow