Excerpts from Best Practices Securing Ecommerce (PCI SSC, January 2017)
(https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf?agreement=true&time=1491340733142)

Electronic commerce, commonly known as e-commerce, is the use of the Internet to facilitate transactions for the sale and payment of goods and services. E-commerce is a card-not-present (CNP) payment channel and may include:

- E-commerce websites accessible from any web-browser, including "mobile-device friendly" versions accessible via the browser on smart phones, tablets, and other consumer mobile devices
- "App" versions of your e-commerce website, i.e., apps downloadable to the consumer's mobile device or saving of the URL as an application icon on a mobile device that has online payment functionality (consumer mobile payments)

An e-commerce solution comprises the software, hardware, processes, services, and methodology that enable and support these transactions. Merchants choosing to sell their goods and services online have a number of methods to consider, for example:

- Merchants may develop their own e-commerce payment software, use a third-party developed solution, or use a combination of both.
- Merchants may use a variety of technologies to implement e-commerce functionality, including payment-processing applications, application-programming interfaces (APIs), Inline Frames (IFrames), or payment pages hosted by a third party.
- Merchants may also choose to maintain different levels of control and responsibility for managing the supporting information technology infrastructure. For example, a merchant may choose to manage all networks and servers in-house, outsource management of all systems and infrastructure to hosting providers and/or e-commerce payment processors, or manage some components in house while outsourcing other components to third parties.

Merchants may also decide to engage a third party to perform services that support their e-commerce solution. The service provider or the services may be considered in scope for a merchant's PCI DSS compliance if the security of the solution is impacted by this service and the service provider has not performed its own assessment. For more information, see the section on "Use of Third-Party Service Providers/Outsourcing" in the PCI DSS. Examples of common e-commerce support services that may impact cardholder data security include:

a) Software development on behalf of the merchant
b) Hosted website, either fully or partially managed by the solution provider
c) Hosted data center/network/physical systems in support of a website
d) Shopping-cart software (including software that hands off transactions or customer information to other systems)
e) Order-management software such as chargebacks, returns, etc. that may have access to cardholder data
f) Other hosting options (offline data storage, backups, etc.)—depending on whether the data is encrypted and whether the service provider has access to the decryption keys
g) Merchant plug-ins to support payment brand and issuer authentication mechanisms
h) Managed services, including WAF or log-management services
i) Any service that transmits cardholder data (CHD) or handles this data in some other fashion on behalf of the merchant services that have access to the checkout or payment-processing flow, including those without a need to access cardholder data, third-party fraud analysis, or analytics tools

No matter which option a merchant may choose, there are several key considerations to keep in mind regarding the security of cardholder data, including:

- No option completely removes a merchant's PCI DSS responsibilities. Regardless of the extent of outsourcing to third parties, the merchant retains responsibility for ensuring that payment card data is protected. A merchant is responsible for performing due diligence to ensure the service provider is protecting the CHD shared with it in accordance with PCI DSS. Whether a merchant must conduct an onsite assessment or is eligible for a Self-Assessment Questionnaire (SAQ) is determined by the acquirer or payment card brands.
- Third-party relationships and the PCI DSS responsibilities of the merchant and each third party should be clearly documented in a contract or service-level agreement to ensure that each party understands and implements the appropriate PCI DSS controls. More information on these relationships can be found in the *Third-Party Security Assurance* Information Supplement on the PCI SSC website.
- It is recommended the merchant monitor connections and redirections between the merchant and the third party since the connections can be compromised. The merchant should ensure that no unexpected changes have occurred and that the integrity of the e-commerce solution is maintained.

- It is recommended that e-commerce payment applications, such as shopping carts, be validated according to PA-DSS, and confirmed to be included on PCI SSC's list of Validated Payment Applications. For in-house developed e-commerce applications, PA-DSS should be used as a best practice during development.

Payment protection resources for small merchants, guidance documents: *Guide to Safe Payments*, *Common Payment Systems*, *Questions to ask Your Vendors*, and *Glossary of Payment and Information Security Terms*