billable service that may provide a nearly endless amount of billable work for you and your firm.

If you haven't heard by now, the Payment Card Industry (PCI) Security Standards Council has developed a rigorous set of "data security standards" (DSS) for how businesses must protect the security of customer credit card numbers.

These standards for compliance are incredibly far-reaching, and will put the fear of God into any business owner who has heretofore paid little attention to the details of how credit card numbers are stored into the QuickBooks data file, CRM database or online Web store. New compliance regulations are mandated by the credit card companies, and deadlines for complying have already passed (July 1, 2010 was the final compliance date).

I can't emphasize enough how big of a problem there is in small businesses with regard to securing customer credit card numbers. For years, the businesses on Main Street have paid little or no attention to *security* of customer credit card numbers. Instead, the main focus has been on how to streamline the process of *storing* the numbers into software systems such that they can facilitate fast retrieval of the card numbers during the sales process. What we have now is a major case of trying to get all the cattle back into the barn, and then buying a lock for the door.

What is PCI DSS?

The PCI DSS is a set of comprehensive requirements for enhancing customer credit card data security. The standards were developed by the PCI Security Standards Council. This council includes representatives from dozens of credit card companies, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa. The purpose of these standards is to help facilitate

the broad adoption of consistent data security measures among merchants who store

data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

2. Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

3. Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

4. Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

5. Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

6. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security.

could lose their whole business over if they have a breach of security. Each credit card company (American Express, VISA, etc.) has its own penalties for a breach of security, but suffice it to say that a breach would be very expensive to the business in addition to requiring the business to notify all of their customers about the breach of security. Can you say "loss of trust"?

In addition to having internal knowledge of the compliance issues, every firm should have a ready answer for clients who seek help in becoming PCI DSS compliant. If the firm doesn't develop an in-house service to clients, then at least have a designated outside consultant to whom you can refer clients in need of help.

Here are a few ways to get more information about the requirements, along with some information about where to get trained to provide client services to help them ensure compliance with PCI DSS.

– The PCI Data Security Specification, authored by the PCI Security Standards Council is available on the council's website at www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

– The PCI Security Standards Council operates an in-depth program for security companies seeking to become Qualified Security Assessors (QSAs), and to be re-certified each year. In order to become a QSA, you must first be an employee of a Qualified Security Assessor company. So there are many requirements both you and your company must satisfy before providing client services that are recognized by the council. For more information about becoming a QSA, see www.pcisecuritystandards.org/qsa_asv/become_qsa.shtml.

PCI Compliance in QuickBooks

Every business using QuickBooks should at the very minimum perform the steps here to ensure basic compliance with PCI DSS with respect to storing credit card numbers

in QuickBooks. Keep in mind that these steps are just the QuickBooks part, so make

is enabled).

2. Ensure that all users of QuickBooks store customer credit cards ***only*** in the *Credit Card No.* field on the *Payment Info* tab of customer records.

3. Do not store sensitive authentication data such as card-validation codes (the three-digit number near the signature panel), personal identification numbers (PIN) or magnetic strip data.

4. Limit access to credit card data by assigning or removing permission for users to view full customer credit card numbers.

5. Set complex passwords and change them every 90 days for all users with access to credit card data.

6. Keep QuickBooks updated by turning on automatic updates. n

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.