Report on PCI Compliancy

Context

Cardholder data such as Primary Account Number (PAN), Cardholder Name, Expiration Date, CVV code, PIN, and authentication data is highly sensitive customer data that needs high protection.
Industry standard Payment Card Industry (PCI) Data Security Standard (DSS) defines compliancy rules for processing cardholder data in order to prevent credit card fraud.
With this report, MENU describes its role in the context of the PCI DSS.

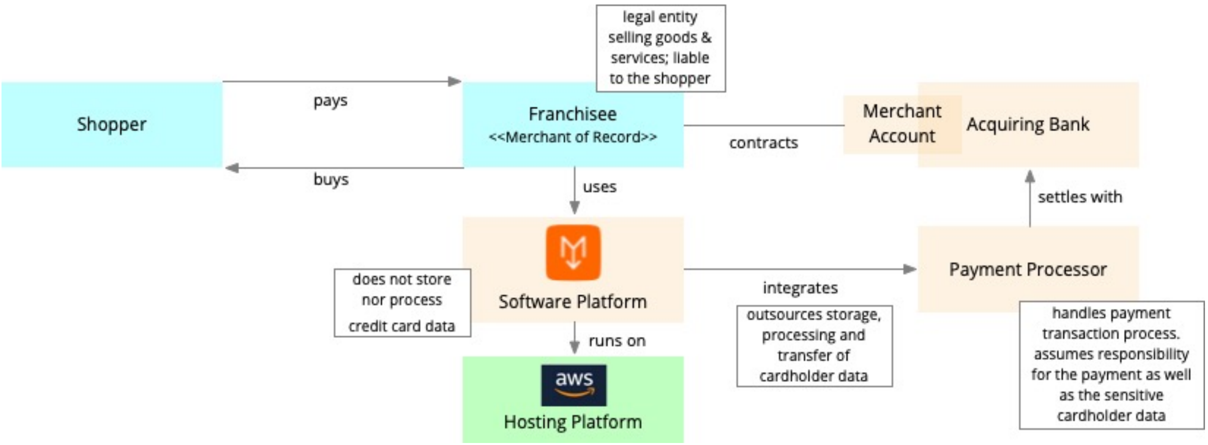
legal entity selling goods & services; liable to the shopper
Shopper
pays
buys
Franchisee
<<Merchant of Record>>
contracts
Merchant Account
Acquiring Bank
uses
settles with
does not store nor process credit card data
Software Platform
integrates
Payment Processor
outsources storage, processing and transfer of cardholder data
handles payment transaction process. assumes responsibility for the payment as well as the sensitive cardholder data
runs on
aws
Hosting Platform

Fig. 1: Merchant of Record Model applied by MENU

Roles

When using the MENU system, the MENU client (typically a franchisee) takes the role of a **merchant of record (MoR)**. The MoR is the legal entity selling goods or services to a cardholder and to whom the cardholder owes payment for such goods and services.
The MoR processes all payments and takes on all of the liability related to those transactions, including collecting sales tax, ensuring payment card industry (PCI) compliance, and honouring refunds and chargebacks.
The MoR uses the MENU system to execute these operations. The MENU system outsources the storage, processing and transmission of cardholder data to third party services (payment gateways and payment processors).
The **payment service provider** (PSP) handles the transaction process – the part where money leaves the customer's bank account and arrives in the merchants bank account. With PSP, sensitive data is sent directly from the payer's browser to the Payment Provider, without actually running through 'merchants' servers. PSP assumes responsibility for the payments, relieving the merchants of transactional security risks.

Implementation

The MENU system does not store nor process or transmit any sensitive cardholder data. Depending on the specific payment integration, this is implemented with native SDKs on mobile devices and hosted pages in iFrames in the web application.
Users insert credit card information directly in forms provided by the PSP. The PSP returns a token to the MENU system that uniquely identifies the payment without exposing the cardholder data.

PCI Standards compliancy

Because the MENU system is not storing nor processing nor transmitting any sensitive cardholder data, it is PCI compliant according to **PCI DSS version 3 conforms to SAQ A**. See the self-assessment questionnaire (SAQ) of 8.2.2021 for reference.
For the same reasons, PCI Payment Application Data Security Standard (PA-DSS) is not applicable to MENU. PA-DSS applies to payment application vendors.
MENU fully outsources all cardholder data functions to a payment provider. This payment provider needs to adhere to PA-DSS.