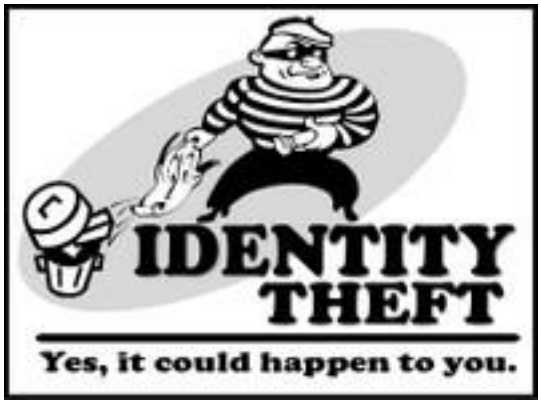
Chapter 5: Identity Theft

Keep Your Personal and Financial Information Secure

No treatise on asset building and financial empowerment would be complete without a discussion of identity theft. Particularly for folks with disabilities, who often share information with trusted friends, family members and attendants, this issue can be critically important.



Identity theft and the unauthorized use of financial and credit resources have been impacting consumers in the U.S. for years. In 2014, the most recent year with available data, nearly 13 million people became victims of identity fraud in the U.S., costing them a cumulative $16 billion. (Info via Javelin Strategy and Research) That means identity theft impacted someone every 2.5 seconds! Although these numbers are down from the $18 billion in losses in 2013 and $21 billion in 2012, they are still dramatic reminders that you may be at risk for identity theft.

Many of the 2014 reported cases of fraud included misuse of credit cards, misuse of personal information, and bank account fraud. These types of fraud can leave lasting impressions on victims and their ongoing financial wellness. Clearly, identity theft is a huge problem that can impact anyone! Here are a few action steps you can take right now to increase your financial and personal security!

Strengthening Your Digital Security

Let's face it: Most of us have quite an electronic presence on the Internet**.** Whether we do online banking, use social media, or visit Chicago Cubs fan sites (actually, I think there might only be one), many of us spend more time online than we have in the past. And because that online presence holds a bunch of sensitive information, and thus access to things like finances and the ability to obtain credit, it's critical to keep online data secure. This could be particularly important if personal attendants or family members have access to some of your information. Having a disability often changes relationships between people, but even if you trust them deeply, it's better to be cautious than not.

The first big step for keeping data secure is to choose strong passwords and PINs. You should always choose a password composed of words and numbers that no one would be able to guess, even if they knew details about other parts of your personal information. Have you ever seen the annual list of most common passwords? Seriously, according to Gizmodo, last year it included 123456, Password, football, and starwars. Your accounts are unlikely to be safe if you pick a password this basic. You should trend away from popular passwords and pick something unique to you, then throw in a few capital letters, and maybe even a special character like a % or # or $ (some websites even require a minimum password length, numbers, and/or special characters). As far as ATM cards go, most experts suggest that you also avoid using easily guessed PINs, like birth dates, common numerical sequences, phone numbers, the last four digits of your Social Security number, etc., as these can be easily guessed with little research.

One other important tip: Never, ever, use the same password for all your accounts, because once hackers find a working password, they will have the key to the entirety of your online existence. If you have trouble remembering your passwords, write down a hint that only you will understand and where it won't get lost. For example, one member of the EQUITY team keeps her hints (just the hints, not the whole passwords!) in an online Google spreadsheet, and another has his tucked away securely in his wallet. Finally, avoid automatically saved passwords in your browser, especially for email and financially sensitive logins, such as your bank account, as someone who gets a hold of your computer could swipe all your info easily. These strong account passwords are just the first components of many needed to keep your identity safe.

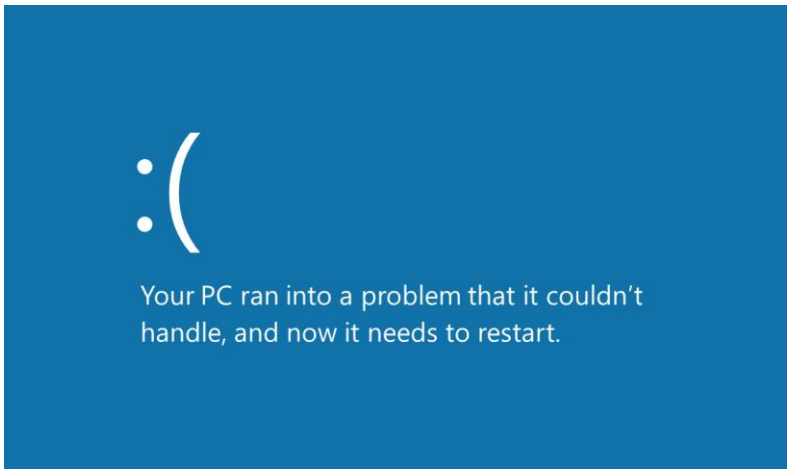
Don't Forget to Protect Your Computer

Another critical component to protecting your identity is protecting your computer. If hackers break into your computer, they can steal all sorts of sensitive information, including any stored files and their contents, your browser history, and any passwords you've used, even your Social Security number if you've entered it online. They often get this info without you even knowing it, and keep doing it indefinitely, or they might decide that they've gotten enough and just kill your computer from afar. Heck, sometimes they'll kill your computer without stealing the info, because they're jerks!

To counter this, a regularly updated firewall, antivirus program and antispyware program can keep the contents of your computer safe from intruders. There are many credible, verified companies that sell these protections in package deals for a modest annual or biannual fee. I suggest reading some online reviews for antivirus software program companies and their package deals to get a good idea of what is right for your computer needs. And I totally have to confess, I learned the "regularly updated" part the hard way. Several years ago, I purchased a new computer with a year of free firewall and antivirus software on it. After about a year, I began receiving reminders to update this, and update that, but I really didn't think it was all that important. I figured that if it had protected my computer this long that everything would be fine and all those updates were probably a rip-off advertising overpriced, unnecessary products anyway. When the blue screen of death (BSOD) arrived — that is, my computer just sat there with a very calm blue screen, doing nothing, at all, forever — I quickly called my computer programmer friend Mary and asked her to take a look. Because this is a family publication, I'll spare you Mary's justifiable diatribe… but sadly, my computer was gone forever, along with my

files and probably some personal info (which so far hasn't been used against me, but we'll see). So trust me on this one: Get a good antivirus software program, keep it updated, and you will have most of the protection an individual computer needs.

The Blue Screen of Death… Except it never actually restarts…
(Here's the classic "blue screen of death" - a blue screen with a sad face emoticon that says: "Your PC ran into a problem that it couldn't handle, and now it needs to restart.")



So, now let's go through some other ways to keep your digital information safe.

Be Aware of Phishing Scams

Phishing scams are common ways for hackers to gain information**.** Phishing involves seemingly harmless emails being sent to you, asking you to verify certain things, such as passwords, account numbers, or credit card and Social Security details. Any email seeking this sort of information should be an immediate red flag for you. If you get an email claiming to be from your bank or creditor that tells you to check or update your information, such as a password (for any reason), do not use the link in the email, even if it looks like it came from your bank or creditor. If you enter your login information for an account from a fraudulent email, hackers will have access to your information, and therefore your account. If you think the email is real, log directly onto the company or bank's website and check your records there. You can alternatively call the company or bank to verify an issue. This way, if the email in question is a phishing scam, you know to avoid it and the company can check to see if there has been a security breach on their end and address it accordingly.

On that note, just never click a link from an unknown sender (and it's not only emails —hackers are even opening fake dating profiles these days with links in them)! You don't even have to enter a password into a fake website for hackers to get sensitive information. Sometimes, visiting a website is all you have to do to give them access to your computer. For example, some random link could automatically download a virus onto your computer, or there could be something in the code of the website that could let hackers get to your personal information. So if the email seems shady, just stay away!

There is another type of email phishing scam that's easier to spot than the first one. These types of emails typically have subject lines that convey urgency, advertise something, or even trick you into thinking the email is from someone you know with a subject line like "haven't seen you in a while!" Even just sending a reply email to these verifies your existence to the would-be scammers, so simply not replying is the way to go, because it's best that senders of these emails think you don't even exist. When you avoid opening and responding to emails that don't make sense to you or that come from people or organizations that you don't recognize, you can avoid risking an email security breach. Viruses or worms hidden in these types of emails can render your computer useless and gather your personal information for hackers to use.

Here's a little cartoon about phishing: Three fish underwater (a father and his two children) are looking at a sign attached to a hook coming down from a boat. The sign reads: "We need to verify your credit card number." The father fish is telling his offspring: "Don't take the bait. Protect your financial information."

Even if the email is from a friend, but the content looks like it might be spam, don't click on any links! Your friend might be the victim of a scam or hackers (maybe they clicked a link they shouldn't have or got tricked by a dating profile), and if hackers got into their account, they could send emails from your friend's account to their entire address book. Also, be doubly suspicious if an email ends up in your spam folder. Keeping your antivirus protection updated and turned on can also reduce your risk in this area.

Don't be too worried, though, there's a bright side! A lot of these emails are pretty easy to spot just off their bad grammar, since many spammers are overseas and have a poor command of English. So if something opens with a sentence like "if it will be kind of you, may I know your wish to write me direct with my email address at…," just chuckle at the ridiculousness and click "delete." And yes, that's the content of an actual spam message!

Don't Give Away Your Computer Along with Your Identity

Don't accidentally on-sell or give away your identity details. When you sell, donate, or throw away your computer, be sure to wipe out all of your information first, including any files or stored passwords in the browser. Ideally, you should restore it to the factory settings. This will prevent the spread of sensitive personal information, the ability of people to imitate you online, and also any embarrassing emails you forgot to delete. This is a common sense security precaution that people often forget.

Shop and Bank Online with Caution

Never, ever go to a website directly from a random email and start making purchases. Go to the site through a known and trusted URL or by searching for it on a search engine first. You can also keep a separate credit card, just for online transactions to ensure that thieves cannot infiltrate all of your finances if they have access to a single card (and so you can cancel a card if it gets infiltrated, without messing up your everyday transactions because you don't have any cards to use). This is a particularly good strategy if you have personal attendants, family, or friends who help you make purchases online. This way, they may only have access to one card, and you can keep the limit on this card low and easily track any purchases. This tip can overall protect you from a security breach online and in-person.

Use Passcodes for Your Electronic Devices

Secure your electronic devices with passcodes and be wary of what information you keep on your devices. You (hopefully) lock your doors to prevent your home from being easily burglarized, so why wouldn't you lock your devices to prevent information theft? Set a passcode on your mobile phone, tablet, and computer to keep thieves from easily accessing your information.

There is another component to the security of devices that many easily forget — it's what you keep on your devices! You obviously should not keep bank PINs and other sensitive financial information on your devices, but you should also consider what information you list in the "contacts" section of your device. When they steal phones, thieves have been known to message people who are listed as "hubby," "mom," "dad," and others with relationships disclosed in the victim's contacts, in order to gain access to bank PINs and other financial information. Sadly, this means that you probably have to get rid of all the winky faced and heart shaped emoticons next to your contact names. ☹

Don't Reveal Personal Information over the Phone

Be cautious of scammers posing as business representatives asking you to relay your Social Security number, credit card information, or bank account information over the phone. A legitimate business will never call you unsolicited and ask for this information and if you are already a customer of a business, they will request you come to the business to provide them with this information. You should always give personal financial information in person to ensure your information is going to a verified, trusted member of an organization.

Control Your Own Transactions

If you have a personal attendant, family member or friend who assists you with finances and banking transactions, it is best that you limit the amount of information they have about you. For instance, if an attendant accompanies you to your bank to withdraw money, avoid using an ATM because your attendant may have to type out your PIN number for you. Instead, go inside a bank and either have your attendant pass the bank teller your bankcard or ask a staff member for help. Then, give them your photo ID to confirm that it's you, instead of telling somebody your PIN. And let's say that you are on your own, need some cash, all the banks are closed, and you can't easily reach or use an ATM. In that case, never ask a stranger for help with your card and cash! Instead, try to find alternatives. I actually go to the grocery store and buy a $1 pack of gum, then just ask for some cash back. I still get my cash, I don't risk being robbed, and I get some gum to chew on. Win-win-win!

Depending on your disability, though, you might need help with things like entering your credit card number online or using an ATM. If that's the case, consider limiting the number of people that actively help you out (say, only have one attendant that helps you with online shopping or going to the bank). Also, always check your bank statements to make sure that things line up with your actual purchases and withdrawals. Things could be happening online, but attendants could even grab a credit card from a wallet in the middle of the night. Speaking of thieves, it's not a bad idea to keep track of the cash you have in your wallet, either. Even if you really trust somebody, it's better to be safe than sorry! We've heard plenty of stories of personal attendants and family members stealing hundreds or thousands of dollars, and the person with a disability said they had trusted them completely. One more tip: If somebody who knows your PIN or passwords no longer needs access to them to help you — say, they move away or aren't your attendant anymore — just go ahead and change the PINs on your cards and accounts. It doesn't do any harm (there's not much trouble to remembering a new PIN or password, especially after using it a couple times) but can keep you safe moving forward.

OK, so we aren't advocating looking over your shoulder and being suspicious of the folks that help you out. The good thing about this is that these are reasonable things to do either way. Double-checking your bank account transactions and making sure you have the right amount of cash covers other bases, such as identity theft, credit card theft, or some sneaky pickpocket taking cash out of your wallet.

There is just one last component to keeping your digital information safe!

Monitor Your Accounts Regularly

People who steal your banking or credit card information might not empty your account entirely. Instead, they could be making small purchases that you otherwise wouldn't notice. In their mind, that might actually be better, because they can take out more over the long run and it'll be harder to track them down! So check your credit card and bank statements (either in print or through online banking) regularly, double-check each purchase to make sure that nobody is making fraudulent transactions, and alert your bank immediately if you see anything unusual. This

actually happened to my buddy Mike a couple months ago. One day, he was double checking my bank statements and noticed that there was a $45 charge for a Metro pass for the London underground — yet he's living in California! After going through his statements, it turned out that someone in London had been buying a $45 Metro pass every month for the previous 6 months (but strangely, that's all they were buying). In total, it was almost $300, but because the thieves broke it up month-by-month, Mike didn't even notice. A bit panicked, he told his bank staff immediately. Luckily, they were able to refund him the charges and replace his credit card, which was a bit of a hassle — he had to change all of his automatic online and in-person accounts — but everything turned out OK in the end. Now, Mike checks every bank and credit card statement at the end of the month, and sometimes more often than that. No more London underground passes on his dime!

A staff member for the London subway with a huge (!) colored Mohawk

Keeping Your Information Safe While Out and About

Now that we have gone over some tips for digital security, let's go through some important tips for protecting your identity when you are out and about.

Watch out for "Shoulder Surfers"

That person behind you in line at the ATM or at the supermarket may just be another shopper, or they could be paying close attention to you in hopes of seeing your account balance or PIN. Then, if they are pickpockets and take your ATM card right afterward, they can empty your account almost immediately. So when you're doing cash transactions, shade the monitor area with your hand as you type in your PIN and try to block others' view of the screen. An audio-only option on some ATM machines that turns off the visual display is a useful security feature used by many visually impaired bank account holders. If your bank doesn't offer this ATM feature, it might make a good suggestion to make to the manager. Even if you do not have a visual impairment, you should bring a set of earphones sometime and give it a try.

Watch What You Carry

You should not carry a lot of identifying information in your wallet, purse, or phone. Avoid carrying credit/debit cards (or anything that can be used like a credit card, such as a debit card with a VISA logo) if you don't need them. If you must carry credit cards, try to carry only one, and write "See ID" next to your signature on the back. You can also change all your credit cards to a PIN only option, if possible. Don't carry extra blank checks, your passport, Social Security card, or any other ID that you are not planning to use that day. These precautions will prevent you from widespread account breaches that would occur if a thief were to get their hands on your purse or wallet. Understandably, you might need your passport and other IDs to go on vacation, but you probably don't need to carry it with you to buy produce from your local grocer.
Now that we've reviewed what to carry — and not carry — in your wallet or purse, let's go over how to carry these items safely.

Safe Transportation

Carrying your wallet or bag safely can also prevent ID and credit card theft. Most thieves are plenty skilled at reaching into bags, purses, and even pockets to swipe a wallet away. So be careful about which things you put your wallet in, and where you place them! So don't just leave your wallet or purse in a jacket or coat pocket that is hanging on the back of a cafe or restaurant chair, or even in a shopping cart while you shop. If you have a purse with long-enough straps or a cross-body style bag, wear it across your body, so it can't easily be pulled right off your shoulder by a thief. You might want to make sure your fanny pack can't be easily unsnapped from your waistline, you know, if a fanny pack fits your style. And remember that people are called pickpockets for a reason! So if you keep your wallet in a pocket, put it in the front pocket instead of the back, because it's easier to notice the thief that way.

Some folks who use wheelchairs can't carry their wallet in their pockets, because it'll be difficult to access, and keep a small bag on the side of their chairs to hold it (one of the EQUITY team members does). If that's the case, make sure that the bag is securely attached to your wheelchair and zipped up at all times. You can even get a wallet with a little ring on it, and attach it with a chain to the side of your chair or your pants' belt loop. Then, even if somebody tries to take it out, they'll have a hard time and you'll probably notice the tugging.

Having your wallet stolen is one of the more frustrating types of theft, because you have to replace everything that was in it. That means going to the DMV to get a new driver's license or

ID card, calling your health insurance provider to get a new insurance card, and of course doing the credit card deal. Some things will even be lost forever, such as any cash you had or that Ben & Jerry's gift card your grandma gave you for your birthday (and we know how much you love ice cream). On the one hand, that's one reason to keep your wallet extra secure. On the other hand, it's also a reason to limit how much you keep with you at any one time.

And remember that whole deal about not keeping passwords and other sensitive information on your cell phone? Well, pickpockets these days look around for cell phones just as much as for wallets. On the one hand, they can sell a cell phone for lots of money; on the other hand, they can go through its sensitive info to steal someone's identity and everything with it. So keep your phone secure and your eyes on it. One EQUITY team member, who uses a wheelchair, rolls around with his phone in his lap. One night, he was out with some friends in a place with low lighting, just having a good time. Then, when he went to grab his phone at the end of the night, it was completely missing! Somebody had actually reached into his lap without him noticing and took the phone right out. Use that story as a word of caution (well, a few words, if you want to be all grammatical about it). Treat your phone as you would your wallet, even if you keep it somewhere that your wallet wouldn't sit.

Of course, even if you take tons of precautions, it's impossible to completely prevent theft. So if your wallet or cell phone is stolen, tell your bank and phone company right away. Ask your bank to cancel your credit cards, or tell your phone company to remotely "kill" your phone, which makes it unusable and wipes all of the info off of it. Even if your bank is closed, you can log into your account online or call 24/7 customer service and put a hold on your credit cards until you cancel them during business hours, and some cell phone websites provide the same service. As for the cell phone bit, it's easy to hope that you'll get it back, but that's almost never the case. So unfortunately, you'll probably have to swallow that hope and kill the phone before the thieves get any sensitive info.

A warning sign saying "High risk pickpocket area"

Don't Display or Leave Personal Information in Your Car

You should never leave items openly displayed on your dashboard or car seat, because thieves might break in and try to steal them (nowadays, it's practically an invitation). It's important any time of day, too. A skilled thief doesn't have to break open your side window to get your stuff, because many can pick a lock without anybody noticing. Obvious valuables like a wallet on the dashboard should definitely be avoided, but so should be bags or anything that a thief could think might contain valuables. You might be saying to yourself, "Why should I worry if I leave a backpack with some notebooks and gym clothes in the back seat?" Well, if they break in, it's a huge pain to get a lock or window fixed. But it'll also give them the opportunity to search elsewhere, and maybe they'll find a purse or laptop in the glove compartment that'll give them personal information. And on that note, you should avoid leaving personal info in the car in the first place, because even a random break-in not inspired by a backpack could expose you to identity theft. So long story short, don't give thieves inspiration to check out your car for valuables, and don't leave personal info inside, just in case they do break in!

Another tip is to avoid leaving insurance and registration cards, garage door openers, and GPS systems with your home address (yes, those do still exist!) easily visible in your car whenever possible. There are stories of thieves using that info and devices to find someone's home, and break in when they are away. My friend Steve, who's unlucky enough to be a Chicago Cubs fan

to begin with, went to a game and parked his car in a visitor lot. Steve (who could probably get lost in his own driveway) left his GPS mounted prominently on his car dashboard. Thieves broke into the car, took the GPS and a garage door opener. They then used the GPS to find Steve's saved home address and used the garage door opener to gain entry to the house. Knowing the length of a baseball game, the thieves knew they had plenty of time to ransack the house, before he even got home. Steve no longer leaves his GPS and garage opener in clear view in his car, and even uses the address for a landmark close to his house as "home" in the GPS, so that any would-be thieves would be confused. Pretty smart for a Cubs fan!

But wait, there's even more to protecting your information! (And I know it's been a longer chapter, but we're almost done. I promise). So let's check out some things you can do at home, just in case someone breaks in.

At-Home Security

When most people think about being robbed at home, they imagine somebody breaking through a window. But somebody could steal your identity by grabbing mail out of your mailbox or even fishing through your recycling bin for billing statements. We've talked plenty about digital security for your finances, but sometimes protecting your identity at home is just as important. So check out these tips for at-home security.

Shred Any Documents with Identifying Information

It's not just raccoons that go through garbage these days. Thieves will sometimes fish through the trash as well (or if they care about their hygiene, paper recycling). So if you're not careful with what you throw away, anyone with access to your garbage or recycling bins outside of your house will also have access to your information. That's why it's important to be careful with your tossed paper documents. So shred everything! Don't just throw your old billing statements and other documents containing sensitive information into your garbage. Invest in a crosscut paper shredder and completely destroy any piece of paper that has your credit card number, your Social Security number, or your bank account number on it. Definitely shred pre-approved and other credit offers (like when they send you blank checks). Better yet, call your bank and all major credit card companies and request that they don't send those things in the first place. And if you don't have a shredder, check with your office staff or bank to use theirs.

Protect Your Snail Mail

First off, make sure that your mailbox is locked and secure. If it isn't, or if it's in an area where others can access it easily, talk to your landlord or a handyman to see if they can add some sort of lock (or even a slot in your front door). Either way, pay attention to your mail, especially if you don't have that lock yet. Check that you receive all of your billing statements on time to make sure a thief hasn't snagged them. And if they're not on time, call your bank right away to let them know. Sometimes the mail carrier accidentally puts things in other people's mailboxes, but it's a useful precaution no matter what. Most banks also offer paperless statements via email or smartphone, and those are a great way to go. If you still want a paper statement, you could just print out the digital copy at home and file it away. I actually keep a password-protected folder on

my computer with all the digital copies, which is way easier to manage than a bunch of paper — and better for the environment!

If You're a Victim

So unfortunately, no matter how much you do, there's always a chance that someone will gain access to your personal or financial information. And we all slip up every now and then. If it happens, though, acting quickly and being thorough are absolute necessities to minimize damage to your reputation and funds — and eventually build them back up to baseline. Here's what you should do, right off the bat, to make that happen.

Always Act Quickly

OK, so first off, don't panic! Having your identity stolen can be tough to deal with, but you can minimize the damage by contacting relevant financial institutions as soon as possible. Depending on what was stolen, you may need to do everything from canceling a credit card to reporting identity theft to the IRS and major credit bureaus. www.identitytheft.gov provides a list of recommendations, including what to do right away to prevent more fraud, and what to do over time to restore your funds and reputation.

Some of the immediate steps are to contact the financial institutions where the fraud occurred (for example, your bank if a credit card was stolen); place a fraud alert with the national credit bureaus and request a credit report to double-check; report identity theft to the FTC; and file a police report with your local police department. Your next steps include closing new accounts opened in your name, removing bogus charges (such as that monthly London underground pass), correcting your credit report, and considering an extended fraud alert or credit freeze. Some of these might sound drastic, and the next steps might take some time, but they are super important to prevent further damage — or giving some dude free subway rides.

Prepare Yourself for the Footwork and Effort Needed to Restore Your Reputation

Depending on your situation, reducing the damage from identity theft and restoring things to normal can take some serious time and energy. Many identity thieves actually count on people not covering all of their bases, which allows them to keep siphoning money and ruining credit going forward. So don't give them that opportunity at your expense. Invest the necessary time and energy, and be extra thorough to make sure you've really protected yourself for the future.

First off, assess your damage and the potential for more. If someone just stole your credit card, you might just need to call a bank to cancel the number and get a new card send over. But if they got your Social Security number and have opened accounts in your name, you'll need to get those accounts closed, report the identity theft to the major credit agencies and federal authorities, and put a temporary freeze on any future credit lines. A full list of steps is available at www.identitytheft.gov or in the Federal Trade Commission's Identity Theft Clearinghouse.

As you go through all of this, make sure that you keep records along the way so that you can prove that you've taken the necessary steps if someone else makes a mistake, or if you need to go back and double-check whom you contacted at some point. This includes copies of any letters you sent, details of any conversations you've had (whom you spoke to, when you spoke, and

what you talked about), and documentation of any fraudulent activity. And finally, don't just throw these records away when you think you're in the clear. Issues around identity theft can pop up months or even years later. For example, someone can hold onto your Social Security number for a while and open a new credit line a couple of years down the road. So acting quickly, being thorough, keeping records, and staying vigilant are vital to keeping your identity safe long into the future.

Published by the World Institute on Disability
3075 Adeline St., Suite 155
Berkley, CA 94703
www.wid.org

Published 2015.
Printed in the United States of America
ISBN 0-942799-09-7 (ebook)
Note: This chapter has been edited in January 2018.

Chapter 5 of EQUITY: Asset Building Strategies for People with Disabilities. A Guide to Financial Empowerment