Frank Abagnale’s Tips for Protecting Your Credit

World-renowned identity theft expert and subject of the blockbuster motion picture and Broadway play *Catch Me If You Can*.  

Frank W. Abagnale

PrivacyGuard®
Don’t be caught off-guard
When it Comes to Your Credit, Listen Carefully…

There are two phrases you never want to hear: Identity Theft and Credit Fraud.

Why? Because it means there’s been unauthorized use of your personal information to commit fraud. And the worst part is, you might not know about it until a great deal of damage has been done to your credit and your identity.

With the advanced technology used by many identity thieves today, it could be months before you realize you’ve become a victim of identity theft or credit fraud.

It doesn’t matter what personal information a criminal might use (Social Security number, credit card data), the damage can be devastating because many companies often check your credit score and credit history to make the following decisions…

**Lenders** – Accept or deny you credit and set interest rates.

**Credit Card Companies** – Accept or deny you a credit card.

**Home and Auto Insurers** – Accept or deny you insurance and set your rate.

**Landlords** – Accept or deny you a residence.

And the list continues… with employers, utility companies, government agencies, and other businesses that use your financial history as a gauge of your creditworthiness.
To keep a step ahead of credit problems that can be caused by criminals, it’s crucial to keep a constant eye on your credit – managing your personal files and information so that you’ll know if your credit might be compromised in any way.

Fortunately, you have PrivacyGuard® to help take a lot of the burden off your shoulders. With access to your triple-bureau credit reports1, 24/7 credit monitoring2, and internet surveillance of your personal information, PrivacyGuard lets you know who might be looking at your credit and if your personal information might be compromised. However, there are still some things you need to do in order to keep your credit safe from criminals. (See Page 19: Frank’s Top Ten Tips to Help Prevent Identity Theft.)

We’ve created this guide for you to use along with your PrivacyGuard benefits. It’s the perfect way to make sure you’re always helping to protect your credit, your identity, and your life.

---

1,2 Please see page 31 for details.
### Table of Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take a Look in the Mirror</td>
<td>5</td>
</tr>
<tr>
<td>Expert Advice from the Original Expert</td>
<td>6</td>
</tr>
<tr>
<td>Let’s Talk About You</td>
<td>8</td>
</tr>
<tr>
<td>What and Who – The Factors That Make Up Identity Theft</td>
<td>10</td>
</tr>
<tr>
<td>Stolen Data – How Thieves Like to Use Your Information</td>
<td>12</td>
</tr>
<tr>
<td>Time for a Credit Check</td>
<td>14</td>
</tr>
<tr>
<td>“I’m a Victim! Now What?”</td>
<td>16</td>
</tr>
<tr>
<td>Help is Just a Phone Call (or Mouse Click) Away!</td>
<td>18</td>
</tr>
<tr>
<td>Frank’s Top 10 Tips to Help Prevent Identity Theft</td>
<td>19</td>
</tr>
<tr>
<td>Extra Protection for You and Your Credit</td>
<td>30</td>
</tr>
</tbody>
</table>
Take a Look in the Mirror

When you look in the mirror, you know who you are, right? You’re you and no one can take that away from you. Or can they?

When a criminal uses your personal information to open a credit card account, the bank thinks you opened the account. So when bills for this account don’t get paid, they think you are in default. When it comes to creditors, your credit is your identity. And when your good name and good credit have been compromised, you need to start the process of proving who you really are.

The number of ways an identity thief can access personal information is almost unlimited. They can get your information from...

- Stealing a Wallet or Purse
- Going Through Your Trash
- Hacking into Online Credit Card Data Banks
- Swiping Bills or Statements from Your Mailbox
- Stealing Credit/Debit Information from ATMs

It’s Time to Fight Back!

As an identity theft victim, it’s bad enough that someone has stolen your identity and you have to clean up the mess. But with your credit now at stake, you could be denied a mortgage, a loan, an apartment… even a job.

However, by using the tips in this guide and taking full advantage of your PrivacyGuard benefits, you can put your mind at ease knowing that you’re now fighting back against these criminals.

The Most Common Ways Criminals Access Personal Information

- Lost or stolen wallets, 42%
- While conducting an ATM transaction, 19%
- “Friendly” theft, 13% (Family, friends or co-workers)
- Stolen paper mail, 3%
- Online, 11%
- Data breach, 11%
- Other, 1%

Please see page 31 for details.
The easiest way to stop identity theft for good? Have consumers follow just a few simple rules. It’s that easy! – Frank Abagnale
Some additional “Frank Facts”

There are countless reasons why we’ve partnered with Frank Abagnale to create Tips for Protecting Your Credit. He has insight and knowledge that comes not only from experience, but also from his commitment to putting an end to fraud. Along the road to fulfilling this commitment, he has added to his already long list of accomplishments:

- Author of four books: *Catch Me If You Can*, *The Art of the Steal*, *The Real U Guide to Identity Theft*, and *Stealing Your Life*.
- Designed the SuperCheck®, which is considered to be one of the world’s most secure checks.
- Helped build identity management software currently used by thousands of corporations, governments, and financial institutions.
- Advisor to 41st Parameter on development of ImageMask™, software that digitally blocks check and document information from being seen online.
- Facilitated in the development of PrivacyGuard, which has helped protect the credit of millions of people for over 19 years.
Let’s Talk About You

Most people don’t think they’ll ever become a victim of identity theft or credit fraud. They feel it will always happen to “the other guy”… that their credit and identity are immune to theft.

Unfortunately, identity thieves don’t have a preference for the age, race, sex, income or geographic location of their victims. If your personal information somehow makes itself available to a criminal, it’s up for grabs and you might be the last to know it’s been stolen.

So let’s talk about you for a minute… or two. Have you taken steps to protect your identity? Do you place your personal information in potentially compromising positions? Are you sure that your identity and credit have not been compromised?

IDENTITY FRAUD AFFECTED OVER 8 million CONSUMERS LAST YEAR

To better answer these questions, we’ve designed a short Risk Assessment to help you determine if you might be at risk of becoming an identity theft victim. It’s very important to the safety and security of your name and your credit.

4 Please see page 31 for details.
Are You At Risk?

Place a check mark next to all that apply to you.

- I DO have both anti virus and firewall protection on my computer.
- I DO NOT share my vacation or personal plans with “friends” on social networking sites.
- I DO use a micro-precision shredder on all of my financial documents before disposing of them.
- I DO NOT carry my Social Security card in my wallet.
- I DO NOT write my Social Security number on my checks.
- I DO shred all pre-approved ”credit offers” I receive via mail before throwing them out.
- I DO check the validity of site certificates when sending sensitive information over the Internet.
- I DO NOT leave my mail for pickup in an unlocked location.
- I DO check my credit report at least once every three months.
- I DO NOT show my full birthdate on social networking sites.
- I DO NOT give out my Social Security number to anyone who asks for it.
- I DO cover the keypad when making transactions at an ATM.
- I DO NOT keep personal information (e.g. Social Security number, financial account numbers, etc.) on a computer that is connected to the Internet.
- I DO check my computer weekly for security updates and/or use automatic updates.

How many of the above statements did you check? According to Frank Abagnale, the fewer check marks you placed above, the more vulnerable you are to identity theft.

If you’re unsure how to further protect your information, see Page 19 for Frank’s Top 10 Tips.
What and Who – The Factors That Make Up Identity Theft

There are two factors that are always present in the identity theft process: sensitive information and an identity thief. Without one, the other doesn’t exist.

FACTOR #1: The Sensitive Information
Sensitive personal data can be found on the Internet, in a trash bin, in an unprotected mailbox, in a stolen or lost wallet... and that’s just the start. And when identity thieves are involved, it doesn’t matter how or where they gain access to information. Their minds are on one thing: using or selling the information for their own gain.

FACTOR #2: The Identity Thief
Who would do such a thing? Who would steal someone else’s personal information? Simply stated, identity thieves have one thing in common: they don’t care whose information they steal, as long as they can make a profit from it.

CAUTION!! It appears that “friendly fraud” is on the rise. 13% of fraud victims discover that family, friends, or co-workers are stealing their identities, and the number is growing every year.

When it Comes to Identity Theft, All Ages are NOT Created Equal.

Age 18-24 25-34 35-44 45-54 55-64 65+
Your PrivacyGuard Solution: Credit Monitoring

As a PrivacyGuard member, you can rest assured that your credit is being monitored 24/7/365 at the three major credit reporting agencies. Through our Credit Monitoring feature, alerts will be sent to you should certain important information be changed in your credit file. You can also choose to receive these alerts via e-mail or SMS text message.²

If you make it easy for people to steal from you, chances are someone will. – Frank Abagnale
The majority of stolen personal information is used to open new accounts. These account types include checking and savings, mobile phone, loan, credit card, e-mail payment, and Internet accounts.

Most other data misuse is through a victim's existing card or non-card accounts. Unfortunately, all it takes is a small bit of information for a criminal to open a new account in your name.

If you take a look at the chart to the right, you can see the frequency thieves steal the information they need to open new accounts or misuse existing accounts.

At the top of the list are Full Name and Social Security number. Combined, these two pieces of data could give an identity thief enough information to do everything from opening up a credit card account to taking out a loan. And what happens once these new accounts (or existing accounts) are abused by a thief? From insurance companies to banks to utility companies and landlords, a victim can be denied service based on the unsound condition of his or her credit.

**Personal Data Most Often Stolen by Thieves.**

- Full name: 32%
- Social Security number: 29%
- Physical address: 20%
- Checking account number: 20%
- ATM PIN on your debit card: 17%
- PIN on your credit card: 12%
- Driver's license number: 11%
- Credit card number: 10%
- Other: 7%
- Online banking username and password: 5%
- Health insurance information: 4%
- Medical records: 3%
- Military ID card: 2%
- Debit card number: 2%
- Passport: 1%

---

12 Frank Abagnale’s Tips for Protecting Your Credit
Your PrivacyGuard Solution:  
**Internet Surveillance**

Remember… as a PrivacyGuard member, the Internet is being monitored for your personal information by our proprietary “early warning,” real-time technology. Underground chat rooms, Web sites, and blogs where thieves trade and sell stolen data are watched 24/7. If any of your registered cards or your Social Security number are found within these locations, you will automatically receive an alert that helps give you time to protect yourself.²

² Please see page 31 for details.
To maintain your credit status, you first need to make sure there aren’t any inaccuracies on your credit report and that someone is not using your identity. One of the best ways to do that is by consistently checking your credit report.

What is a Credit Report?
A credit report contains information about your credit borrowing history. With data gathered from one or all three major credit reporting agencies (Equifax®, Experian®, TransUnion®), potential lenders can see details about your borrowing behavior.

What is a Credit Score?
To make it easy for lenders and other creditors to assess your creditworthiness, the credit score was developed. Since each of the three credit reporting agencies have their own data, your score might differ among them. It’s very important to know all three scores because if one agency’s score is much lower (or higher) than the others, it means there could be an identity theft or credit reporting inaccuracy.
Why you should never stop keeping an eye on your credit report and credit score.

Identity Theft and Credit Fraud – By monitoring your credit report on a consistent basis, you will discover if new accounts have been opened that you didn’t open yourself. You will also be able to see if account balances have increased due to a stranger’s spending spree.

Credit Reporting Inaccuracies – With so many credit records being accessed every day, inaccuracies are bound to occur. Unfortunately, some of these can be so serious they can lead to a denial of credit. By continually reviewing your credit report, you can find any inaccuracies and dispute them quickly in order to resolve potential issues.

Score Ups and Downs – If you see that your credit score goes up or down dramatically and you know you haven’t done anything to warrant that activity, it could mean you’ve become a victim of identity theft. Knowing this sooner rather than later can help stop a criminal in their tracks.

Your Financial Future – Knowledge is power and knowing what’s going on with your credit at all times is important to your financial future. Being aware of any potential problems gives you the ability to take action and prevent or stop these issues from getting out of hand.

Your PrivacyGuard Solution:
Credit Report and Credit Score Monitoring

PrivacyGuard members have access to their Credit Report with combined information from all three credit reporting agencies. It’s in an easy-to-read format so you can know at a glance where your credit stands. Plus you get your credit scores compiled from files at the three major credit reporting agencies with an explanation on how you might be able to enhance them.5

YOUR CREDIT REPORT:
THE TOP 4 ITEMS TO CHECK

1. Check your ACCOUNT LISTING – This section includes each of your credit accounts and details about your payments. Make sure that the accounts listed are actually accounts that you opened and that they are up-to-date.

2. Check INQUIRIES – There are “hard” inquiries which may impact your credit rating and “soft” inquiries which do not impact your rating. Look for an EMPL (or similar) category which is typically an employment inquiry.

3. Check for NEGATIVE INFORMATION – This usually consists of accounts in negative status (not paid as agreed), collections (accounts turned over to a collection agency), and public records (typically bankruptcies, liens or judgments from government records).

4. Check PERSONAL INFORMATION – Make certain your personal information is correct because it’s often used to confirm your identity when you apply for various accounts.
“I’m a Victim! Now What?”

So the first question is, “How do you know if you’re a victim of identity theft?”. There are numerous signs, but most likely you’ll notice one of the following:

• You’re denied a credit card because of a low credit score when you know you’ve always paid your bills on time.
• You receive a phone call or written communication that tells you you’ve been approved or denied credit for an account you never requested.
• You stop receiving credit card statements.
• Your credit card statement includes charges for things you know you never bought.

• A collection agency calls to request payment for an account you never opened.

At this point, it’s obvious you’re a victim. You might feel violated or helpless. You might even feel guilty that somehow you allowed this to happen. No matter what the truth is, or isn’t, you must take action immediately before the consequences get out of hand.

How Criminals Like to Spend Your Money: The Top 5 Methods of Misuse.¹⁴

- 13% Make phone/mail purchases
- 9% Withdraw cash from ATM
- 30% Make in-person purchases
- 8% Write checks
- 40% Make purchases online
Resolving Your Identity Theft Problem: This Could Take Some Time.  

<table>
<thead>
<tr>
<th>All new account fraud</th>
<th>Existing non-card fraud</th>
<th>Existing card fraud</th>
<th>All fraud victims</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>59</strong> HOURS</td>
<td><strong>46</strong> HOURS</td>
<td><strong>26</strong> HOURS</td>
<td><strong>33</strong> HOURS</td>
</tr>
</tbody>
</table>

The Steps to Take

If you find you are a victim of identity theft or credit fraud, there are specific things you must do to resolve the situation. As a PrivacyGuard member, you have access to benefits that will assist you and fraud specialists who can help walk you through each step.

1. **Notify credit agencies and establish fraud alerts.** Immediately report your situation to the fraud department of the three credit reporting agencies – Experian, Equifax, and TransUnion. (See Page 18 for resource information). When you notify one, that agency will notify the other two. By placing a fraud alert on your file, your credit file will be “flagged” which means creditors are required to take extra caution before extending credit. In most cases this means they will call you to confirm the application is legitimate.

2. **Check your credit report.** Review your credit report for signs of theft. Consider freezing your credit reports so that credit issuers cannot access your credit files except when you give permission. This prevents thieves from opening up new credit card and loan accounts.

3. **Report the crime to law enforcement.** Tell your local police or sheriff’s department about the crime right away. Provide them with as much documented evidence as possible and retain your investigator’s contact information for verification when creditors and others ask about your case.

4. **Managing credit accounts.** Immediately contact your creditors by telephone and in writing so they are aware of the situation. Request replacement cards with new account numbers immediately.

Your PrivacyGuard Solution: Identity Fraud Support Service®

As a PrivacyGuard member, you will have a dedicated FCRA (Fair Credit Reporting Act) trained caseworker assigned to work with you if you become a victim of identity theft. Your caseworker is FCRA-certified, which means he or she has complete knowledge of how credit grantors, consumers and the credit reporting agencies interact. Their job is to help you help restore your identity and support you every step of the way with ongoing assistance throughout the recovery process.

*Please see page 31 for details.*
Help Is Just a Phone Call (or Mouse Click) Away!

It’s important to know that if you become a victim of identity theft you are not alone. As a PrivacyGuard member, you have access to two significant resources:

1. The Credit Information Hotline which is available to answer questions you may have about your credit report. From assisting you in understanding the details of your report to supporting you when you need to dispute errors, PrivacyGuard credit experts are ready to help.
   **Call: 1-800-270-3819**

2. Identity Fraud Support Service that helps you restore your identity and also assists in resolving many of the issues created by identity theft. You’ll have a personal caseworker at your service to provide assistance when you need it the most.
   **Call: 1-866-889-8506**

You might also need to contact the credit reporting agencies’ fraud departments or governmental agencies who help you handle these types of crimes. If you do...

**Equifax:**
P.O. Box 740250, Atlanta, GA 30374-0241
(888) 766-0008
Web: www.equifax.com

**Experian:**
P.O. Box 9532, Allen, TX 75013
(888) 397-3742
Web: www.experian.com/fraud

**TransUnion:**
P.O. Box 6790, Fullerton, CA 92834-6790
(800) 680-7289
Web: www.transunion.com

**Federal Trade Commission**
(877) ID-THEFT (877-438-4338)
Web: www.consumer.gov/idtheft

**Social Security Administration**
(800) 269-0271
Web: www.socialsecurity.gov

**U.S. Postal Inspection Service**
(800) 275-8777
To find nearest Postal Inspector:
Web: www.usps.com/postalinspectors

**Privacy Rights Clearinghouse**
Web: www.privacyrights.org
As you can probably imagine, there are a multitude of ways to help prevent identity theft. However, Frank Abagnale has a “Top 10” list – ten rules he feels can best help you protect yourself, your credit, and your good name from identity thieves.

It’s important to remember that all of the tips must be used consistently. For instance, it doesn’t help to shred some personal documents and not others. Nor does it make sense to create strong passwords for some accounts and not for others. Staying consistent in the fight against criminals will make it increasingly difficult for them to steal your personal information and turn you into a victim.

So, let’s start with Number One…
As you’ve seen throughout this handbook, checking your credit report regularly is crucial to helping protect your credit. There are three primary reasons for this:

1. **It enables you to see if there’s any suspicious activity present in your file.** By checking your report, you’ll be able to discover if a thief has opened new accounts in your name or has run up large balances on your credit cards. This will help you minimize the impact an identity thief could have on your credit.

2. **It gives you the opportunity to check for inaccurate information.** With millions of credit reports filled with inaccuracies, it’s important to check the accuracy of your file information so you can dispute any problems as soon as possible. The last thing you want is to be denied credit because of something as simple as a misspelling of your name.

3. **It allows you to learn how you might be able to manage your credit.** Knowing what’s in your report helps you identify potential (or current) problems that you can work on to help maintain your credit status. This is important because, based upon your credit status, lenders decide whether or not to lend you money and how much interest they will charge.
Along with the increasing use of the Social Security number as an identifier, has come a growth in its abuse. Criminals who get hold of your Social Security number can use it to assume your identity and gain access to your bank account, credit account, utility records, and other personal information.

That’s why it’s imperative to provide your Social Security number only when absolutely necessary and share it exclusively with reputable, trustworthy individuals.

**When it comes to protecting your Social Security number, here are some other important things to remember…**

- Do not print your Social Security number on checks, business cards or stationery.
- Only carry your Social Security number in your wallet when you know you’re going to need it. Otherwise, if your wallet is lost or stolen, you risk the chance of a stranger using it for their own means.
- Make sure the information on your Social Security Personal Earnings and Benefit Estimate Statement is correct. You can get more information about this statement and how to obtain it at: [www.ssa.gov/mystatement](http://www.ssa.gov/mystatement).
- Do not use your Social Security number as a password or Personal Identification Number (PIN) on the telephone or the Internet. It’s very simple for hackers to obtain this number and destroy your credit.
Shred It! All of It!

Financial statements... pre-approved credit card offers... printed e-mails with sensitive and personal information on them – shred them! It’s one of the most secure (and affordable) ways to help stop your personal information from getting into the hands of an identity thief.

Other than helping to prevent identity theft, there are other reasons why investing in a shredder can be beneficial – for both homes and businesses:

1. **It’s Just Good Business**
   Government is placing the burden of protecting individuals on businesses – making sure they protect the documents and information in their possession. It is a best practice for a business that works with consumer data to use a shredder.

2. **Medical Record Security**
   In 1996, Congress enacted the Health Insurance Portability and Accountability Act. So any business that is responsible for keeping medical records or transferring medical information, must be familiar with this law and shred documents accordingly.

3. **Help the Environment**
   When you shred your documents, less landfill space is used, trees are saved and airborne pollutants are not expelled through the burning of the paper. So if you think about it, shredding your documents not only helps protect your identity, but it protects the environment as well.

»» I prefer micro-cut shredders that turn paper into confetti.
   – Frank Abagnale
Credit Card Statements: It’s in the Details.

Why check your credit card statement?

First and foremost, it’s one of the fastest ways to determine if someone else has been using your card. If you see purchases listed that don’t look familiar to you or if the balance is much higher than you had anticipated, these are signs that someone has been using your credit card number without your knowledge. Not surprisingly, if you don’t check your statement and fraudulent charges are being made, you could just keep paying for a criminal’s purchases without even knowing about it!

**IMPORTANT:**
Just because a criminal gets hold of your credit card number doesn’t mean he or she will immediately run up huge bills. Not all thieves work this way. Many of them only withdraw or charge small amounts at different times so that they are less likely to be detected and the card issuers’ monitoring systems might not spot the fraud as easily.

Checking your statement also allows you to get an understanding of your spending habits. Not only can it result in a tighter budget (and more money savings), but it also allows you to see when your spending goes “out of whack” – another sign that an identity thief might have gotten hold of your credit card. When you check your credit card statement, make sure to check each transaction and you’ll stand a much better chance of minimizing damage caused by an identity thief.
Picture it: A mailbox overflowing with catalogs, envelopes and other types of mail for days in a row. That’s the perfect signal to criminals that there’s personal information for the taking and more often than not, they will take it.

Your mailbox is one of the riskiest “non-technological” points of identity theft. Why? Thieves have two ways of stealing your identity through your mail: re-routing your mail and mail theft.

**Mail Re-routing**
Criminals place a “change of address” with the U.S. Postal Service by filling out a form online or mailing in a card. Once the change of address takes place, the thief will start getting your mail – unfortunately that means they will then have access to mail that contains your bank account, credit card, and Social Security numbers.

**Mail Theft**
This is a more direct form of theft: the thief simply takes your mail right out of the mailbox. It could be while you’re visiting friends or family, taking a walk around the neighborhood, or whenever else the opportunity presents itself. Once again, more often than not there’s information a thief can use to steal your identity.

**Remember:**
- Pick up your mail as soon as possible.
- If you’re going away, have someone you trust pick up your mail.
- Don’t leave out-going mail in your mailbox. Drop it off at the post office. But if you must leave mail in the mailbox, do not put the flag up. It’s a sign to thieves that there’s mail for the taking.
- Use electronic and online payments whenever possible.

**ALERT!!** If you notice that you don’t receive mail for a few days in a row, this could mean that mail re-routing has occurred. Mail theft is a little less obvious because it can take place just once or over a period of time. If you haven’t received bills or notices that you know should have been delivered, it’s time to check with the companies from which the bills or notices would have been sent.
Frank’s Tip #6

Sharing is Good: Unless it’s Personal.

Sharing can be a wonderful thing. When you share knowledge… happiness… gifts… and other things that add positively to someone else’s life, it’s a good thing. But when you share your personal data, information that might be used to commit fraud, things can go bad quickly.

Here are some questions to ask yourself about your information sharing habits:

• Do you sometimes write your Social Security number on checks?
• Do you share files and personal information over the Internet?
• Do you ever provide credit card information to telemarketers?
• Do you show your birthdate and address on social networking sites?

If you answered “YES” to the questions above, you might not be sufficiently protecting your credit and identity.

Sometimes information is shared without even realizing it. For instance, when communicating on social networking sites with “friends,” many people announce events like an upcoming vacation or the recent purchase of an expensive item. Unfortunately, it’s not only “friends” who see these postings, but everyone who has access to them.

Your job is to protect your information. So simply being more selective with whom you share your information can decrease your chances of ever becoming an identity theft victim.
Automatic Teller Machines (ATMs):
Be on the Lookout.

How did we ever live without ATMs? They give us cash, retrieve our balances, even deposit checks – 24/7. The problem is, identity thieves work the same hours.

For instance, thieves set up some ATMs to “skim” cards. A small device captures information on your card’s magnetic strip. Criminals can then acquire your credit or debit card information and make duplicates of your card to sell as they please.

Thieves have also found ways to “bug” keypads. Typically, the keypads show no signs of manipulation because the “bugging” device is on the inside of the keypad. These devices still transmit customer data to the merchant, but they also capture personal information from the card and your PIN. When the thieves retrieve the device, they have everything they need to commit credit fraud.

Protect Yourself from ATM Fraud
1. Review your credit and debit card accounts so you can spot suspicious activity right away.
2. Do not trust keypads that don’t look right because tampering by inexperienced criminals can sometimes be obvious. Make certain the keypad is firmly attached to the counter or console.
3. Protect your PIN by covering the keypad with your hand and do not use ATMs where there is a camera positioned behind you.

Reminder!! ATM Transactions come in second place as one of the many ways criminals gain access to information. See Page 5 for details.
Password Protection: Stay Strong.

When first creating a password, there are two things to consider:

1. Selecting a password strong enough to guard against cyber intruders. With such sophisticated hacking software available, it’s a simple process for criminals to decode passwords and gain access to personal information.

2. Remembering the selected password. We’re told that in order to protect ourselves, we should create a password using uncommon strings of numbers and letters. But how are we supposed to remember them?

The DOs and DON’Ts of Password Creation

DOs

1. Use 8 or more characters – 14 characters is ideal.

2. Combine letters, numbers, and symbols. If the Web site does not allow symbols, create a password with more than 15 characters (if the site allows that password length).

3. Write your passwords down and keep them in a safe place. (Written passwords are safer than those maintained in computer password manager programs.)

4. Change your passwords on a regular basis.

DON’Ts

1. Do not use character sequences or repetitive characters (e.g. 123456, 8#8#8#8, 444444).

2. Do not use personal information. (e.g. part of your name, birthday, or Social Security number).

3. Do not use the same password in too many places. (If your password should become compromised, all other systems using that password will become compromised.)

4. Do not share your password with anyone or reveal it over e-mail.
Frank’s Tip #9

Credit Cards: The Fewer the Better.

Simply stated, the fewer credit and debit cards you have, the less chance you have of running into problems. What kind of problems? Let’s take a look…

Inability to Detect Fraud
If you use ten credit cards and five debit cards, how would you know if a criminal is using any of them? You’d have to keep daily tabs on each card – something most people are too busy to do.

Increased Risk of Identity Theft
It comes down to logic – the more cards you use (or have in your wallet), the greater the chance that one will get lost or stolen. The damage to your credit might also increase since it’s easier to overlook a missing card when you have a lot.

Credit Problems
It’s easy to run into credit problems if you use multiple credit and debit cards. For instance, you might be out shopping and grab a card from your wallet or purse. Forgetting you used that card only a few days before, your charge is denied because you’ve exceeded your spending limit.

Did You Know? The number of credit cards you have could affect your credit score. According to Experian (one of the three major credit report agencies), having too many credit cards with either high balances or large amounts of credit available can negatively impact one’s credit score – depending on the overall credit history. 6
It used to be that the term *hacker* was thought of as a “gifted programmer.” But times have changed. And with so many technological advances and such easy access to multiple systems, hacking is now defined as “the unauthorized use of computer and network resources.”

**How can you protect yourself?**

**Firewall Protection**
In the days when we accessed the Internet through dial-up connections, our computers were assigned a new and unique IP address. In a way, that made us a moving target, making it more difficult for a hacker to attack us. Today we use DSL and cable connections, which give us high speed, but unlike the dial-up connection, it also gives us a single IP address. This makes us more vulnerable to hackers and identity thieves. A firewall blocks hackers from accessing your computer.

**Antivirus Protection**
Although we use the Internet and e-mail for lots of things, a big part of what we use it for is sharing. From photos and news articles to videos and documents, it’s all about sharing data. Sometimes, however, this data can contain viruses that attack our computer hard drives and can ruin our computers. Antivirus protection (like the Norton Internet Security software that’s part of your PrivacyGuard benefits) helps keep bugs and viruses far away from your system.

**Spyware Protection**
SPYWARE: malicious software that hides on your computer and sends information about you, your computer, or your Web-surfing habits to someone else on the Internet. Attack spyware using spyware protection software that’s typically available from antivirus software manufacturers. And again… always be careful of the ads you click and what programs and other items you decide to download!
Extra Protection for You and Your Credit

As a PrivacyGuard member, your benefits are always available and “at your service.” In addition to the benefits already highlighted in this handbook, there are other protection and credit tools. See your membership materials or visit www.PrivacyGuard.com for full details.

Take a look at some of the additional assistance you get with PrivacyGuard…

**Score Tracker with Score Alerts**
This benefit provides you with your Experian Plus credit score, plotted on a monthly basis. The tracker typically plots your score within the first ten business days of each month and is tracked on a historical graph (up to two years).

You can also set up alerts to notify you when your score moves up and down within a selected range, when your risk level moves between specific levels, or when your score hits a pre-determined number. In addition to the e-mail alerts, the details of these alerts will be displayed on the Alert Summary Page within your account at www.PrivacyGuard.com.

**Credit Score “What If” Simulator**
Would you like to see how possible changes in your spending (and saving) behavior can affect your credit score? The Credit Score “What If” simulator uses your credit report and score to analyze how specific actions can impact your credit score.

**Credit Card/Document Registration with Lost and Stolen Assistance**
To help protect your credit, debit, ATM, and store cards along with your important documents, PrivacyGuard lets you store credit card, bank card and important documents in a single secure location. In the event of a loss, fraud, or a theft, just call the toll-free number (24/7) and request cancellation and replacement of all cards.

If you lose an important document and have it stored in our repository, we will fax or e-mail you a copy, at your request, so you will have the information you need (and thought you might have lost forever!) right away.
Norton™ Internet Security PC Protection Software
To help protect you against viruses and potential problems from online PC exposure, your membership includes Norton Internet Security Online protection. This package includes the following protection: Anti virus, anti-spyware, parental control, password management, identity safe protection, anti-root kit and anti-phishing… download it as part of your membership at www.PrivacyGuard.com.7

Financial Calculator Suite
Your membership gives you access to a suite of financial calculators that allow you to run different financial scenarios. For instance, there’s an Auto Loan calculator that helps determine monthly loan payments and provides you with a complete loan amortization schedule. There’s also a Loan Payoff calculator that helps you figure out the best way to pay off your debts, and a Mortgage calculator that generates a mortgage payment schedule specific for you.

Records and Reports
With PrivacyGuard it’s easy to review a number of your confidential records…

Medical Information Bureau (MIB) records, should any exist, can be requested through the service. Your MIB records may be utilized by companies to determine your eligibility and liabilities in obtaining an array of insurance including health, life, long term care and critical illness coverage.

Driver’s records can be sent to you so you can see the information an auto insurance company may use to set your rates.

Neighborhood reports, which contain information like home values, crime rates, and climate, can be requested if you’re considering a move or just traveling to an unfamiliar area.

PrivacyGuard is a service of Trilegiant Corporation in conjunction with Trilegiant Insurance Services, Inc. and Alliance Marketing Association. Trilegiant Insurance Services, Inc. does not receive any compensation from the sale of the identity theft insurance benefit included as part of the PrivacyGuard service. Any part of the service may be modified or improved at any time and without prior notice. PrivacyGuard and Credit Alert are registered service marks of Affinion Publishing, LLC.

1 Trilegiant Corporation, Trilegiant Insurance Services, Inc., Alliance Marketing Association and their credit information subcontractors shall not have any liability for the accuracy of the information contained in the credit reports or Credit Alert reports which you receive, including any liability for damages, direct or indirect, consequential or incidental. PrivacyGuard is not a credit counseling service and does not promise to help you obtain a loan or improve your credit record, history or rating.

2 Daily monitoring will notify members of any new inquiries, certain derogatory information, accounts, public records, or change of address that have been added to their credit reports as reported by any of the three major credit reporting agencies. If no information has been added or changed, then the member will receive a quarterly notification stating that no information has changed within their credit file.

3 Javelin, 2009 Identity Fraud Survey Report.
4 Javelin, 2011 Identity Fraud Survey Report.

PrivacyGuard.com
After a while, these terms – and the effect they could have on our credit – all seem a little complicated, and oftentimes scary.

With the help of world-renowned identity theft expert Frank Abagnale – hero of the blockbuster movie *Catch Me If You Can* and associated with the FBI for over 35 years – we’ve designed this Credit Protection Handbook to help you better understand what it all means and help protect your personal information, your credit and your identity.

In this book, you’ll find dozens of ways to help protect your credit, plus unique and helpful information, such as:

- What is a Credit Score?
- Why your Credit Report can affect your financial future
- Assessing your risk of Identity Theft
- Help reading and understanding your Credit Report
- How your PrivacyGuard benefits help you every day
- And a lot more, including: Frank Abagnale’s Top 10 Tips to Help Prevent Identity Theft.

**So go inside!**

Start from the beginning or turn to any page to find the information you need to help protect your credit, your identity, and your life.