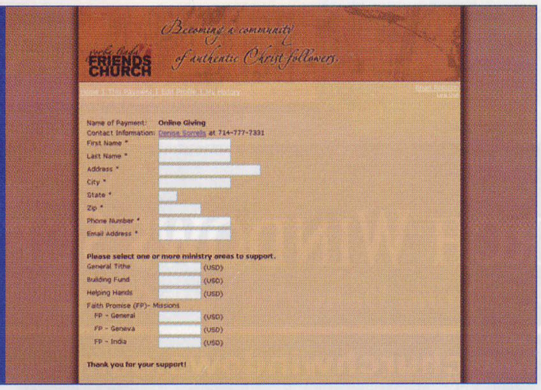
How PCI compliance will protect your congregants

Churches need to take necessary measures to avoid fraud when accepting online payments.

More churches and nonprofits are looking to their Web sites to raise funds and collect donations as well as do the work of processing registrations and payments for events, classes, Bible studies, VBS — you name it — all online. Some large churches develop custom applications to take payments online; others outsource the processes to online service providers. In either case, the church is responsible for ensuring that cardholder information is protected according to industry guidelines.

Security is a topic that seems to be at the forefront of thought for many organizations across multiple industries. With terror threats, physical threats and identity theft becoming real problems for many businesses, making sure your church complies with all security regulations is an important planning component that is often overlooked. For churches, the focus is typically on making sure that their children are protected, their buildings are monitored and volunteers have been appropriately screened.


ONLINE GIVING PAGE ON YORBA LINDA FRIENDS CHURCH WEB SITE

yorba linda FRIENDS CHURCH
Becoming a community of authentic Christ followers.

Name of Payment: Online Giving
Contact Information: Denise Sorrels at 714-777-7331
First Name *
Last Name *
Address *
City *
State *
Zip *
Phone Number *
Email Address *

Please select one or more ministry areas to support.
General Tithe (USD)
Building Fund (USD)
Helping Hands (USD)
Faith Promise (FP)- Missions
FP - General (USD)
FP - Geneva (USD)
FP - India (USD)

Thank you for your support!

For those churches that take any type of payments online — such as donations, event registrations, or tickets — putting security measures into place can be an even more important task due to increased risks of identity theft and fraud.

Protecting the information

According to a Better Business Bureau Survey this year, within the last 12 months, 8.9 million Americans were victims of identity theft. A study by CipherOptics found that 76 percent of data theft was due to hacking via the Internet. Nonprofits need to be especially concerned with protecting such information that would put their patrons at risk and compromise their organization's integrity and financial stability.

Often, churches and ministries aren't aware of the strict requirements placed upon those who process credit cards. It doesn't matter if an organization serves the for-profit market or the nonprofit market, the regulations set forth by Visa and MasterCard are the same: Organizations that process credit cards must comply with the security requirements set forth by the Payment Card Industry Data Security Standard.

What is PCI compliance?

So what is the Payment Card Industry Security Standard, or PCI, you might ask? It's a set of rigid guidelines meant to protect from security breaches where cardholders would be open to identity theft or payment fraud via stolen credit card and personal data.

The Payment Card Industry (PCI) Data Security Standard is a result of the collaboration between Visa USA, MasterCard, and other companies to establish universal security requirements within the industry to ensure that service providers and merchants employ the highest standard of information security to protect cardholder data.

Because the PCI Data Security Standard regulates the security and business processes of service providers and merchants that store, process, or transmit consumer credit card data, customers making payments through a PCI-compliant establishment can feel safe that their bank card account information will be secure under all circumstances.

New standards

In an effort to increase overall security, credit card companies imposed new standards this year to ease the growing concerns with impending identity theft and stolen cardholder information. Under the new PCI regulations, all merchants that accept credit cards are required to comply with requirements that call for the following security measures to be in place: (1) encrypted transmission of cardholder data, (2) periodic network scans, (3) logical and physical access controls and (4) activity monitoring and logging. The standard is intended to reduce fraud and identify security issues that could lead to the compromise of cardholder information (thewhir.com/features/king-pci.cfm).

To a church, these standards sound daunting to say the very least. On average, the process of undergoing PCI compliance can take one to two years at minimum and cost thousands of dollars to hire PCI specialists to set up technology that meets all requirements. It's just not feasible or logical for churches, ministries or other nonprofits to go through this process. However,

>>

By Lauren Hunter

given the risks from hacking and the liabilities for failing to comply with security regulations, churches cannot afford to simply ignore the issues.

That being said, there is hope. Instead of subjecting themselves to the rigors of PCI compliance, churches and nonprofits can choose to use a vendor that offers a PCI-compliant solution. As more service providers realize the need to comply with industry regulations, organizations that provide online payment services are becoming compliant so their clients don't have to.

Any service provider that stores, processes or transmits cardholder data as part of a payment transaction is defined by Visa to be a Level 1 service provider and must have their compliance validated. This includes an annual on-site PCI Data Security Assessment by a qualified data security company and ongoing network security scanning by a qualified independent scan vendor.

The list of PCI-compliant service providers is published by Visa USA at (visa.com/cisp). As of March 2008, ServiceU Corporation (ServiceU.com) is the only PCI-compliant Level 1 service provider that provides online giving services specifically to the church and nonprofit market.

Selecting a service provider

When evaluating online payment services, make sure that you can seamlessly integrate them with your existing Web site, including the ability to customize payment processing pages to look and feel like your Web site.

Also, look for a provider that accepts a variety of payment methods: credit cards, debit cards, checks, and even PayPal. Another area that is often overlooked is reporting: Make sure that the service provider's reports will enable your accounting staff to quickly and easily reconcile deposits to your bank account.

In addition, you'll want to evaluate whether or not it's best to go with an independent online giving provider or your church management software (CMS) provider. Many CMS companies are adding online giving services to the software they provide; while this can be convenient, it's important to ask questions about security and find out if their online giving solutions are indeed PCI-compliant. The benefits to implementing an online giving-only software solution include: industry compliant security (double check the provider), initial merchant account set-up, comprehensive and customizable reporting functionality, and targeted support for this area of your ministry.

By working with an online payments provider that is PCI-compliant, you can have peace of mind because your member's data is protected at the highest level and you are not liable to cover the cost of customer loss if there is a breach. Whether using a compliant service provider for online event registration, ticketing, or donations, your organization will experience the security that comes from using a payments processing partner that ensures proper compliance to avoid identity theft or fraud. CE

Lauren Hunter is a freelance writer in Roseville, CA. [laurenhunter.net]