CardSystems Solutions was a third-party payment processor that gathered transactions from thousands of small- and medium-sized businesses and processed them in batches for major credit card providers, such as Visa and MasterCard. This made them a perfect target for attack. Because of their high profile, they were told they had to comply with federal, state, and industry data security standards.

CardSystems contacted an auditor and in June 2004, they were certified as Payment Card Industry (PCI) Data Security Standard compliant. Relevant to the case, this standard certified that they were following a high standard of security and that their data was encrypted, but an assessment after the breach showed it was not. As a result of this comparatively simple hack, vulnerability at CardSystems Solutions was exploited and the company nearly ceased to trade and was eventually bought out.

On June 17, 2005, MasterCard disclosed that there had been a major data breach at CardSystems (Refer to the 1st Web site link given under the references section). It appears that a hacker or hackers gained access to the system through a web application, which customers used to access their own data. They used a SQL injection attack, where a small snippet of code is inserted onto the database through the front end (browser page). Once inserted onto the server, the code ran every four days. It gathered credit card data from the database, put it in a file (zipped to reduce size) and sent it to the hackers via FTP.

SQL injections can be as simple as copying and pasting code into a box on a Web page’s form. They are stopped comparatively easily by properly designed applications, a web firewall, and many other ways. These safeguards are required by the standard CardSystems to be allegedly in compliance. The fact an injection attack got through raised questions about their firewall. In addition, CardSystems had been storing the data for research in an unencrypted format.

The investigation found that CardSystems failed to apply a firewall or maintain virus definitions.

The Payment Card Industry Data Security Standard (PCI DSS) consists of standards, such as installing a firewall and anti-virus software while regularly updating virus definitions. It also requires companies to encrypt data. (Refer to the 2nd and the 3rd Web site links given under the references section).

**References:**

1. http://www.securityfocus.com/news/11219
2. http://www.wired.com/science/discoveries/news/2005/06/67980
3. http://usa.visa.com/download/merchants/pci-standard-best-answer.pdf