

Credit Card Security & PCI Compliance

Contributed by VinterActive Research

Disclaimer

VinterActive LLC does not offer legal advice and strongly encourages anyone seeking an opinion on compliance matters to consult with a qualified attorney. The information provided here is intended only to help interested readers learn more about some of the significant issues facing wineries and wine retailers on the internet.

Summary

Even the smallest wineries and wine retailers accepting credit card orders online are required by Visa, MasterCard and other major card companies to comply with the Payment Card Industry (PCI) Data Security Standard.

Failure to comply with the PCI standard can increase the risk of compromising your customers' cardholder data and subject your business to significant fines and restrictions imposed by credit card companies in the event of a security breach.

Knowing the requirements of the PCI Data Security Standard and demonstrating compliance can improve the security of your customer data and protect your business from fines and merchant restrictions.

In addition, prominently displaying evidence of PCI Certification on your ecommerce site has been shown to increase online sales 10-15% by making customers feel more secure.

How to Comply

The PCI Data Security Standard consists of 12 basic requirements intended to protect against cardholder data exposure and compromise:

- 1) Install and maintain a firewall configuration to protect data
- 2) Do not use vendor-supplied defaults for system passwords and other security parameters

- 3) Protect stored cardholder data

- 4) Encrypt transmission of cardholder data and sensitive information across public networks

- 5) Use and regularly update anti-virus software

- 6) Develop and maintain secure systems and applications

- 7) Restrict access to data by business need-to-know

- 8) Assign a unique ID to each person with computer access

- 9) Restrict physical access to cardholder data

- 10) Track and monitor all access to network resources and cardholder data

- 11) Regularly test security systems and processes

- 12) Maintain a policy that addresses information security

Regardless of the number of credit card transactions processed each year, every U.S. merchant accepting Visa, Mastercard or other major cards for online purchases must meet all the requirements of the PCI Data Security Standard.

In addition to meeting PCI requirements for data security, the Visa USA Cardholder Information Security Program (CISP) also mandates validation of compliance for any merchant processing 20,000 or more Visa ecommerce transactions per year. For smaller accounts, Visa recommends annual completion of a Self-Assessment Questionnaire and quarterly completion of Network Scan to identify potential security vulnerabilities.

The VinterActive Solution

VinterActive LLC helps wineries and wine retailers comply with the PCI Data Security Standard and recommended/required compliance validation by:

- 1) Including daily network scans & PCI compliance certification at no extra cost in our SecureWineShop™ ecommerce solution.
- 2) Offering FREE quarterly network scans, a self-assessment questionnaire, and certificate of PCI compliance in conjunction with our security partner, ScanAlert™.

We also strongly recommend our winery clients delete any credit card data stored online as soon as it has been used for payment processing. Our SecureWineShop™ offers a convenient Remove Credit Card Data button for this very purpose! Regardless of other security measures, the safest approach is to always minimize the amount of data you need to protect.

Learning More

Detailed requirements for compliance with the PCI Data Security Standard and validation requirements can be found at www.visa.com/CISP.

[Click here to visit ScanAlert and create a FREE Certified PCI Compliance account now, courtesy of VinterActive LLC.](#)