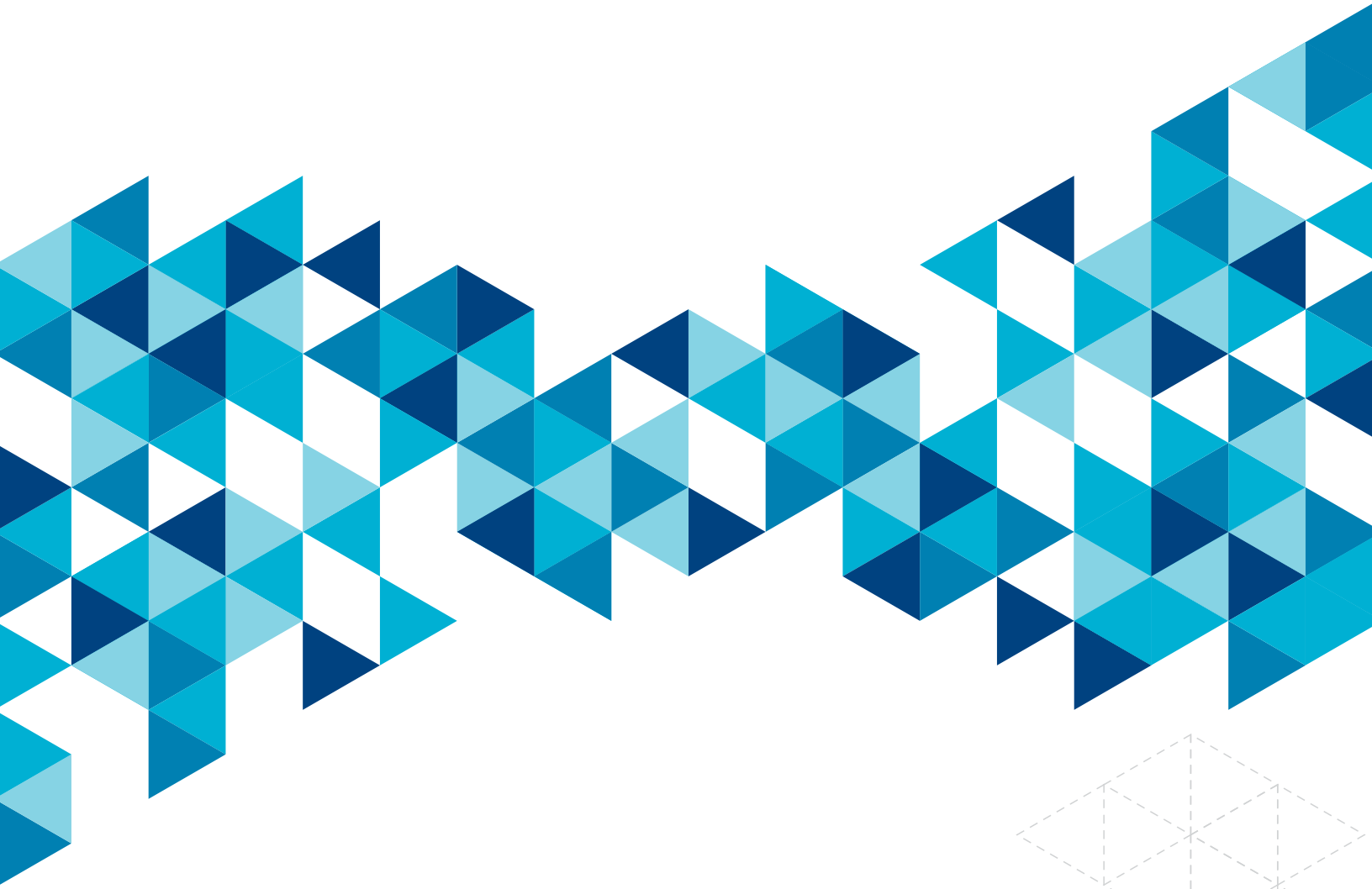
MARSH

PRIVATE CLIENT SERVICES

CYBER RISK AND IDENTITY THEFT:
PROTECT YOUR LIFESTYLE



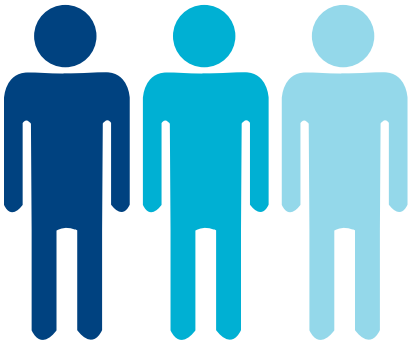
RISK MANAGEMENT EDUCATIONAL SERIES

INTRODUCTION

News reports show large-scale data breaches are on the rise and affecting large retailers like Target, Home Depot, and eBay. But we don't hear many reports about consumers falling victim to cyber crime, even though individuals — especially the affluent — are also frequently targeted, and this real threat is on the rise.

Cyber crime is defined as any criminal act that involves computers and networks. In addition, it includes traditional crimes conducted through the Internet. Today, cyber crime is a greater risk than ever before because of the copious amount of time people spend online and the vast number of personal handheld devices owned. It's a rapidly evolving landscape that demands attention.

There are numerous categories of cyber crime, but the ones that affect the most victims include identity theft, credit card fraud, and social networking scams. Review the information presented in this report to learn how to better protect yourself, your family, and your lifestyle from cyber crime and its long-lasting effects.



The Federal Trade Commission reported that identity theft affected **13 million** consumers in 2013.

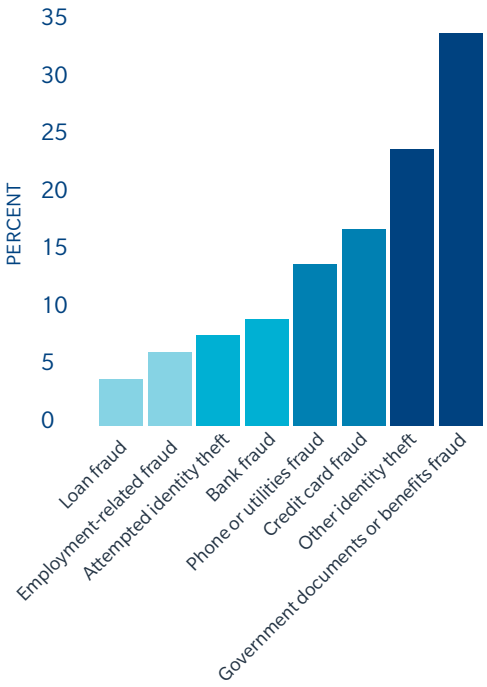
IDENTITY THEFT — A TOP CYBER THREAT

Because of the amount of personal information stored and shared on electronic devices, identity theft is one of the largest cyber crime threats today. The best way to protect yourself is to be aware of your activity when using smartphones, tablets, and other devices that store personal information digitally.

According to the Insurance Information Institute, identity theft is the act of taking someone's personal information and using it to impersonate them, steal from bank accounts, establish phony insurance policies, open unauthorized credit cards, or obtain unauthorized bank loans. In more elaborate schemes, criminals use the stolen personal information to get a job, rent a home, or take out a mortgage in the victim's name.

Close to half of identity theft cases are the result of a lost or stolen wallet, checkbook, credit card, or other physical document. Because of the popularity of online shopping, it too can pose as a serious identity theft risk.

Victims of identity theft are often left with lower credit scores and spend months or even years getting credit records corrected. They frequently have difficulty getting new credit, obtaining loans, and even finding employment. Victims of identity theft fraud often travel a long and frustrating road to recovery; depending on the severity of the identity theft fraud damage, the recovery process can take anywhere from a few weeks to several years.[i]



HOW VICTIMS' INFORMATION IS MISUSED[ii]

TYPE OF IDENTITY THEFT FRAUD	PERCENT
Loan fraud	4
Employment-related fraud	6
Attempted identity theft	7
Bank fraud*	8
Phone or utilities fraud	14
Credit card fraud	17
Other identity theft	24
Government documents or benefits fraud	34

Percentages are based on the total number of complaints in the Federal Trade Commission's Consumer Sentinel Network (290,056 in 2013). Percentages total to more than 100 because some victims reported experiencing more than one type of identity theft (16% in 2013).
*Includes fraud involving checking and savings accounts and electronic fund transfers.

TIPS FOR AVOIDING IDENTITY THEFT

Reduce your chances of becoming a victim of identity theft by practicing the following tips developed by the Insurance Information Institute:

- Keep the amount of personal information in your purse or wallet to the bare minimum. Avoid carrying additional credit cards, your social security card, or passport unless absolutely necessary.
- Guard your credit card when making purchases. Shield your hand when using ATM machines or making long distance phone calls with phone cards. Don't fall prey to "shoulder surfers" who may be nearby.
- Always take credit card or ATM receipts. Don't throw them into public trash containers, leave them on the counter, or put them in your shopping bag where they can easily fall out or get stolen.
- Do not give out personal information. Whether on the phone, through the mail, or over the Internet; don't give out any personal information unless you have initiated the contact or are sure you know who you are dealing with and that they have a secure line.
- Proceed with caution when shopping online. Use only authenticated websites to conduct business online. Before submitting personal or financial information through a website, check for the locked padlock image on your browser's status bar or look for "https://" (rather than http://) in your browser window. If you have any concerns about the authenticity of a web page, contact the owner of the site to confirm the URL.

Use only authenticated websites to conduct business online.

- Be aware of phishing and pharming scams. In these scams, criminals use fake emails and websites to impersonate legitimate organizations. Exercise caution when opening emails and instant messages from unknown sources and never give out personal, financial, or password-related information via email.
- Make sure you have firewall, anti-spyware, and anti-virus programs installed on your computer. These programs should always be up to date.
- Monitor your accounts. Don't rely on your credit card company or bank to alert you of suspicious activity. Carefully monitor your bank and credit card statements to make sure all transactions are accurate. If you suspect a problem, contact your credit card company or bank immediately.
- Order a copy of your credit report from each of the three major credit bureaus. A law that took effect December 1, 2004, entitles you to one free credit report per year. Your credit report contains information on where you work and live; the credit accounts that have been opened in your name; how you pay your bills; and whether you've been sued, arrested, or filed for bankruptcy. Make sure the reports are accurate and include only activities you've authorized.
- Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, any part of your Social Security number or phone number, or any series of consecutive numbers. If you suspect a problem with your credit card, change your password. It is a good rule of thumb to periodically change your passwords.
- Shred any documents containing personal information such as credit card numbers, bank statements, charge receipts, or credit card applications, before disposing of them.
- If you maintain a listing of account numbers and passwords, make sure to always keep this information in a secure place rather than on your cell phone or other potentially accessible devices.

In order to make it more difficult for identity thieves to open accounts in your name, you can also contact the fraud department of any of the three credit reporting agencies to place a fraud alert on your credit report — by law, the agency you contact is required to contact the other two agencies. The fraud alert tells creditors to contact you before opening any new accounts or making any changes to your existing accounts. The three major credit bureaus are Equifax, TransUnion, and Experian.[iii]

TEST YOUR IDENTITY THEFT KNOWLEDGE

How well are you and your family protected from identity theft when online and as a whole?

Gauge your risk level and find out how to be more proactive by taking the quiz developed by the U.S. Department of Justice found at the end of this article.

ACT QUICKLY IF YOU SUSPECT CREDIT CARD FRAUD

As mentioned in the introduction, use of stolen credit card numbers is one of the most common forms of identity theft and it no longer happens primarily from failure to shred paper documents.

Another way cyber criminals get credit card numbers is through radio-frequency identification (RFID) chips that credit card issuers are placing on cards now instead of magnetic stripes. The advantage of RFID chips is quicker transactions at retail outlets like fast-food restaurants and convenience stores. The problem is, radio frequency identification makes it possible for identity thieves to use a simple electronic device to capture the information.

Some effective was to stay on top of credit card fraud include:

- Follow your credit card billing cycles closely.
- Keep a list of account numbers, expiration dates, and credit issuers telephone numbers on hand.
- Sign up for a credit monitoring service.
- Clear online passwords and logins.

If you suspect you're a victim of credit card fraud or identity theft, act quickly to protect yourself. Work with your credit monitoring service or contact the issuers directly to verify if fraud has occurred and remove fraudulent charges if necessary.

Be aware of how much personal information you give out on social networks, who you connect with, and what links you click on.

SOCIAL NETWORKS — THE LATEST CYBER PLAYGROUND

Social networks including Facebook, Twitter, Instagram, LinkedIn, and Pinterest have become a part of many people's daily lives. It's a great way to stay connected, but it's important to be aware of how much personal information you give out, who you connect with, and what links you click on. The Federal Bureau of Investigation has identified a number of scams to be cautious of when using social networking sites.

SOCIAL ENGINEERING

It's no surprise that cyber criminals can fake everything about themselves online, including their names and business affiliations, gender, age, and location. The FBI is continuously investigating investment fraud schemes happening online. Cyber criminals carry out identity theft crimes by misidentifying themselves on social networking sites and then tricking victims into giving them their account names and passwords, as well as other personally identifiable information.

Avoid posting any personal information about you or your family.

FRAUD SCHEMES

Cyber criminals are quite creative when it comes to online fraud schemes. The FBI reports recent fraud schemes involving cyber criminals gaining access to a victim's social networking or email account. The criminals claim to be the victim and send messages to the victim's friends. In the messages, the criminal claims he or she is traveling and has been robbed of their credit cards, passport, money, and cell phone and is in need of money immediately. Without realizing that the message is from a criminal, the friends wire money to an overseas account and become victims.

PHISHING SCAMS

Phishing scams are used by cyber criminals to make potential victims think they are receiving messages from a trusted source. According to the FBI, phishing schemes on social networking sites are cleverly packaged and may include: messages from strangers or compromised friends' accounts, links or videos claiming to lead to something harmless, or messages that claim to be from the social networking site itself. Social networking users fall victim to the schemes because of the high level of trust associated with social networking sites. Users often accept invites to connect with people they don't actually know or don't adjust profile privacy settings appropriately. This gives cyber criminals an upper hand to send messages containing software designed to give the criminal control over the victim's entire computer. Once the malware infection is discovered, it is often too late to protect personal data from compromise.

DATA MINING

Cyber criminals use data mining techniques to obtain information from victims through social networking. A cyber criminal may send out a "get to know you" questionnaire to potential users asking them questions that sound like they are coming from a financial institution. The answers to the questionnaire can provide the cyber criminal with the information they need to enter the victim's bank account, email account, or credit card and do severe financial damage.

SOCIAL NETWORKING BEST PRACTICES

Educate yourself and your family members about the risks of posting information on social networks that an identity thief could use for malicious purposes. Learn how to spot potential Internet scams and what to do to protect your sensitive information from cyber crime.

Follow these guidelines to keep personal information secure when using social networking sites:

- Avoid posting any personal information about you or your family, including your name or contact information that could put you at risk of identity theft.
- Never send personal information through a message or click on a link in a suspicious message.

- Keep in mind that information posted on social media sites can be seen by anyone; even if you use security settings, hackers can still access this data.
- Never post about upcoming vacations, especially specific details like dates of travel.
- Opt out of Facebook and Twitter functions that automatically tag posts with a location. If a site asks to "use your location" reply "no."
- Regularly check your privacy settings on social media sites to learn if your friends and followers receive your updates.
- Use strong password management strategies.
- Set appropriate privacy and security defaults.
- Be cautious about installing third-party applications. Do not install applications from sources you do not know.
- Only accept friend requests from people you know directly.
- Be careful what you post and consider all information and pictures you post as public.

Be aware of what you're storing in cloud services.

PROTECT YOUR DATA IN THE CLOUD

Cloud services, such as Dropbox, Google Docs, and iCloud, transmit and store users' data across Internet connections that are susceptible to monitoring and interception. This type of computing is growing in popularity because it allows users access to files from any connected device, but cyber security problems are increasing at the same time.

There are some steps you can take to protect your data from getting into the wrong hands when using cloud services:

- Be aware of what you're storing in cloud services.
- Use different passwords for all your cloud services accounts, and change them all frequently.
- Don't use answers to security questions about yourself that may be available publically.
- Take advantage of the two-step identification process that most services offer.
- Encrypt your data with a third-party data encryption service.
- Unlink devices you don't use.
- Enable email settings to alert you when new devices gain access to your accounts.

If you don't see or understand a site's privacy policy, consider doing business elsewhere.

KEEP YOUR DEVICES SECURE

Many people have more than one mobile device. Follow these recommended best practices from the Federal Trade Commission to keep all your devices safe from cyber crime risk:

USE OF SECURITY SOFTWARE

Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

BE SMART ABOUT WI-FI

Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. Use a secure wireless connection for protection.

LOCK YOUR LAPTOP

Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

READ PRIVACY POLICIES

Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

SAFELY DISPOSE OF PERSONAL INFORMATION

Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.

Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (sim) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

Use strong passwords with your laptop, credit, bank, and other accounts.

ENCRYPT YOUR DATA

Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

KEEP PASSWORDS PRIVATE

Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the pacific ocean" could become 1w2ctpo.[iv]

PRODUCTS DESIGNED TO PROTECT YOUR IDENTITY

A number of insurance carriers offer personal identity products to help protect you from cyber crime threats, such as identity theft. Some carriers include coverage for identity theft and restoration services as part of their homeowners insurance policies. Other companies sell more comprehensive coverage as a stand-alone policy or as an endorsement to a homeowners insurance policy.

Identity theft insurance provides reimbursement to crime victims for the cost of restoring their identity and repairing credit reports. It generally covers expenses such as phone bills, lost wages, notary and certified mailing costs, fees when reapplying for loans, grants or other credit instruments, and sometimes attorney fees (with the prior consent of the insurer).

Some companies also offer restoration or resolution services to guide you through the process of recovering your identity, which can include working with credit card companies, credit bureaus, creditors, and businesses on your behalf to correct any covered identify fraud issues. Identity theft insurance will reimburse a policyholder for expenses incurred to restore his or her identity, up to the limits stated in the policy. Coverage limits typically range from $10,000 to $1 million.

TEST YOUR IDENTITY THEFT KNOWLEDGE

1. When I keep my ATM cards and credit cards in my wallet, I never write my PIN (Personal Identification Number) on any of my cards.

   Reason: If you lose your ATM or credit card, identity thieves or other criminals can have instant access to your bank or credit-card account.

2. When I leave my house, I take with me only the ATM and credit cards I need for personal or business purchases.

   Reason: If your wallet or purse is lost or stolen, and you're carrying fewer cards, you'll have to make fewer calls to banks and credit card companies to report the losses, and the odds of fraudulent charges in your name will be lower.

3. When I get my monthly credit card bills, I always look carefully at the specific transactions charged to my account before I pay the bill.

   Reason: Someone who gets your credit card number and expiration date doesn't need the actual card to charge purchases to your account. If you don't look closely at your credit card statement each month, you might not have any recourse if fraudulent transactions go through and you don't dispute them promptly with your credit card company. As soon as you see unauthorized charges on your statement, contact the credit card company immediately to report them.

4. When I get my monthly bank statements, credit-card bills, or other documents with personal financial information on them, I always shred them before putting them in the trash.

   Reason: Some identity thieves aren't shy about "dumpster diving" — literally climbing into dumpsters or rooting through trash bins to look for identifying information that someone threw out. Buying and using a shredder in your home or office is an inexpensive way to frustrate dumpster divers and protect your personal data.

5. When I get mail saying I've been preapproved for a credit card, and don't want to accept or activate that card, I always tear up or shred the preapproval forms before putting them in the trash.

   Reason: If you throw out the documents without tearing them up or shredding them, "dumpster divers" can send them back to the credit-card company, pretending to be you but saying that your address has changed. If they can use the account from a new location, you may not know the account's being used in your name until you see it on a credit report (see below).

6. I request a copy of my credit report at least once a year.

   Reason: Any consumer can request one free copy of his or her credit report per year. Reviewing your credit report can help you find out if someone has opened unauthorized financial accounts, or taken out unauthorized loans, in your name. Contact the three major credit bureaus to request a copy:

   - Equifax (1 800 685 1111)
   - Experian (1 888 397 3742)
   - Trans Union (1 800 916 8800)

7. If the volume of the mail I get at home has dropped off substantially, I always check with my local post office to see if anyone has improperly filed a change-of-address card in my name.

   Reason: Some identity thieves may try to take over your credit card and bank accounts, and delay your discovery of their criminal activities, by having your mail diverted to a new address where they can go through it without your knowledge. Your local post office should have on file any change-of-address cards, and can respond if you find that someone is improperly diverting your mail.

8. If I think that I may be a victim of identity theft, I immediately contact
   - The Federal Trade Commission to report the situation and get guidance on how to deal with it.
   - The three major credit bureaus to inform them of the situation.
   - My local police department to have an officer take a report.
   - Any businesses where the identity thief fraudulently conducted transactions in my name.

   Reason: Identity theft is a crime under federal law, and under the laws of more than 44 states, that carries serious penalties including imprisonment and fines. To help law enforcement in investigating and prosecuting identity theft, the Federal Trade Commission (FTC) maintains a national database of complaints by identity theft victims. The FTC, through a toll-free hotline (1-877-ID-THEFT), can also help you decide what steps to take in trying to remedy the situation and restore your good name and credit. Credit bureaus should also be notified so that they can flag your credit report. Local police, by taking a report and providing you with a copy, can help you show creditors that an identity thief has been conducting certain transactions in your name and without your permission.

How did you score on this quiz? If you answered three to four questions incorrectly, it means you may need to take more of the precautions described. The more you do to protect your personal information, the lower the odds that you'll become a victim of identity theft.

Resource: U.S. Department of Justice

Talk to your trusted Marsh Personal Risk Advisor to ensure you are adequately protected against identity theft. With the proper coverage in place, you can avoid major upset to your financial wellbeing and save yourself time restoring your credit and good name.

ABOUT MARSH PRIVATE CLIENT SERVICES

At Marsh Private Client Services (PCS), our mission is simple: to help successful individuals and families protect their property and their lifestyles by providing expert personal insurance consultation, solutions, and services.

Marsh PCS has been a pioneer in the field of personal insurance advisory services since our beginnings in 1980. We realized then that the standard approach followed by most insurance companies does not take into account the unique risks facing those with wealth, so we built our business by individually customizing personal insurance programs for each of our clients.

REFERENCES

[i]Insurance Information Institute: iii.org/article/identity-theft-insurance
[ii]Federal Trade Commission: ftc.gov
[iii]Insurance Information Institute: iii.org/article/identity-theft-insurance
[iv]Federal Trade Commission: consumer.ftc.gov