

CISP (Cardholder Information Security Program – Credit Card Masking)

What is Visa/MasterCard Cardholder Information Security Program (CISP)?

Visa's CISP defines a standard for securing Visa cardholder data, wherever it is located. CISP compliance is required of all entities that store, process, or transmit Visa cardholder data. **All member financial institutions must comply with CISP and are responsible for ensuring the compliance of their merchants for all payment channels. For this reason, many financial institutions are sending letters to their merchants identifying them "at risk of security issues".**

What do CISP requirements include?

CISP requirements include 12 basic security requirements with which all Visa merchants need to comply. They include the following:

- 1.) Install and maintain a working firewall to protect data
- 2.) Keep security patches up-to-date
- 3.) Protect stored data – *This is the requirement that involves POS software.***
- 4.) Encrypt data sent across public networks
- 5.) Use and regularly update anti-virus software
- 6.) Restrict access according to "need to know" basis
- 7.) Assign unique ID to each person with computer access
- 8.) Don't use vendor-supplied defaults for passwords and security parameters
- 9.) Track all access to data by unique ID
- 10.) Regularly test security systems and processes
- 11.) Implement and maintain an information security policy
- 12.) Restrict physical access to data

Why is it important for you to comply?

The CISP requirements help Visa members, merchants and service providers protect their information assets and meet the obligations of the Visa payment structure. Merchants also benefit from:

- **Consumer confidence:** Reports of hacker attacks, stolen credit card numbers, and identity theft have left consumers demanding absolute assurance that their account data and other personal information are safe.
- **Minimized threat to a customer's reputation and financial health:** Financial and resource outlay is minimal compared to the costs associated with the reactive hiring of security and public relations specialists, or the loss of significant revenue and customer goodwill that can result from a compromise.

If a merchant or service provider refuses to participate in CISP, Visa may impose a fine on the responsible Visa Member. Members are subject to fines of up to \$500,000 per incident for any merchant or service provider that is compromised and not CISP-compliant at the time of the breach.

How does point-of-sale software help merchants comply with CISP requirements?

According to the third requirement of compliance, merchants must ensure that they are protecting stored data at all times. Secure payment applications, when implemented in a CISP-compliant environment will minimize the potential for security breaches leading to compromises of full magnetic stripe data and the potential for damaging fraud resulting from these breaches.

What is the state of the POS industry regarding CISP?

With most merchants emphasizing speed of service through credit/debit card use, the payment card industry has placed a renewed focus on protecting consumer information. POS vendors have recognized these increasing pressures and have addressed the needs of the market by releasing updated versions of their software to comply with the CISP requirements.

Your Next Step...

Contact your NCBP representative today for a risk assessment and recommended protection.