Keeping Your Church’s Electronic Giving Safe

While thefts of physical offerings are tragic, usually only the cash is lost because it is so difficult for a thief to deposit checks made out to the church.

But with digital gifts, there is no challenge of converting checks to cash—it is as simple as redirecting the flow of the digital funds. This threat is now just as significant to churches as physical thefts or embezzlement, because of the increase of online giving. Church leaders tell me they are receiving 60 percent or more of their gifts digitally. Even small churches are jumping on the digital giving train. Gifts are flooding in through churches’ websites and other portals, as givers use debit and credit cards, ACH (Automated Clearing House) debits to their bank accounts, electronic checks, charges to their cellular accounts, and even virtual currency, using a variety of devices, including their computers, tablets, and smart phones as well as church giving kiosks.

While the threat of electronic theft is just as real as physical theft, the consequences can be even greater. A digital breach creates a double whammy, robbing the donor’s gift, and leaving them less likely to make future digital gifts because they’re reluctant to continue providing confidential credit card and bank account information to the church.

According to Vonna Laue, CPA and partner with Capin Crouse, “Digital giving can be beneficial to the church and provide stronger protections than other giving options if strong controls are in place.”

But without those protections in place, there is a greater potential for digital fraud than for fraud related to physical offerings. For a church receiving millions of dollars a year in digital gifts, a major loss can occur in a short period of time.

Changing landscape: understanding online giving

“As giving methods transition from checks and cash to electronic data transmissions, the methods necessary to ensure sound internal control must change as well,” says Michael E. Batts, CPA and managing partner of Batts Morrison Wales & Lee, P.A. He continues, “Internal controls in the electronic giving age are more sophisticated and are more systems-based. Churches that acknowledge this reality and actively address it can greatly reduce the risk of a breach that can sink confidence in their fiscal management.”

Knowing your tools

To understand how to prevent your church from online theft, you must first understand the basics of how electronic giving is set up. It’s a matter of understanding the three processes included in all e-giving setups, and the safeguards that go along with them.

1. Giving. Typically, the church collects credit card information and, depending on the way it’s designed, the bank account information through an online giving platform, such as GivingKiosk, PushPay, and SecureGive. Data security on the giving platform is essential. Look for the following to ensure your giving platform is secure:

   • SSL (Secure Sockets Layer) encryption, which establishes an encrypted link, allowing data to be transmitted securely between browsers and web servers (you’ll know if you see “https” in the web address instead of just “http”);
   • security card codes; and
   • address verification.

Nick Nicolaou, president of Ministry Business Services, also suggests looking for the lock in the browser URL address bar. “If it is solid, the security certificate is fully in force. If it is broken, there may be issues with the security certificate on the server.”

Multiple Options

While all churches offer multiple options for giving, donations are slightly higher in large churches that pass the plate than those who don’t.

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offer online giving</td>
<td>81%</td>
</tr>
<tr>
<td>Pass a collection plate</td>
<td>80%</td>
</tr>
<tr>
<td>Have donation boxes in the lobby</td>
<td>37%</td>
</tr>
<tr>
<td>Have an electronic kiosk in the lobby</td>
<td>25%</td>
</tr>
</tbody>
</table>

Used with permission from Leadership Network
2. **Payment processor.** The giving platform is in between the giver and the payment processor (also called the merchant account provider), which processes the gift and delivers it to the church’s financial institution. It is usually a third-party service using a system of computer processes to receive, verify, and accept or decline credit card transactions on behalf of the church through secure Internet connections.

3. **Giver management system.** While some giving platforms have the option of processing giving records, most churches host giving records on their own IT systems, which may or may not easily integrate with a giving platform.

**Potential weaknesses**

While these three steps do a great job of protecting the church from outside theft, the unfortunate truth is that many church thefts happen from the inside. Churches often trust staffers and volunteers to a fault, and fail to insist on sound controls over accounting systems. If internal controls of a church are weak in general, it is unlikely that controls over digital giving will be strong.

**Establishing strong internal controls for digital giving**

The following steps will help establish internal controls vital to securing digital giving:

- **Build a strong, multi-person payment processor relationship.**
  Digital giving involves interaction with at least one outside vendor—the payment processor. Who should have the initial and ongoing interaction with this, and other, vendors in the digital giving process? The natural tendency is to ask someone with information technology (IT) skills to handle it. You may involve IT staff, but someone in a top leadership position at the church must control the process.

  While one person must initially establish an account with each payment processor, multiple staff should verify the initial set-up, including a high-ranking church staffer. For example, the high-ranking church staffer should subsequently access the set-up information to verify the accuracy of the information.

- **Limit authorized changes to payment processor accounts.**
  After initially establishing a payment processor relationship, changes to the account routing number should be limited to high-ranking church staff, none of whom participate in the reconciliation of digital funds or have access to the giver management system.

  **Note:** This prevents any one person with access to change the routing of funds from the church’s account to a personal account without being caught. Without this system in place, the routing number could be changed to divert incoming funds from a church account to an employee’s personal account for just a few hours or a few days each month. The church is still receiving most of the digital gifts and may not notice the missing funds. If the payment processor does not notify the church of routing number changes or, if they send a notification and it goes to the person in control of making the change, who will know the funds have been diverted?

- **Set notifications to come any time changes are made to payment processor accounts.** Each payment processor should be requested to immediately notify a high-ranking church leader of any change to the bank routing information. If the processor will not commit to complying with this request, strong alternative controls should be used. For example, periodic surprise tests should be made of each payment processor account to ensure the appropriate bank routing information is being used.

- **Verify the payment processor has internal controls in place.** How do you evaluate the quality of the internal controls employed by your payment-processing vendor? Only by insisting it has a SSAE 16 Type 2 (also commonly referred to as a SOC 1 Type 2) report issued by an independent auditing firm covering its internal controls. The processor is undoubtedly PCI DSS-compliant—that’s required by law. But that isn’t enough. Insist on a SOC 1 Type 2 report with a favorable opinion regarding the organization’s internal control over processing of transactions.

- **Require regular payment processor transaction reports.** All payment processor transaction monthly reports should be received by a high-ranking church leader, in addition to a staff member more directly involved with the transactions. Use the reports to confirm the proper routing number was used.

- **Reconcile digital giving accounts regularly.** A high-ranking church official should begin each examination of digital gifts with the following reconciliations:
  - **Bank accounts to payment processor transaction reports.** This reconciliation ensures that all digital gifts were deposited in the appropriate bank account (digital gifts will be separately identified in the bank statements).
Proactive churches allow givers to access giving records online through a secure system and mail quarterly giving statements. These extra “eyes” on the data help ensure that gifts are properly posted to giving records.

- **Giving records to payment processor transaction reports.** This reconciliation verifies that all digital gifts are recorded in the giver management system (this is in addition to verifying that all non-digital gifts are recorded).

- **Giving records to bank accounts.** This reconciliation verifies that all digital gifts deposited into bank accounts are reflected in the giving records.

  **Important note:** Reconciling bank accounts with the giver management system is a good start. But who is doing the reconciliations? If the same person is in charge of the payment processor relationship and the giver management system, a negative entry—perhaps posted to the fraudster’s own giving account—will keep the giver management system in balance with the bank. That means the diversion of funds will go undetected. These duties must be separated.

**Limit access to giving systems.** Heighten security by limiting access to the giving platform, payment processors, and the giver management system.

While givers shouldn’t have access to the systems, the truth is, relatively few church givers can even access their giving records. Proactive churches allow givers to access giving records online through a secure system and mail quarterly giving statements. These extra “eyes” on the data help ensure that gifts are properly posted to giving records.

Rodney Ross, Giving Experience Director with LifeChurch.tv, says the church’s Giving Experience team reconciles the giving records to each payment processor on a weekly basis. The Finance team reconciles the giving records to the bank accounts monthly.

Ross explains, “Our Finance team members have read-only access to our payment processors and no access to the online giving platform. The Giving Experience team has read-only access to our online giving platform and no access to the bank accounts. Access to each system is limited, with a record of who did what, when, based on logins. Various permission levels also restrict what each individual is able to do within each system.”

**Conclusion**

When one or a few people control the giving platform, payment processor, and giver management system, the church has just invited fraud to come in and take a front row seat. Who interacts with your payment processor, designating the church’s financial institution and the specific account to which the payment processor will direct the funds? Does the payment processor confirm bank routing changes to the church, and, if so, who receives those notifications?

If a church has delegated responsibilities to two individuals, security is heightened, but the above fraud steps could still be accomplished simply by collusion between two people. As more people are added to the internal control matrix, collusion of additional people is required, reducing the risk of fraud.

Find the balance between trusting your staff and verifying their work. Help them understand that high accountability in the digital giving arrangement protects them and demonstrates sound stewardship of God’s resources. Establishing and maintaining God-honoring digital giving for your church is not for the weak at heart. It is hard work! But we must provide the necessary oversight to ensure proper stewardship over the resources God provides.

Dan Busby is a certified public accountant and the president of ECFA (Evangelical Council for Financial Accountability), an oversight and accreditation organization. He also serves as an editorial advisor for Church Finance Today.

**INTERNAL AUDITS MADE EASY**

10 CPA field-tested tips on working with auditors.

**By Marian V. Liautaud**

1. Determine if the audit is the best service for your church. Funds may be better spent on a financial review or some kind of consulting arrangement.

2. Develop a good relationship with your auditor. They should be a strategic business partner with a good knowledge of nonprofits and specifically ministries.

3. Be involved in major decisions within the church and determine the accounting implications of those decisions.

4. Have a monthly closing process to help with accurate accounting and audit preparation throughout the year.

5. Discuss the audit timing, issues, and requirements with your staff and keep them informed throughout the process.

6. Make any timelines and expectations that you have known to your auditors upfront.

7. Allow adequate preparation time and be ready at the start of fieldwork. Don’t plan to give the auditor a few things to start with and work on the rest while they are there. It takes them less time to audit items than it takes you to prepare and they will have follow-up questions during fieldwork that will interrupt your time.

8. Ask questions of your auditor throughout the process whenever you are unclear.

9. Be available during the fieldwork and for any necessary follow-up afterwards. If you are not available for questions (because of meetings or vacation time, for example), it will significantly slow the process.

10. Remember you hired the auditors and they really are there to help you!
Tax Calendar
Important Tax Deadlines in December 2014

In addition to the regular semimonthly and monthly withholding requirements, church treasurers should note the following tax deadlines for next month.

Monthly requirements
- If your church or organization reported withheld taxes of $50,000 or less during the most recent lookback period (for 2014 the lookback period is July 1, 2012, through June 30, 2013), then withheld payroll taxes are deposited monthly. Monthly deposits are due by the 15th day of the following month. Note, however, that if withheld taxes are less than $2,500 at the end of any calendar quarter (March 31, June 30, September 30, or December 31), the church need not deposit the taxes. Instead, it can pay the total withheld taxes directly to the IRS with its quarterly Form 941.

December 31, 2014
- Complete all year-end transactions to be sure that they are reportable on your income tax return.
- A church must make quarterly estimated tax payments if it expects an unrelated business income tax liability for the year to be $500 or more. Use IRS Form 990-W to figure your estimated taxes. Quarterly estimated tax payments of one-fourth of the total tax liability are due by April 15, June 15, September 15, and December 15, 2014 for churches on a calendar year basis. Deposit quarterly tax payments electronically using the EFTPS system.
- Church must designate a portion of each minister’s compensation as a housing allowance by December 31 in order for ministers who own or rent their homes to receive the full benefit of a housing allowance exclusion for calendar year 2015. The designation should be adopted during a regular or special meeting of the church board, and should be contained in the written minutes of the meeting. Churches also should designate a parsonage allowance for any minister who lives in a parsonage and who is expected to pay some of the expenses of maintaining the parsonage (e.g., utilities, furnishings, repairs, improvements, yard care).

FINANCIAL Q&A

By Vonna Laue
How do I get the staff to turn in more detailed expense reports?

By setting the tone at the top. If the tone by the senior pastor and the board is, “We’re going to do things right,” then that has a significant impact on the ministry. But if it’s, “Turning in receipts is not really important, what’s really important is ministry, and so we’ll do whatever we have to do to make ministry happen,” then that becomes a prevalent attitude in the organization. If staff doesn’t think it’s important to the pastor, and they don’t see a push from the board, they won’t find it important, either. If the pastor isn’t good about turning in his receipts with his expense report, guess what? The youth pastor and worship pastor and everybody else aren’t going to be good about it, either. So the tone at the top is important.

The goal is to help the board and the pastors see that it is all related—to teach them that yes, we need to have credit cards approved and expense reports turned in, and we need to have approval on purchases and the right people signing checks, because all of that ties into ministry. Part of the way we can show them this is by explaining, “If we misuse these dollars, then we don’t have dollars for the missions department, or we don’t have dollars to do this program or ministry that we want to do. And that’s why we want these things done right.”

Putting the minute financial details in the scope of a missonal mindset will help you get through to the board, the pastors, and the staff.

To submit a question for consideration in a future Q&A, e-mail CFEditor@ChristianityToday.com.