clearent™
built different.

PCI Compliance FAQs

For ISO & ISV Partners

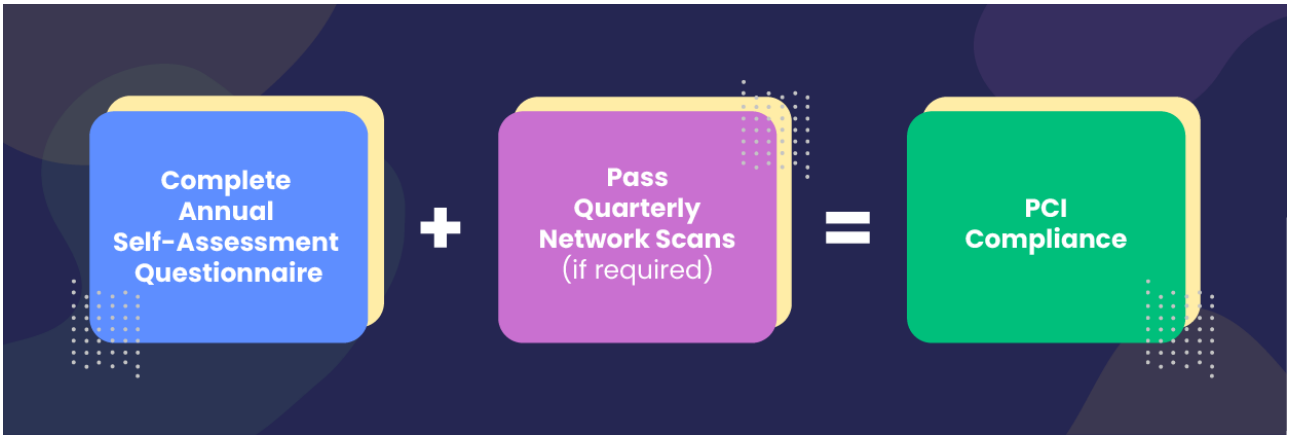
Compliance with the Payment Card Industry Data Security Standards (PCI DSS) is a requirement for all merchants set by the card associations. It's also one of the best ways to help protect business owners and their customers from a data breach and the severe financial loss that often accompanies these events. We have prepared these FAQs to help you and your merchants better understand what's new with our PCI program and what merchants need to do to become compliant. If you have questions or need more information, please contact Sales Support at salessupport@clearent.com or 866.203.7157 or contact your Partner Development Manager.

Q. What's changing with Clearent's PCI compliance program?

A. Effective April 1, 2022, if a business is required to complete quarterly network scans they must run and pass their scans in order to avoid the PCI Non-Compliance fee. The PCI Non-Compliance fee was formerly known as the PCI Non-Complete Questionnaire fee.

Q. How do merchants become PCI compliant?

A. Businesses are considered to be in compliance when they complete an annual self-assessment questionnaire and pass quarterly network vulnerability scans, if required by their questionnaire. Whether or not a business is required to scan their network every 90 days depends on how they process payments.



Q. How much will merchants be charged if they do not run and pass their quarterly scans before the required deadline?

A. If merchants do not run and pass any required scans by the appropriate deadline they will be charged a monthly PCI Non-Compliance Fee. The amount of this fee is listed on their merchant agreement.

Q. If a merchant runs and passes their network scans one quarter, but fails them the next, will they be charged the fee?

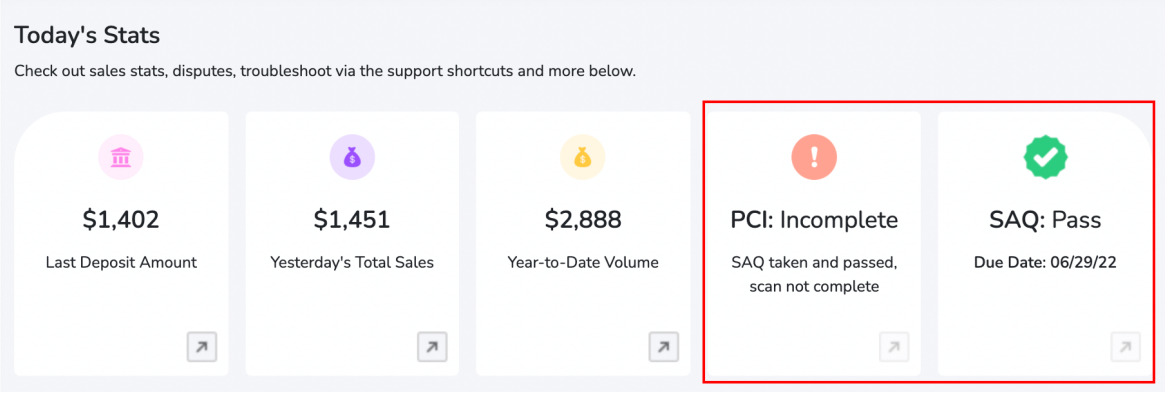
A. Yes. If merchants are required to run and pass network scans, they must pass them each quarter in order to avoid the PCI Non-Compliance fee.

Q. Will merchants continue to use New Merchant Home to find out their compliance status?

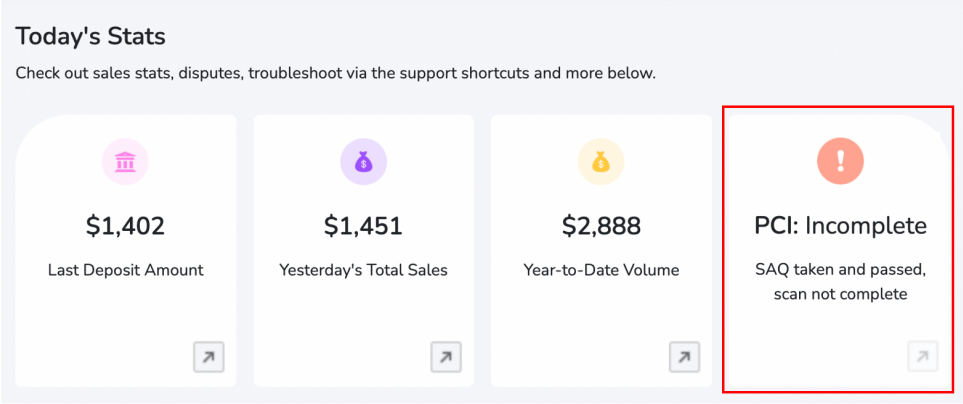
A. Yes. Merchants will continue to use New Merchant Home to learn their compliance status and access the DataGuardian portal. This is where they complete their questionnaire and schedule and run any required scans.

We're changing the New Merchant Home dashboard to make it easier for merchants to understand their compliance status. Merchants currently see two areas related to PCI compliance, as shown below. Going forward, there will only be one.

Current Dashboard



New Dashboard



Q. What statuses might a merchant see on the dashboard?

A. Depending on where merchants are in the PCI compliance process, they might see one of the following statuses in the PCI section of their dashboard in Merchant Home. The following chart lists those statuses and whether or not merchants will be billed the PCI Non-Compliance Fee.

PCI Compliance Status Description	Will merchant be billed PCI Non-Compliance Fee?
SAQ taken and passed, scan not required	No
SAQ taken and passed, scan passed	No
SAQ expired	Yes if SAQ is not taken and passed by renewal date
SAQ required, not taken	Yes
SAQ taken and failed	Yes
SAQ taken and passed, scan failed	Yes
SAQ taken and passed, scan not complete	Yes

Q. The requirement to run and pass quarterly scans will be new to some merchants. Will there be a grace period?

A. We understand merchants may need some time to get up to speed on the scanning requirement. This is where the Billable Merchant Policy comes into play. Clearent offers a grace period on all monthly fees for three billing cycles or until the merchant's activity is greater than or equal to $15.00, whichever occurs first. The timing of when these monthly fees are billed is based on when the merchant is boarded and when their activity begins, providing it is before the end of the three billing cycle grace period.

Q. How do merchants know if they need to complete a network vulnerability scan?

A. The chart below provides an overview of the processing methods associated with each self-assessment questionnaire. Whether or not a merchant is required to scan their network every 90 days is also included. As you will see, not all questionnaires require scans.

Scans Required	Scans NOT Required
• **SAQ A-EP:** Merchant has an eCommerce website that does not receive cardholder data but controls how consumers or their cardholder data are redirected to a validated third party payment processor. Merchant does not store credit card information electronically. • **SAQ B-IP:** Merchant uses a stand-alone or PTS-approved point-of-interaction device with an IP connection to the payment processor. Merchant does not store credit card information electronically. • **SAQ C:** Merchant uses a payment application system that is connected to the Internet. This includes most modern off-the-shelf POS systems and terminals on IP connections. Merchant does not store credit card information electronically. • **SAQ D:** Generally intended for merchants that electronically store cardholder data, use custom or proprietary payment applications, or payment applications installed on a network.	• **SAQ A:** Merchant outsources all credit card processing and credit cards are not present. Merchant has no face-to-face transactions and does not store credit card information electronically. • **SAQ B:** Business uses a manual imprinter, stand alone or dial out terminal. Merchant does not store credit card information electronically. • **SAQ C-VT:** Merchant uses a virtual terminal (Internet-based application) on a personal computer connected to the Internet. Merchant does not store credit card information electronically. • **SAQ P2PE:** Merchant uses hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption solution. Merchant does not store, process or transmit data outside of the hardware payment terminal.

Q. How do these changes impact the terms and conditions of the Merchant Agreement?

A. The terms and conditions of our Merchant Agreement are changing, effective April 1, 2022. These changes are being made in accordance with section 21 of the Merchant Agreement.

Q. How does Clearent help merchants become PCI compliant?

A. At Clearent, we make PCI compliance fast and easy by automatically enrolling merchants in the DataGuardian compliance and security program. Businesses receive a Data Breach Protection Policy that covers up to $100,000 in data-breach related expenses, hardware and software upgrades, consumer notifications and a team of forensic experts to guide them if they ever experience a breach. Plus, they can easily schedule any required network scans to automatically check their network and systems for vulnerabilities that could expose them to a data breach. You can learn more about DataGuardian in this flyer.