Parish Electronic Giving Program – Best Practices

In 2010, only one in five payments will be made with a check. By the year 2014, experts suggest that the current checking system will be nearly obsolete. Yet, estimates are that at least 80% of the $9 Billion collected annually by the Church is still given through the envelope system supported by checks or donors writing checks to an annual appeal or capital campaign. The capability to accept electronic donations - whether through automatic bank debit or credit card - will be a requirement for any church organization's financial stability in the not too distant future. As the next natural step in the evolution of offertory and Church support, Dioceses and parishes should consider the following steps when implementing electronic giving. We believe these steps will help you be proactive and not reactive in establishing a successful electronic giving system.

The Leadership Roundtable's *Standards for Excellence* call for sound financial management, accurate financial records, internal control procedures, adequate liability insurance, and full conformance with canon and civil laws relating to fundraising and financial reporting. The checklist below identifies important considerations for parishes relating to best practices in the area of electronic giving.

Checklist

1. Security & Compliance

		Important Considerations
☑	Payment Card Industry (PCI) Compliant	The security standards imposed by the Payment Card Industry Security Standards Council are accepted by all major credit card companies and are required of all merchants (ie: parishes or organizations) that accept or store credit card information. (See full details below)
☑	Data Recovery Plan	In the event of a fire, or other catastrophic incident, does the parish or provider have an off site data system to maintain offertory collection for those enrolled?
☑	Data Security	Where are sensitive financial data and information (personal account numbers and credit card numbers) stored? Is financial information keyed at the parish? Are paper enrollments received for processing at the parish?
☑	Professional Liability & Crime Insurance	Are parish insurance requirements adequately addressed to cover potential liability issues?
☑	Privacy Policy	Does provider or parish have clear policy regarding privacy related issues?

2. Program Administration

		Important Considerations
☑	Marketing to Parishioners and Enrollment Responses	Is it incumbent upon the parish to introduce the electronic giving program to parishioners, provide enrollment materials, and handle enrollment responses? Successful enrollment is incumbent upon a coordinated marketing effort that inspires users to convert from envelope donors to electronic givers.
☑	Management of Secure Website Enrollment & Account Maintenance	Can parishioners enroll on line, and establish a secure on line account? Is the website enrollment application unique to the parish, or "generic" for the provider?

☑	Offertory, Second Collections, & Unique Appeals	Users will expect to give to all collections (offertory, diocesan collections, and unique appeals, ie: Capital Campaigns).
☑	ACH Debits (Checking & Savings) & Credit Cards (Visa, MasterCard, American Express)	Does the parish or provider offer both options? 50% of users give using credit cards highlighting the significance of PCI Compliance.

3. Fiscal Management

		Important Considerations
☑	Manage Debiting	Does the parish have to initiate the debiting process? What staffing is in place to facilitate?
☑	Manage Wire Transfers to Parish	How are funds received in parish bank account?
☑	Credit Card Expiration & Changes	Is parish responsible for contacting parishioners regarding needed updates to their credit card information?
☑	Monthly Reconciliation & Auditing	What auditing procedures and reporting are in place to monitor and reconcile electronic giving?

4. Program Fulfillment

		Important Considerations
☑	Personalized Offertory Cards to Replace Envelopes	The liturgy invites us to place something in the basket as a sign of support.
☑	Monthly Data Upload of Program Results	Does parish have to manually re-key on a monthly basis those parishioners using electronic giving for offertory and second collections?
☑	Year End Tax Statements	Changes in tax laws require parishioners to have documentation for their gifts. Tax statements should be available for all users.
☑	Dedicated Customer Service by Phone and email	How are the multiple phone and email inquiries managed?

What Parishes Should Know About Maintaining Financial Data

The following are guidelines parishes operating or considering implementation of a parish managed electronic giving program (using an in-house parish database electronic funds transfer application, bank, or transaction service) should adhere to.

What is PCI?
In response to further banking regulations, the Patriot Act, and multiple threats to the security of credit card information, the major credit card companies developed the Payment Card Industry Security Standards Council. The security standards imposed by this council are accepted by all major credit card companies and are required of all merchants (ie: parishes or organizations) that accept or store credit card information.

Does my organization have to be PCI compliant?
Any organization processing, storing, or transmitting credit card data must be PCI DSS (Payment Card Industry Data Security Standard) compliant. The processing, storing or transmission of credit card data is the physical or electronic storage or use of credit card information in either real time or recurring payments. The levels of compliance required change based on the amounts and types of transactions, but all organizations processing credit card information must adhere to the PCI DSS.

What aspects of a transaction based system administered by a parish should be scrutinized?
1. Physical storage of credit card information in office desks, filing cabinets, etc.
2. Any electronic storage of credit card information in internal database software and email.
3. Unencrypted transmission of credit card information through the internet.
4. The use any third party processing system with access to any other computers in an office.

What does maintaining PCI compliance mean?
Adhering to the PCI compliance standards can require costly changes to both technical and personnel infrastructures. The multifaceted approach implemented by the PCI DSS is important to protect the sensitive credit card information entrusted to your organization by your members. The requirements mandated by the PCI Security Standards include, but are not limited to:

1. Building and maintaining a secure network.
2. Protecting cardholder data.
3. Maintaining a vulnerability management program.
4. Implementing strong access control measures.
5. Regularly monitoring and testing networks.
6. Maintaining an information security policy.

What can happen if my parish does not maintain PCI compliance?
Organizations that do not adhere to the PCI DSS are exposing themselves to penalties of up to $500,000 and the inability to process gifts.

What does PCI compliance do for my parish?
An organization or vendor that is PCI compliant has had their infrastructure, personnel, and processes fully vetted and approved by a select number of accredited compliance auditors. Personal identity and credit protection are significant concerns for today's consumers, merchants (ie: parishes or organizations) and processors. By taking the steps necessary to protect cardholder information organizations not only provide a secure platform for receiving payments, but they provide a foundation upon which a successful credit card acceptance program can be built.

These best practices for electronic giving are provided by Brian Walsh of FaithDirect.net