Archdiocese of Baltimore Management In-Service

Electronic Payments

May 17, 2011

Agenda

1. Types of Electronic Payments

2. Why Use E-Payments?

3. Compliance Regarding E-Payments

4. Options

5. Controls For Secure Incoming E-Payments

6. Controls For Secure Outgoing E-Payments

7. Credit Card Controls

8. Additional Resources

9. Sources

Definition: An electronic payment is any kind of non-cash payment that doesn't involve a paper check.

Three Main Types:

1. One Time, Customer-to-Vendor

2. Recurring Customer-to-Vendor

3. Automatic Bill Payment (Bank-to-Vendor)

1. One Time, Customer-to-Vendor Payment

When a customer provides their credit card information online, submits their information to make a payment, and the payment is processed through the site.

Common Uses for Parishioners and School Families:

- To make a one-time pledge or donation to a capital campaign or annual fund online
- Contribute to a fundraiser (World's Finest Chocolate, Gift Wrap, etc)
- Make purchases (field trips, cafeteria meals, spirit wear, books, etc)

2. *Recurring Customer-to-Vendor Payment*

When parishioners or school families pay a regularly scheduled direct debit from their checking account or an automatic charge to their credit card that is deposited into the parish's or school's bank account

Common Uses for Parishes & Schools:

- Recurring Tuition Payments (FACTS , SMART, etc)

- Recurring Offertory (FaithDirect, PNC, ParishSOFT, etc)

- Recurring Pledge Payments

Example of a Recurring Customer-to-Vendor Payment Form

Authorization Agreement For Direct Payments (ACH Debits)

I (we) hereby authorize _____, hereinafter called COMPANY, to initiate debit entries to my (our) ❑ Checking Account (please attach a voided check) or to my (our) ❑ Savings Account (please attach a savings deposit slip) at the depository financial institution named below, hereinafter called DEPOSITORY.

I (we) acknowledge that the origination of ACH transactions to my (our) account must comply with the provisions of the U.S. law.

Preferred Payment Options: $_____ ___ Once a month on the 1st day of the month, OR

$_____ ___ Once a month on the 15th day of the month, OR

$_____ ___ Twice a month on the 1st and 15th day of the month

Depository Name _____

City _____ State _____

This authorization is to remain in full force and effect until COMPANY has received written notification from me (or ether of us) of its termination in such time and in such manner as to afford COMPANY and DEPOSITORY a reasonable opportunity to act on it. I understand that my financial institution may charge my account a $ fee for any insufficient funds (NSF) transactions.

Name(s) _____ ID (Envelope) Number _____

Date _____ Authorized Signature _____

3. Automatic Bill Payment (Bank-to-Vendor)

- Using the parish's or school's bank account to pay bills online and automatically
  - Examples can include payments for phone & internet bills.
- Parishioners and parents can set up automatic, online payments to their parish/school
    - The bank must offer a service called online bill pay.
    - Log on to the bank's Web site, enter the vendor's information and authorize the bank to electronically pay your bill.
    - In most cases, you can choose whether to do this manually for each billing cycle or have bills automatically paid on the same day each month.

Why Use Electronic Payments?

- **Convenience**
  - No check writing, swiping credit cards, or handling paper money
  - Online donations are available right away

- **Increase Likelihood of Consistent Donations**
  - Set up a recurring contribution for each month
  - Receive donations even during snow storms & vacation season
    - A study by the National Automated Clearing House (NACHA) revealed that consumers who use direct debit are more likely to donate on a regular basis.
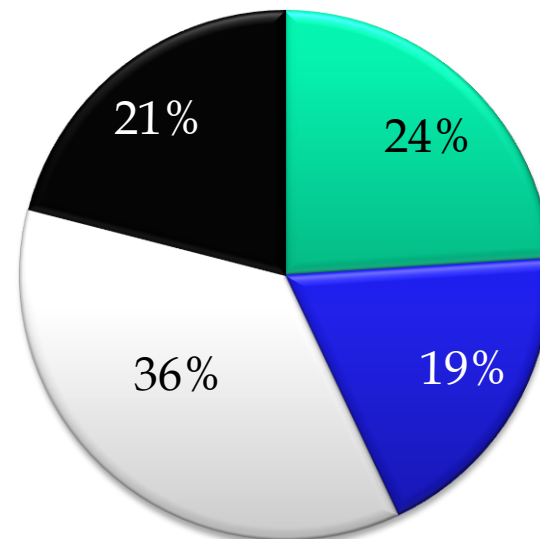
Trend in Distribution of Non-Cash Payments

2003

■ Check   ■ Credit Card
□ Debit Card   ■ ACH/EBT

- **Check: 46%**
- **Credit Card: 23%**
- **Debit Card: 19%**
- **ACH/EBT: 12%**
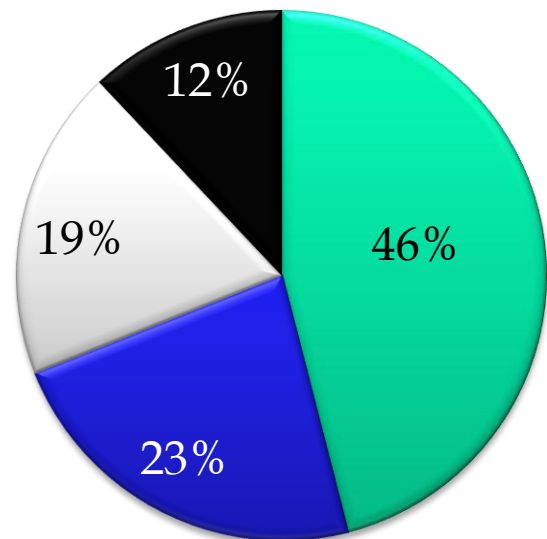
2009

■ Check   ■ Credit Card
□ Debit Card   ■ ACH/EBT

- **Check: 24%**
- **Credit Card: 19%**
- **Debit Card: 36%**
- **ACH/EBT: 21%**

- **Additionally, in 1995, 77% of all non-cash payments were made using checks and in 1979, 84% of all non-cash payments were checks.**

Statistics from the Federal Reserve 2010 Payment Study

- **Saves You $$ & Resources**
  - Lower costs related to purchasing paper, postage, printer ink, and other materials
  - More "Green"
    - A 2007 survey by Javelin Strategy and Research indicates that if all U.S. households received and paid their bills electronically, the United States would:
      - Save 16.5 million trees every year, providing enough lumber for 216,054 single-family homes
      - Reduce toxic air pollutants by 3.9 billion tons of carbon dioxide equivalents, the equivalent of taking 355,015 cars off the road
      - Reduce the solid waste generated each year by 1.6 billion pounds, the weight of 56,000 fully loaded garbage trucks

- **Improves Predictability of Cash Flow**
  - Scheduled, recurring transactions, resulting in more predictable income and accurate budgeting for your parishes and schools
- **Improves Delinquencies**
  - More likely to make sure that money exists
    - A study by the NACHA shows that for churches and nonprofits that rely on donations, fulfillment rates for pledges made by EFT averaged 98% versus 48% with mail-based monthly donor programs
- **Relieves some Segregation of Duties Issues**
  - Alleviates certain responsibilities involving funds
- **Security of Funds**
  - Less physical money being handled (counted & deposited).

Compliance Regarding Electronic Payments

- There are risks & concerns related to handling sensitive data such as credit & debit card numbers:

  - Do you write down and store card information?

  - Is the information safe and secure?

  - Where is the information being stored?

  - How long do you store the information?

  - Do you have a policy in place?

  - Who has access to the sensitive information?

Compliance Regarding Electronic Payments

Concerns regarding privacy & safety from identify theft lead to the formation of the **Payment Credit Industry** (PCI) **Data Security Standard** (DSS).

- These standards are relevant for credit card transactions as well as other types of electronic payments
  - While not governed by federal law, they require that even small organizations who process at lease 1 credit card transaction need to comply.
  - Fines and penalty decisions rest with credit card companies themselves
    - A single parish's or school's noncompliance can impact the whole Archdiocese's ability to process credit cards
  - There are 12 requirements (missing even 1 results in non compliance)

The 12 requirements address 6 overall compliance categories:

- Network Security

- Cardholder Data

- Vulnerability Management

- Access Control

- Monitoring & Testing

- Security Policy

Options

The least risky way to process credit cards:

- Hire a third party vendor to handle processing for your organization.
  - When Choosing a Vendor:
    - Check with your bank or software application provider to see if they can recommend a reputable provider

    - Make sure the processor is compliant with PCI DSS standards by obtaining a certification or letter indicating a compliance assessment

    - Check the Visa, MasterCard, and American Express listings of PCI compliant vendors

    - Ask the service provider for an AICPA Statement of Auditing Standards #70 **(SAS 70)** Report

List of Compliant Service Providers - All

SERVICE PROVIDER	VALIDATION DATE	SERVICES COVERED BY REVIEW (1)	ASSESSOR	AP	CEMEA	LAC	NA
1ShoppingCart.com	June 30, 2010	Other Payment Gateway	Security Metrics	☐	☐	☐	☑
1st Americard	March 31, 2011	Data Preparation Records Management	nGuard Inc.	☐	☐	☐	☑
1stPayGateway, LLC	May 31, 2010	Authorization Payment Gateway	Internet Security Systems (a wholly owned IBM company)	☐	☐	☐	☑
2checkout.com	February 28, 2011	Back Office Services Other	Arsenal Security Group	☐	☐	☐	☑
3dCart	March 31, 2011	Hosting Provider Payment Gateway	SecurityMetrics	☐	☐	☐	☑
3Delta Systems	September 30, 2010	Authorization MOTO Payment Processing Payment Gateway Process Magnetic-Stripe Transactions Switching	Fortrex Technologies	☐	☐	☐	☑

Options (cont.)

There are many third party vendors out there who can assist your parish or school in processing electronic payments, a few of those are:

- ParishSOFT Online Giving
- Faith Direct
- PNC Pinacle
- FACTS
- QuickBooks Merchant Services
- Blackbaud
- PayPal
- ProPay

Options (cont.)

- Even when using a third party service provider to process credit card information, your parish or school will still need to be PCI compliant
  - There are different levels of compliance
  - For your organization to become PCI compliant check first with your 3rd party service provider or with your bank for a recommended 3rd party assessor
    - Utilize a 3rd party assessor

BEST

      - Will identify weaknesses & noncompliance
      - Will identify what your parish or school needs to do to become compliant

    - If your organization does not store credit card information of any kind, it may be able to fill out a self-assessment questionnaire in order to gain compliance

Least Risky = Least Labor

-Do not use a 3rd party processor
-Process and store credit card information on site

-Use a com...
-Perform PCI compliance self-assessment
-Do not touch credit card information

-Use a compliant 3rd party processor
-Use a 3rd party assessor to issue your compliance
-Do not touch credit card information

Least Risky   **Most Risky**

Options (cont.) – Considering Costs

As the use of electronic payment methods is on the rise it is important to evaluate the pricing of different vendors

- Low initial costs may grow as your program grows and more members are using the vendor

Keep in mind other considerations that can aid in the decision making process:

- Start Up, Security, & Credit Card Processing Fees
  - How is the credit card being processed?
- Additional Costs for Communications and Reports
- Costs of Maintenance
- Charge Back Fees & Questioned Cost fees
- Frequency of Batches

Ability to grow your offertory

- Will an increase in cost equal an increase in revenue?

Controls for Secure Incoming E-Payments

- Lock up or destroy all sensitive information such as credit card data
  - Do not make copies of credit card information or send sensitive info through emails or via fax
  - Retention period should be no more than 1 year long
  - Shred data to destroy it; do not throw in trash
- Treat any electronic payment received just as you would any other cash receipt
  - Maintain support, segregate duties and limit access
- Review weekly or monthly statements, reconcile the statement to your bank account as part of your monthly close
  - Make sure that the amounts on the statement can be traced to your bank account and that the income is being properly recorded in the general ledger
  - Require review and approval by the pastor or principal

Controls for Secure Outgoing E-Payments

"What do you need to do to ensure that your outgoing information is safe?"

- Virus protection & firewall software
- Use a secure server
  - Easy signs of security:
    - "http**s**" vs. "http"
    - Lock and key symbol

- Ensure that vendors receiving payments have security features in place
- Do thorough research & don't provide sensitive information to unfamiliar sites

Additional Controls for Outgoing E-Payments

- Implement a policy for usage & process of e-payments

- Require written approval and review of support by the pastor/principal before the e-payment can be initiated
  - Initiators should be the same as the check signers

- Print out copies of confirmations of e-payments made and attach to supporting documents (emails, invoices, bills)

- Review e-payments during monthly bank reconciliation process

- When making an automatic e-payment, there is more risk in going through the vendor's site than through your bank
  - Your bank will never solicit personal banking information via email

Credit Card Controls

1. Who should be the users?

2. What are the policies and procedures?

3. What are the consequences for not having controls in place?

Who should be users?

1. The parishes and schools should limit the number of users as much as possible.

2. Access to cards should be limited to only the specific users.

3. All cards should have both the name of the parish/school and the individual's name on the card.

4. Credit limits should be maintained at a reasonable level, consider all types of limits your credit card issuer may provide, i.e. transaction limits, daily limits

What are the Policies & Procedures?

1. To protect the parish/school, each user must sign a policy form stating that they will not use their assigned cards for personal use.

2. Whether it's a gas card, store card, or a VISA/MasterCard, all users should be required to turn in receipts for all purchases, and be required to state the specific business purpose.

3. As with outgoing e-payments the pastor or principal should initial approval for any large purchases over a certain amount.

4. Receipts should be attached to all the statements. The parish/school must also ensure that every bill is paid in a timely manner to avoid late fees and finance charges.

1. If policies are not put in place, the parish/school will not be able to pursue legal action.

2. Without a policy, users could make personal purchases thinking they can reimburse the parish/school.

3. If the parish/school does not require the specific business purpose to be stated, there is an increased risk that personal purchases will be made and certain purchases will have to be added to taxable income.

Electronic Payments - Additional Resources

SUPPLEMENTAL INFORMATION, RESOURCES, AND CONTACTS

Table of Contents – Additional Resources

- Important Links
- Credit Card Policy Template
- Credit Card Voucher Template
- Information Security Policy Template
- Example of an Authorization Agreement With the Bank (from PNC)
- Vendor Information Slides
  - ParishSOFT Online Giving
  - Faith Direct
  - PNC Pinacle
  - QuickBooks Merchant Services
  - Blackbaud
  - PayPal
  - ProPay
  - FACTS

Important Links

- **PCI DSS website:**
  - https://www.pcisecuritystandards.org/security_standard/
- **MasterCard's Compliant Vendor Listing**
  - http://www.mastercard.com/us/sdp/assets/pdf/Compliant%20Service%20Providers%20-%20November%2029%202010.pdf
- **Visa's Compliant Vendor Listing**
  - http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf
- **PCI DSS Self-Assessment Questionnaire (PDF)**
  - https://www.pcisecuritystandards.org/security_standards/documents.php
    - **Scroll down to SAQ Instructions and Guidelines v2.0**

Credit Card Policy Template – General Policy: Credit Card Voucher

- Create a parish/school credit card voucher form which includes the following:
  - Must be used to account for budgeted expenses related to Parish Business such as supplies, ads, books etc.
    - Examples of items, which should NOT be reported/purchased by employees using the Credit Card include:
      - Personal Expenses   * Unbudgeted Capital Expenditures
      - Charitable and Political Contributions   * Any Item Not Considered Reasonable, Ordinary, and Necessary
  - Personal use of the Credit Card will not be allowed and account will be closed
  - Original receipts should be retained for items purchased in order to properly support all Credit card expenses.
    - The business purpose should be stated on all receipts.
  - A Credit Card Voucher form should be prepared monthly attaching receipts for each expense.
  - The pastor using the Credit Card Voucher form must approve all Credit card expenses
  - The Credit card has a set limit in order to reduce exposure to theft
  - Steps for filling out Credit card voucher:
    - Date of transaction , Vendor name, Description, Account and Amount
    - This should be supported by receipts or documented otherwise
  - Credit card voucher form should be signed by users

PROCUREMENT CARD VOUCHER				
Employee Name: *(Please print)*		Parish:		Date:
Date	**Vendor**	**Description**	**Account Code**	**Expense Amount**
		Total Procurement Expenses		

Approval
Signature

***Require employees to indicate in writing that they are aware of the policy**

1. Include an annual process that identifies threats & vulnerabilities, & results in a formal risk assessment

2. Include a review at least once a year and update if the business & risk environment changes

3. Develop daily operational security procedures (i.e. user account maintenance procedures, log review procedures, back up procedures, procedures for destroying information)

4. Develop usage policies for technologies such as modems & wireless and define proper uses of these technologies for all employees, contractors & guests.

    Ensure that you include in the policy:

    • Explicit approval requirements from management

    • Authentication for use of the technology

    • A list of devices and personnel with access

    • Labeling of devices with owner, contact info, and purpose

    • Acceptable uses of technology

    • Acceptable locations for technologies

    • Automatic disconnect of modem sessions after a certain inactive period

    • Activation of modems for vendors only when needed & immediate deactivation

    • When accessing cardholder data remotely via modem, prohibition of storage of data or cut & paste function

Information Security Policy Guide (cont.)

5. Ensure that responsibilities for all employees and contractors in regards to information security are clearly defined

6. Assign to an individual or team the following information security management responsibilities:

   - Establish, document, and distribute policies and procedures
   - Monitor & analyze security alerts and information and distribute to appropriate personnel
   - Establish, document, and distribute incident response and escalation procedures
   - Administer user accounts Monitor and control all access to data

7. Include that service providers used must adhere to the PCI DSS requirements and that certification must be obtained

8. Include to test the incident response plan annually & provide training

AUTHORIZATION AGREEMENT FOR DIRECT PAYMENTS (ACH DEBITS)

Company   Company

 Name _____   ID Number _____

I (we) hereby authorize _____, hereinafter called COMPANY, to initiate debit entries to my (our) Checking
Account / Savings Account (select one) indicated below at the depository financial institution names below,
hereafter called DEPOSITORY, and to debit the same to such account. I (we) acknowledge that the
origination of ACH transactions to my (our) account must comply with the provisions of U.S. law.

Depository Name _____ Branch _____ City _____ State _____
Zip _____ Routing Number _____ Account Number _____

The authorization is to remain in full force until COMPANY has received written notification from me (or either
of us) of its termination in such time and in such manner as to afford COMPANY and DEPOSITORY a
reasonable opportunity to act on it.

Name _____ ID Number _____ Date_____ Signature _____

**NOTE ALL DEBIT AUTHORIZATION <u>MUST</u> PROVIDE THAT THE RECEIVER MAY REVOKE THE
AUTHORIZATION ONLY BY NOTIFYING THE ORIGINATOR IN THE MANNOR SPECIFIED IN THE
ATHORIZATION.**

ParishSOFT Online Giving

Overview of Features:

- Self-Service, web-based & user friendly system

- Members are in charge of their personal online contributions

- Provides End-of-Year reports, giving histories, and many other customizable reports available online

- Multiple payment methods and funds can be set up as well as choices in frequency of giving (bi-weekly, monthly, quarterly)

- Inputs data directly into your ParishSOFT application

- Set up for electronic giving but can be useful for collecting tuition or other payments

ParishSOFT Online Giving (cont.)

Pricing:

- $200 One Time Set Up Fee

- $15/mo Maintenance Fee

- $.29/bank transaction

- $.31/credit card transaction + 2.6%
  - ($15/mo minimum transaction fees , so if there are 52 families participating it is covered)

- $10/transaction Rejection Fee (NSF, CC Rejection etc)

- Debits are processed through Sage (PCI Compliant)
- Parishes must be PCI Compliant and certified annually

Faith Direct

Overview of Features:

- Handles all the mailings and EFT transactions for your parish
- Shifts the responsibility (PCI Compliance)
- Handles all parishioner banking/credit card info.
- Multiple collections
- Price based on parish size, additional cost for credit card transactions
- A monthly deduction is the only option
- Results may vary, level of interest from parishioners

Pricing:

- Will vary based on:
  - Number of registered households & donating households
  - Current weekly and/or annual offertory
  - Number of envelops sent out/received back typically
  - Number of automated donors

- Email: mike@faithdirect.net for further information

PNC - Pinacle

Overview of Features:

- Base Package
  - 24/7 access to reports, statements & images
  - Unlimited real-time transfers between Pinacle accounts
  - Special reports and statements available
  - Check management
  - ACH Feature available at additional monthly fee

Pricing:

Base Fee:	$15.00 per month
PINACLE EXPRESS SELECT:	$10.00 per month (to use the ACH features)
Additional Fees:	$2.50 per return or NOC report
PINACLE Express:	$0.35 per transaction (only charged once)

QuickBooks – Merchant Services

Overview of Features:

- Credit Card Processing Online
- Process Credit Cards through QuickBooks
  - No extra software fees
  - No plug in fees
  - Includes mobile credit card processing feature
  - Point of Sales Credit Card Swipe Available

Pricing:

- No monthly charge
- No set up fee
- Fee per credit card transaction may vary

Blackbaud

Overview of Features:

- Electronic Funds Transfer module for accounts payable
- The EFT module can be used for fixed and variable automatic payment plans for student billing – "EFT Student Billing"
  - Statement setup, advance deposits, and multiple reports
  - Streamline billing process
  - Integrated with school's specific policies
- "The Financial Edge" has a built in interface with "The Raiser's Edge" a leading fundraising management system
  - Offers consulting and training services

Pricing:

- Varies based on number of students, number of users, & the system migrating from
- Contact: 1.800.443.9441 or email: solutions@blackbaud.com

PayPal

Overview of Features:

- Wide Range of Services Based on your needs
- PCI Compliant
- Secure Site with no monthly fees or credit checks
- **Merchant Account** for online payments and purchases:
  - Accepts credit card payments online/over the phone without payers having their own account
  - Invoices are generated and sent via email w/an easy "PayNow" Button
- Separate Services for **Non-Profits** to receive donations:
  - Easy Set Up & User Friendly

Pricing:

- Discounted Rates available for Non-Profits
  - Less than $100K monthly: Fee per transaction of 2.2% + $0.30   (Ex: $2.50 on a $100 contribution)

ProPay

Overview of Features:

- Payment solutions that include merchant accounts, payment processing, ACH services, pre-paid cards and other payment-related products.

- PCI Compliant

- End-to-end encryption and tokenization services

- *How It Works:*

  1. Enter your customer's credit card information using ProPay's website or a touch-tone phone

  2. Funds are deposited into your ProPay Account

  3. Spend your money or transfer it to a U.S. checking account

Pricing:

- Basic Annual Fee: $49.95

- Credit Card Fee: 3.5% + $0.35

- Transfer Fee: $0.35

FACTS Tuition Management

Overview of Features:

- Multiple payment options
- PCI Compliant
- Flexible payment dates
- Real-time interface to view statuses, download reports, & make changes
- Email reminders to parents
- Data integration

Pricing:

- Varies based on number of transactions, size of school, etc.

Sources

Conry-Murray, Andrew. "Laws for Organizations That Accept Online Payments." *TechSoup - The Technology Place for Non-Profits*. CompuMentor, 2 Sept. 2009. Web. 10 May 2011. <http://www.techsoup.org/learningcenter/webbuilding/page6432.cfm?rss=1>.

Denyer, Charles. "SAS 70 Audits and PCI DSS." *TechRepublic*. CBS Interactive, 19 May 2009. Web. 10 May 2011. <http://www.techrepublic.com/blog/tech-manager/sas-70-audits-and-pci-dss-four-critical-keys-for-cost-effective-compliance/1342#>.

Federal Reserve Banks. "Journey through the Payments Study: Check Changes through the Decade." *Federal Reserve Bank Services*. Federal Reserve System, Mar. 2011. Web. 10 May 2011. <http://www.frbservices.org/fedfocus/archive_general/general_0311_01.html>.

Federal Reserve Banks. "Nearly 80 Percent of Noncash Payments Are Now Electronic." *Federal Reserve Bank Services*. Federal Reserve System, Jan. 2011. Web. 10 May 2011. <http://www.frbservices.org/fedfocus/archive_general/general_0111_01.html>.

Sources

Federal Reserve System. "The 2010 Federal Reserve Payments Study." *Www.frbservices.org*. Federal Reserve System, 5 Apr. 2011. Web. 22 Apr. 2011. <http://www.frbservices.org/files/communications/pdf/press/2010_payments_study.pdf>.

"How PCI DSS Requirements Addressed with EFT Server." *GlobalSCAPE Support: Secure Information Exchange for the Enterprise*. GlobalSCAPE, 2008. Web. 10 May 2011. <http://help.globalscape.com/help/eft5/pci/toc_pci_dss_requirements.htm>.

"NACHA - The Electronic Payments Association - ACH Network Statistics." *NACHA - The Electronic Payments Association -*. NACHA, 2011. Web. 22 Apr. 2011. <http://www.nacha.org/c/ACHntwkstats.cfm>.

"Nonprofit Fundraising: Raise Money Online | Network for Good." *Network for Good | Online Giving Made Easy*. Network for Good, 2011. Web. 10 May 2011. <http://www1.networkforgood.org/for-nonprofits>.

Sources

PCI Security Standards Council, LLC. "Official Source of PCI DSS Data Security Standards Documents and Payment Card Compliance Guidelines." *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. PCI Security Standards Council, LLC, 2006-2011. Web. 10 May 2011. <https://www.pcisecuritystandards.org/security_standards/>.

"ProPay: How ProPay Works." *ProPay: Accept Credit Cards - Simple, Safe, & Affordable*. ProPay Inc., 2011. Web. 10 May 2011. <https://epay.propay.com/account/howpropayworks.aspx>.