wepay
a CHASE company

PCI Compliance

As a platform, it's important to maintain compliance with PCI standards

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all platforms that process, store, or transmit credit card information protect cardholder data. All of these platforms are required to be compliant with PCI DSS, government, and bank requirements.

Payment facilitators working with platforms must also ensure the compliance of individual merchants operating on the platforms. These merchants are not exempt from PCI compliance, even if their payments are administered by a payment facilitator; though it may reduce the risk of exposure and thus the effort required to validate compliance.

While all merchants must be compliant with the PCI DSS, payment facilitators undergo additional scrutiny. Any platform that stores, processes, or transmits cardholder data for any third party must undergo an annual independent security audit as well as regular network vulnerability scans and penetration tests, among other equally stringent requirements.

As a platform, failure to comply with the PCI DSS may result in fines, higher transaction fees, and/or termination of the relationship between the Bank Card Associations (Visa, MasterCard, American Express, etc.) and the payment facilitator or merchant. Furthermore, platforms that suspect or confirm the unauthorized access, use, theft, or misappropriation of cardholder information incur additional obligations, including the responsibility to notify the relevant authorities and conduct a thorough forensic investigation, potentially by a reputable third-party forensic investigator. In addition, the vast majority of individual states throughout the U.S. have also passed laws that require companies to report data breaches to the affected parties.

It is important for platforms to maintain compliance because it demonstrates to customers, vendors, and suppliers the dedication to cardholder privacy. While platforms are required to annually validate compliance, the measures taken to become compliant should be treated as business as usual. Compliance should be maintained throughout the year to truly be effective in mitigating the ever-changing landscape of threats to all types of cardholder data environments. While designing compliance procedures and actions does not guarantee a business will not suffer a data compromise, which in most cases is not only financially but also brand damaging, it greatly reduces the chances of this happening.

Compliance can be difficult to manage. However, platforms don't have to worry about compliance alone. Besides handling payments transactions, the best payment facilitators and providers can assist platforms with value-added benefits to address PCI compliance concerns and share the responsibility, such as:

- Dealing with the banks on behalf of the platform
- Continuously managing and analyzing risk factors
- Automating and sending out tax documents, such as the IRS 1099 Form
- Meeting the necessary transmitter licensing requirements so platforms don't need to obtain a Money Transmitter License themselves
- Securing of payment and customer information with multiple layers of defense and a secure data protection model that combines physical and virtual security methods

WePay always ensures that our PCI compliance certification is up to date. To find out how WePay can help your platform comply with all PCI DSS, government, and bank requirements, click here, or go to wepay.com.