III. PCI compliance (Lan Chang)

Many vulnerabilities might appear anywhere in the payment card system, and millions of cardholder data with sensitive information could be breached. These would affect the entire payment card ecosystem, including the credit of customers and the credibility of the merchants and financial institutions. As a result, it is important to use some standard security procedures and technologies to protect them. The PCI compliance would help alleviate these vulnerabilities and protect cardholder data, and ensure healthy payment card ecosystem.

First of all, what is PCI? PCI is a general term for the Payment Card Industry. It consists of all the organizations which store, process and transmit cardholder data. Specifically, it denotes the debit, credit, prepaid, e-purse, ATM, and POS cards and associated businesses. And the Payment Card Industry Security Standards Council (PCI SSC), which originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, maintains, evolves and promotes the standards for the safety. And the Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes, and it covers technical and operational system components included in or connected to cardholder data. If someone is a merchant who accepts or processes payment cards, he must comply with the PCI DSS.

The Payment Card Industry Data Security Standard helps protect the safety of the cardholder data. According to the Payment Card Industry Security Standards Council, there are twelve PCI compliant requirements that meet six security goals.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	Install and maintain a firewall configuration to protect cardholder data
	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Protect stored cardholder data
	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	Use and regularly update anti-virus software or programs
	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to cardholder data by business need-to-know
	Assign a unique ID to each person with computer access
	Restrict physical access to cardholder data

Regularly Monitor and Test Networks	Track and monitor all access to network resources and cardholder data
	Regularly test security systems and processes
Maintain an Information Security Policy	Maintain a policy that addresses information security for employees and contractors

Following these requirements, merchants and financial institutions could decrease the probability of any potential online theft, fraud and security breach.

In order to comply to the Payment Card Industry Data Security Standard, there are three ongoing steps for adhering:

Assess. Identifying cardholder data, taking an inventory of IT assets and business processes for payment card processing, and analyzing them for vulnerabilities.

Remediate. Fixing vulnerabilities and eliminating the storage of cardholder data unless absolutely necessary.

Report. Compiling and submitting required reports to the appropriate acquiring bank and card brands.

Since compliance is an ongoing process, it is recommended to perform annual audits to ensure real time safety and security of the systems. Compliance needs to be monitored constantly and enhanced according to needs within the organizational policies and procedures.

In summary, with the PCI compliance, we would get an actionable framework for developing a robust payment card data security process, including prevention, detection and appropriate reaction to security incidents.

Source: https://www.pcisecuritystandards.org/