

Data Breach:

Responding to the Loss of Personally Identifying Information

by Eric Spacek, J.D., ARM, senior church risk manager at GuideOne Insurance

MORE THAN EVER BEFORE, churches are warehousing personally identifying information about their members and employees. With the advent of electronic giving, churches are storing members' bank account or credit card numbers, in addition to traditionally kept information, such as addresses and telephone numbers. Staff members' Social Security and drivers license numbers, and other personal information are stored among personnel files. Even unincorporated contractors performing work on church premises may supply a W-9 form that includes the individual's Social Security number.

At the same time, the risk of theft of personally identifying information is at an all-time high. According to the Federal Trade Commission, identity theft, the so-called "Crime of the 21st Century," has an estimated nine million American victims each year. Identity theft occurs when a criminal uses personally identifying information, such as a name, Social Security number, or bank account or credit card number, without permission, to commit fraud.

In fact, insurance companies have experienced a recent rise in the number of inquiries from churches that have experienced a security breach in which members' or employees' personal information was stolen or lost. For example, one church recently had a computer stolen that included all of its membership data. Another church's filing cabinet

containing employee personnel files was ransacked. Another church was robbed of its external hard drive that contained the church's giving records.

The question asked in these situations is almost always the same: Do we have an obligation to notify the people whose personal information was taken about what has happened?

The response to that question involves both legal and moral considerations. This article addresses the former, while the latter is left to the sound judgment of church leaders, considering the circumstances of the loss and always keeping the Golden Rule in mind.

RESPONDING TO STOLEN OR LOST PERSONALLY IDENTIFYING INFORMATION

As of November 2007, 39 states have enacted notification laws on security breaches involving personally identifying information. This is a fast-moving area of the law. While just four years ago there were no such laws on the books, consumer advocates anticipate that in the near future, every state will have enacted some form

of security breach notification legislation. Although security breach notification is part of federal regulations affecting financial institutions and the healthcare industry, there is currently no federal security breach notification requirement for nonprofits, such as churches. Several measures have been introduced in Congress, although it is difficult to predict when or if Congress may act on this topic.

State laws vary considerably, but many are based on California's first-in-the-nation model enacted in 2003. Common considerations in these laws include

1. **Organizations that must notify**—Some state laws apply the notification requirement only to state agencies, while the majority of states apply it to all organizations, including nonprofits, that are doing business in the state. Typically, there is no exemption for religious organizations. You will need to check with an attorney in your state to determine if the law applies to your church. A summary of state laws is available from the Consumers Union at www.consumersunion.org/campaigns/Breach_laws_May05.pdf.

The question asked in these [security breach] situations is almost always the same: Do we have an obligation to notify the people whose personal information was taken about what has happened?

2. **Computerized data**—Most of the statutes specify that only the loss of computerized personal information triggers a notification obligation. Thus, strange as it may seem, theft of a hard (paper) copy of someone's personal information may not technically require your church to notify the individual, but theft of the same data in an electronic format may require notification.

3. **Unencrypted data**—Most statutes specify that the notification requirement is triggered only when the data stolen is unencrypted or un-redacted. In other words, if the data is encrypted, notification is not required under those statutes. Encryption programs are relatively inexpensive and should be considered as a precaution to protect stored personally identifying information.

4. **"Name plus"**—Most statutes require that something more than a person's name be taken before notification is required. Usually, it must be a name plus either Social Security number, date of birth, bank account number, driver's license number, account password information, or credit card number.

5. **Likelihood of harm**—In about half of the states, mere loss of the data triggers the notification requirement, but in the other half, notification is only required if harm is likely. Typically, the wording in these "risk-based" statutes requires notification only if illegal use or misuse of the information has occurred or is likely to occur; thus, if there is no material risk of identity theft or fraud, no notification is required. What is contemplated here is the situation where theft of personal information does not appear to be the target but, instead, is incidental to other criminal activity, such as theft of cash or other valuables. The interpretation of these risk-based provisions is a challenging one and should be made only in consultation with the church's attorney and law enforcement authorities.

While these are the considerations under state laws, they also are relevant for churches when deciding whether to notify individuals about stolen information even if state law does not require it. For example, if the theft of personal information appeared to be merely incidental to theft of monies or other valuables at the church, your church may, in consultation with local law enforcement and its counsel, determine that personal information is not likely to be used, and thus, no notification is indicated. On the other hand, if the loss of data involved hacking into the church's financial computer system, notification is probably the best judgment.

When there is a data breach involving the loss of personally identifying information, the Federal Trade Commission (FTC) suggests that businesses consider notifying

law enforcement authorities as well as notifying other affected businesses, such as credit card issuers, banks, or even the credit bureaus. We might add that churches affected by a data breach also should consult with their attorney and notify their insurance company.

If, in consultation with counsel, a decision is made to notify affected individuals whose personally identifying information has been compromised, the California Office of Privacy Protection suggests that the notice contain the following content:

- A general description of what happened;
- The type of personal information that was involved (SSN, DOB, etc.);
- What you have done to protect the information from further loss;

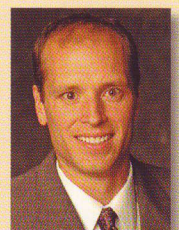
Summary

- The risk of theft of personally identifying information is at an all-time high. The number of churches which have experienced a security breach has risen. This article addresses the issue of what obligation churches have to notify members when there has been a security breach.
- State laws vary, but there are some common considerations:
 - Most states require notification requirements to all organizations.
 - Most statutes specify that only the loss of computerized personal information triggers a notification obligation.
 - Most statutes require notification when the stolen data is unencrypted or un-redacted.
 - Most statutes require notification only when more than a person's name has been stolen.
 - About half of the states require notification only if harm is likely, if illegal use or misuse of the information has occurred, or is likely to occur.

- In addition to these legal considerations, churches may want to evaluate the likely cause of the theft before notification in the decision whether or not to notify people at risk. Additionally, when there is a data breach, the Federal Trade Commission suggests notification of law enforcement authorities as well as other affected businesses.
- This article includes information on the content of the notification. The FTC provides a model letter to send to individuals whose personally identifying information has been lost or stolen.
- Having a thorough understanding of your state's security breach notification requirements will better prepare your church to respond to this scenario.

Author


Eric Spacek, J.D., ARM, is senior church risk manager at GuideOne Insurance. He can be reached at espacek@guideone.com.



- What your organization will do to assist affected individuals, including a designated contact person for assistance;²
- Information on what individuals can do to protect themselves from identity theft, including contact information for the three credit reporting agencies, and
- Contact information for the FTC (www.consumer.gov/idtheft) and your state's office of consumer affairs.

The FTC provides a model letter for businesses to send to individuals whose personally identifying information has been lost or stolen. This sample letter is available at www.ftc.gov/bcp/edu/microsites/idtheft/downloads/model-letter.doc.

BE PREPARED TO HANDLE DATA BREACH SITUATIONS

A church experiencing theft or an incident of computer hacking is troubling enough, but the situation is compounded when personal information is lost and members of the church community are placed at risk of having their identities stolen. By having a thorough understanding of your state's security breach notification requirements and guided by competent counsel and prayerful consideration of all the circumstances, your church will be better prepared to respond to this most unfortunate, but increasingly common, scenario. 

¹ Such assistance can take several forms including offering to pay for credit-monitoring services for affected individuals for a period of time or providing information about how individuals can place either a "fraud alert" or "security freeze" on their credit report.

Announcing a New Graduate Program for Parish Managers

MASTER OF SCIENCE IN COMMUNITY LEADERSHIP CONCENTRATION IN PARISH MANAGEMENT

To combat the significant growth in workload and daily demands, and to maximize the time priests spend ministering to their parishioners, lay persons are being employed in ever-increasing numbers to assume administrative responsibility for parish operations.

Effectively managing these activities requires organization and leadership skills specific to the context of religious institutions. The new online MS in Community Leadership – Concentration in Parish Management has been designed to meet these needs.

Courses in this online, 36-credit graduate program include:

- *Parish Financial Stewardship*
- *Community Service*
- *Parish Marketing and Fund-Raising*
- *Leadership Effectiveness*

Now accepting applications.



**DUQUESNE
UNIVERSITY**

SCHOOL OF LEADERSHIP AND
PROFESSIONAL ADVANCEMENT

800.283.3853

www.leadership.duq.edu/church