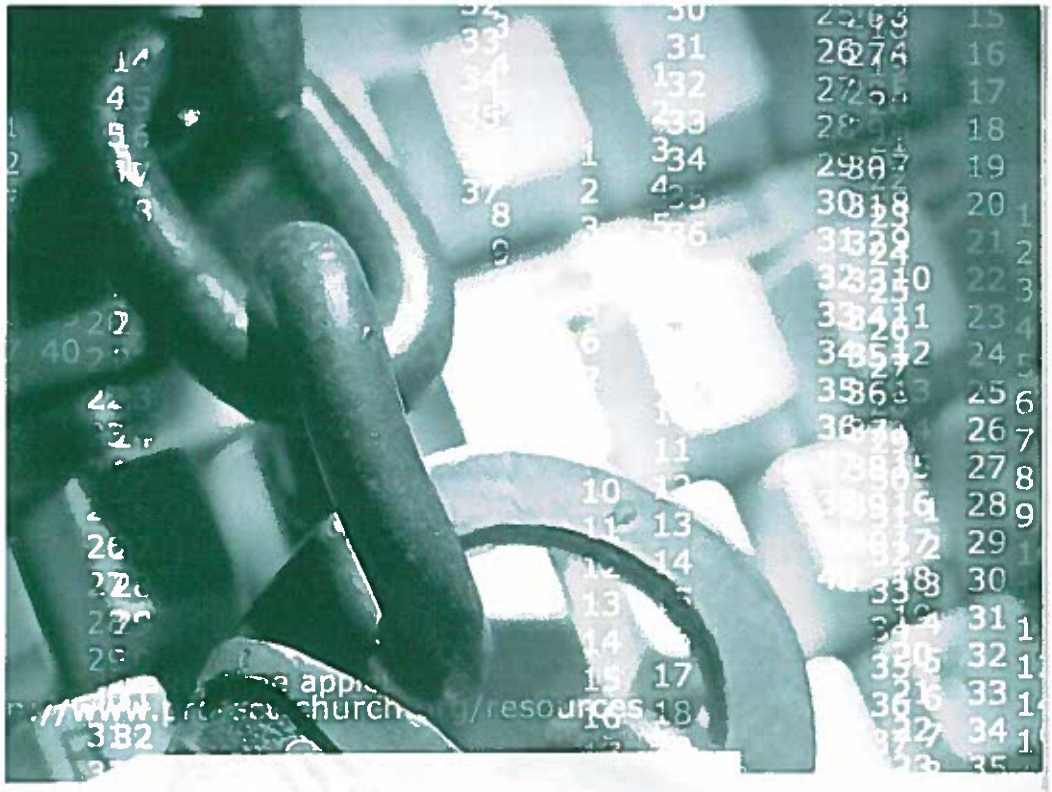


Forty Ways your Church and Church Staff can Help

PROTECT

their Finances from Identity Theft

Keith T. Hamilton, D. Ed. Min., CFP®
Church Financial Services
Georgia Baptist Convention

Identity theft is out of control. Most of us will be subject to identity theft during our lifetime.

Listed below are forty ways you can help to reduce the chances of the church's and your identity being stolen. However, a proven method does not exist that will totally eliminate the risk of identity theft happening to you.

On the other hand, there is one type of identity theft you can absolutely avoid. In the Bible, believers in Christ's identity will be written in the Book of Life. One day, God will read from the Book of Life to see if your identity is present. You can make sure your identity is present in the Book of Life by accepting God's offer of protection through trusting in His Son, Jesus Christ, for your protection and salvation. Only God offers true protection from the greatest challenge to your identity theft from eternal life. Avoid this type of identity theft at all cost by accepting Jesus Christ as your personal Savior.

#1

Use a gel pen like Uni-Ball to write personal checks. Gel pens are difficult for someone to erase the ink and change the check amount.

#2

Open your bank statement immediately and scan the bank statement for any unusual charges or checks cleared that you did not write or endorse.

#3

Balance your checking account within three days of receiving your bank statement so your bank can be alerted to identity theft if that has occurred.

#4

Register your telephone numbers on the national no-call list to stop telemarketing calls. http://donotcall.gov Telemarketing calls should not be answered or responded to so you can avoid giving personal information that might be misused later.

#5

When charging a meal at a restaurant, always fill in the tip line with a dollar amount even if the amount is zero. Also, total the amount of the bill on the charge slip. Always put a dash before and after a dollar amount entered to prevent someone from changing the amount of money you entered.
Example: -$7.25- or -0-

#6

Always shred unsolicited and unwanted credit card applications before placing the applications in the trash. (Shredding helps prevent identity theft.)

#7

Always save credit card receipts to compare the charges on your credit card statement. If a charge exists that you do not have a receipt or do not remember making, protest the charge by calling the credit card company and putting the protest in writing. Make sure to make reference to your phone call in your written correspondence to the credit card company.

#8

If you are a victim of credit card fraud, then call the credit card company immediately. Make sure you follow up with a registered business return reply to the credit card company.

#9

When writing personal checks, fill blank spaces before and after dollar amounts with dashes. For instance: –22.00– and --------Twenty-two and no/100------.

#10

Avoid using debit or check cashing cards since these cards do not have as much protection as credit cards. Some retailers do not require the use of a PIN number on debit and check cashing cards. Your checking account might be cleared out before you realize your money has been stolen. Even though your liability limit from the stolen money is small, replacing the stolen money could take months before it is restored to your checking account.

#11

Keep old bank statements and tax returns permanently to provide a record of your positive credit history. Do not throw away any receipts or invoices for three years to avoid any unfounded questions about paid bills.

#12

Do not use passwords that contain familiar personal information like phone numbers, Social Security numbers, family names, or pet names. Develop a three level security password system that utilizes different security level passwords. For instance, the high-security level password would only be used for banking and other personal financial purposes while the low-level security password would be used for services that do not involve personal or banking information. The medium-level security password would be used for credit card purchases not involving other personal information like birthdates and addresses.

#13

Resist giving out your Social Security number to anyone except for retirement purposes. This might not be entirely possible, but at least ask if not giving your Social Security number is possible.

#14

Check your credit report on an annual basis. A credit report is available by contacting consumer credit-reporting agencies: TransUnion, Experian, Equifax, and INNOVIS.

#15

Call 1.888.567.8688 to stop unwanted selling of your name and credit history from consumer credit reporting companies to mass marketing companies.

#16

Keep your receipts from ATM deposits and withdrawals. Do not throw away the receipts for three years to prove a deposit or withdrawal history in the case of identity theft. Be aware of your surroundings at an ATM to make sure other individuals are not watching you enter your password. Also, try to use the same ATM for most of your transactions. If something is different, unusual, or improper about the teller machine, you might be alerted that someone has altered "your" ATM to steal your password by adding electronic storage devices.

#17

Do not mail your bills by placing them in outside mailboxes at home, work, or post office. Raiding mailboxes is a common practice of identity thieves.

#18

Never buy anything on the Internet without first making sure the web site is secure and hacker-safe.

#19

Immediately, scan your credit card statement for any unusual charges.

#20

Never give personal information nor confirm personal information over the telephone or through the mail service to an unsolicited individual or company without you first contacting the company to make sure the solicitation is legitimate.

#21

Never respond to an email request for personal information even if the request seems legitimate.

#22

Never send your Social Security number or your date of birth through an email.

#23

As much as possible, opt out from allowing companies to sell your personal information to "family" financial companies within the parent company or outside companies.

#24

Possess only two major credit cards to limit your exposure to identity theft.

#25

Use the on-line bill pay available from your local bank to pay the majority of your bills not charged to your credit card. On-line bill pay reduces your chances of thieves stealing personal information from your personal checks.

#26

Use a credit card instead of writing a check. A credit card has more protection features than personal checks. (Of course, you should pay off the credit card balance each month.)

#27

If possible, do not let a retailer store your credit card or banking information on-line. It might take you more time and effort to enter the information manually every time you purchase from a retailer, but your risk of identity theft will be reduced.

#28

Destroy the hard drive from your old computer before disposing of the computer. Even if the old hard drive has been reformatted, a computer expert can recover your personal information.

#29

Purchase firewall protection, spam blocker, spyware protection, pop-up blocker, and virus protection software for your home and office computers. Real-time software is needed for adequate protection.

#30

Periodically, glance at your checkbook to make sure a check is not missing.

#31

If you have been a victim of identity theft, contact the credit reporting agencies to place a fraud alert on your credit report.

#32

Avoid offers that seem to be too good to be true. They usually are!

#33

Do not pre-print your driver's license number, Social Security number, or date of birth on your checks.

#34

Never sign a blank check for someone to fill in the dollar amount later.

#35

Resist opening "retail" store credit cards. The more credit cards in your possession, the more likely you will be subject to identity theft.

#36

Avoid applying for unsolicited credit cards over the telephone, Internet, or mail. For instance, credit card offers made over the telephone are rarely as good as the credit card terms will later reveal.

#37

Avoid automatic payment withdrawals from your banking account. You are giving a business or person access into your personal finances through automatic payment withdrawals. While the business might be legitimate, a possible hacker into the business system might not be as trustworthy. Limit your exposure by instead using on-line bill pay you control through your local bank.

#38

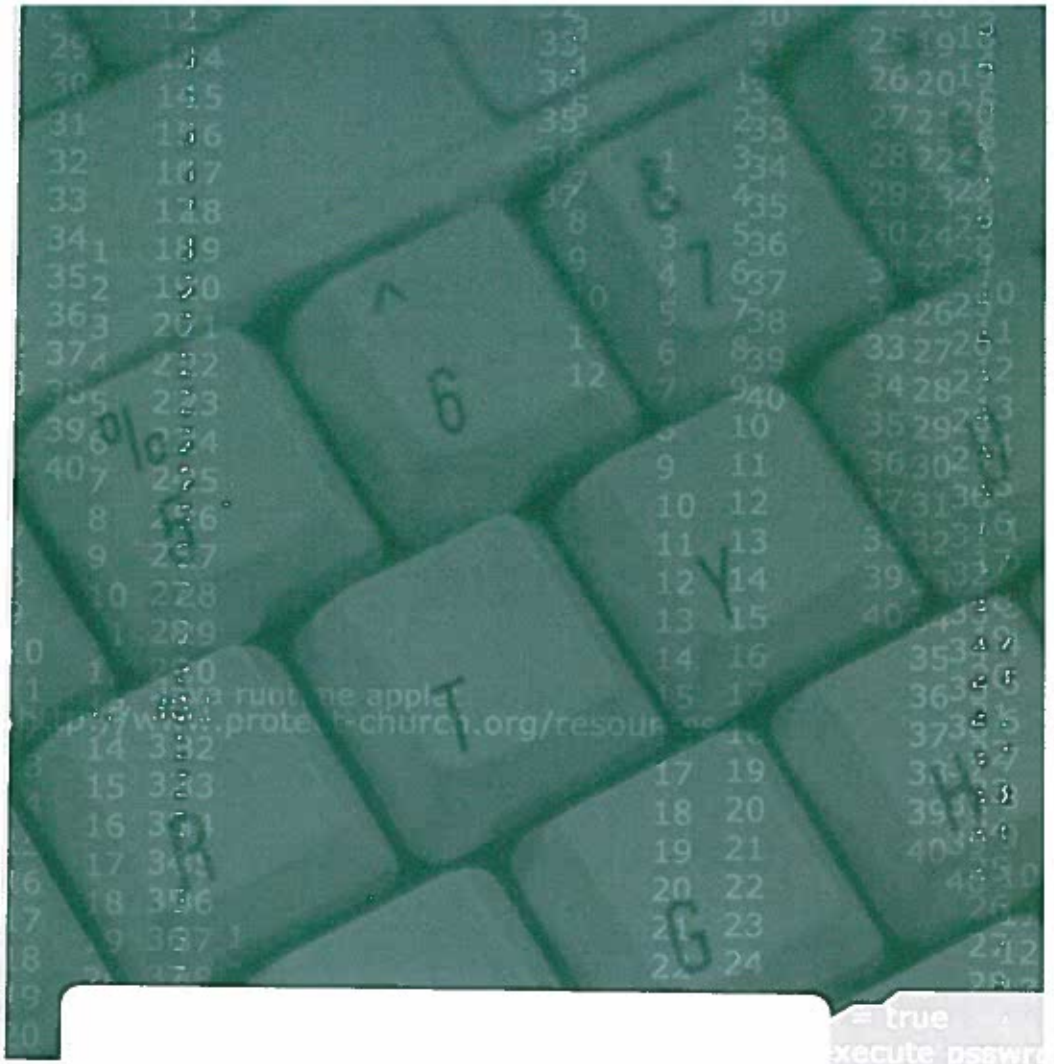
If possible, bank at a local bank that knows your name and banking reputation. In the case of identity theft, you should be able to resolve the matter faster and easier.

#39

Avoid filling out your Social Security number and date of birth as much as possible on applications. This might not be entirely possible, but limit this information as much as possible to reduce your exposure. Talk to your employer about the security of your resume and job applications.

#40

Do not carry your or other family member's Social Security numbers or birthdates in your wallet or pocket book. If stolen, the thieves will have access to most of your personal financial information.



CHURCH FINANCIAL SERVICES

Church Financial Services
Georgia Baptist Missions and
Ministry Center
6405 Sugarloaf Parkway
Duluth, Georgia 30097-4092

800.746.4422 or 770.936.5295

www.churchfinancialservices.org