PCI Compliance FAQ

- **What is PCI DSS Compliance?**
  - PCI DSS (Payment Card Industry Data Security Standard) defines security requirements to protect environments where payment account data is stored, processed, or transmitted. PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data. (PCI Security Standards Council)

- **Why is being PCI-compliant important?**
  - If a merchant is involved in processing cardholder sensitive data, being PCI compliant helps prove that you are securely managing cardholder data that contains identity and financial information. This is a requirement set by the card brands.
  - If a cyberattack occurs through a merchant's system and they are not PCI-compliant, they will be held responsible for any misuse of information accessed through their business.
  - Processors impose PCI Non-compliance fees for any merchant not maintaining compliance.

- **Who is responsible for making a merchant PCI compliant?**
  - It is the merchant's responsibility to complete their yearly SAQ attestation and any quarterly scans, when applicable. If they are not familiar with their system's inner workings, they should request assistance from the person who installed their equipment.

- **Where does a merchant become PCI-compliant?**
  - Every processor provides the merchant with access to the portal designated for their PCI partnership. Merchants need to know the way to access their PCI compliance portal as soon as they are onboarded with any new processor.

- **What information does a merchant need in order to access their PCI compliance portal?**
  - They will need their Merchant Identification Number (MID) to access the portal, register their account, and begin their SAQ.
    - A MID can be found on a merchant's monthly statement or through their Merchant portal.
  - They will need an understanding of how their payment system is set up and the security measures in place to protect the cardholder data.

PCI Compliance FAQ

- **What is the process to become PCI compliant?**
    - A merchant will need to complete a Self Assessment Questionnaire (SAQ) based on their connectivity for processing payments. Example connectivities are Virtual Terminal, IP-Ethernet, Wireless, etc.
    - If their SAQ requires quarterly scans, the merchant will need to schedule a time for their system to be scanned and then attest to the scan results.
    - Once the initial steps are completed, the merchant is responsible for maintaining their compliance by scheduling scans and attesting their SAQ by the deadlines provided.

- **What is a scan?**
    - A merchant will schedule a scan of their system that processes cardholder information by inputting their IP address, setting a date and time for the scan, and making sure that there are no connections that can be accessed by outside sources.

- **When are scans required and how often?**
    - Scans are required based on certain connectivity.
        - SAQ B-IP
        - SAQ D
    - Scans are required to be run every quarter, and the results are attested after the scan passes.
    - If the scan does not pass, the merchant will need to use the results to figure out where the scan failed

- **What kinds of questions will the merchant need to answer on their SAQ?**
    - The questions are designed to make sure that a merchant is securing their data. Questions about whether there is remote access to their system, two-factor authentication, and if their system stores card data are examples of questions that are asked.

- **Some of the questions are outside of a merchant's knowledge. How are they supposed to know the answer?**
    - If they have more questions about the details, they can either ask their POS provider or the PCI platform company for further clarification.
    - As the merchant is a major piece of the payment processing community, they should become knowledgeable about what is required to make sure their business is safe from fraud.

- **Can merchants use an external PCI Company to complete their PCI?**
    - Of course! If there is an external PCI company the merchant is comfortable with, they can complete their SAQ and scan (if applicable). Once they attest the information is accurate and their portal shows they are 'compliant', they will need

to download their Attestation of Compliance and submit it to their new processor to update their current status.

- **How can I access my Attestation of Compliance?**
    - Your portal will have a link to 'Download AOC'. Provide that copy to your processor.

- **What if a merchant has multiple locations of the same restaurant? Are they required to complete a questionnaire for each location?**
    - Not necessarily. If all of the locations are operated by the same owner and all process the same way (i.e., all online-ordering or all brick & mortar), the processor can bundle the locations together, and the merchant will just need to complete the SAQ/scan process for the "main location."

- **How can the merchant combine and merge PCI compliance for all locations?**
    - First, pick a location to be the "main location."
    - Next, complete the SAQ & scan (if applicable) for that location and ensure they are fully compliant.
    - Finally, send a request to the processor or ISO to merge the list of other locations with the main location.
    - The processor will apply the compliance status of the main location to all other locations.