Barclay Damon Live Presents *Cyber Sip™*
Season 5, Episode 5: "Identity Theft 101: How to Fight Back and Win Fast"

Host: Kevin Szczepanski, Barclay Damon

[Kevin Szczepanski]: Today we're going to talk about how you can protect yourself from identity theft and how what you do in the first hour, the first day, the first few days after it happens can make all the difference in the world. So let me start with a scenario. Let's make this real. We have a client. I'm going to call her Sarah. And this is what happens. Sarah gets an alert that her email password has been changed. Only Sarah didn't change it. Within 30 minutes, Sarah learns that her bank password has also been changed, a new credit card has been opened in her name, and someone attempts to redirect her paychecks to a new account. Now, in this situation, most people freeze—and then they panic. And the reason is that they don't have a plan. But for Sarah, things did not spiral out of control. Sarah had this situation under control because she took steps quickly and in the right order to protect her identity.

[Kevin]: So what we're going to talk about today is really a kind of system that I want you to have in place so that you do not suffer a loss; so that your outcome turns out the way Sarah's did. So let's talk about what you do in the first 24 hours of identity theft. There are three steps you're going to take. Step one: you're going to lock down your accounts. How are you going to do that? You're going to change your passwords immediately. And when you change those passwords, you're going to make them smart passwords. We'll get to that in a minute. But I mean every password—your Outlook or email password, your banking password, your credit cards, any financial apps you want to change your login credentials as soon as you can. That will lock out the threat actor. And when you change your password, don't use 123456 or the word "password" or names of members of your family or your pets. Your password should be anonymous to the fullest degree possible. Think about a phrase that's maybe 14 characters long and anonymize it by using large and small capital letters, symbols, numbers. It will take forever for a threat actor to crack a password like that.

[Kevin]: That's step one. Step two, you're going to check your credit immediately. You can go to a website called annualcreditreport.com. You can pull your reports. There are three credit bureaus. You can pull your Equifax, Experian, and TransUnion reports. And when you do, you want to look for a couple of things. First, accounts that you did not open. Second, hard inquiries that you don't recognize. And if you find one, or even if you don't, you're going to contact the major credit bureaus. Again, Equifax, Experian, TransUnion. And you were going to do one of two things. You're either going to implement a fraud alert or a credit freeze. That's step three. So how do you decide between a fraud alert and a credit freeze? Well, first we need to understand what they are because they're very different. A fraud alert is a kind of warning. It tells businesses that they need to check with you before they open a new credit account in your name. Usually that means contacting you to make sure the person trying to open the account is really you. And unlike a credit freeze, a fraud alert does not prevent businesses from seeing your credit report. How long does it last? It lasts a year, but you can renew it after that one year expires. How much does it cost? Nothing. It's free. A fraud alert is free, so there's no reason not to do it. And again, how do you place one? Really easy. You contact one of the three credit bureaus. You actually don't have to contact all three of them for a fraud warning. Just contact one and the credit bureau you do contact must contact the other two. So if you contact Experian, Experian must contact Equifax and TransUnion in order to complete the fraud alert.

[Kevin]: So that's all well and good, but if you're super-concerned, and you're pretty confident that your information has been accessed, and it is being used to perpetrate identity theft, you want to go beyond a fraud alert and implement a full credit freeze. Let me tell you what that entails. Unlike a fraud alert, which is simply a warning, a credit freeze is more like a lock. When a credit freeze is in place, no one, including you, can open an account in your name. If you need to do that—so you're applying for a new credit or a job, or trying to rent an apartment or buy insurance—you can temporarily lift the freeze and put it back when you're done. And here's a hint: Let's say you're applying for an apartment or insurance. You can ask the company or the insurance company what credit union they're going to run the credit check on. And if they tell you we're going to use Experian, then you only need to contact Experian and ask them to lift the credit freeze so you can leave it in place for Equifax and TransUnion. So keep that in mind. But you do need to lift it in order to do that. Now, a credit freeze is still a good idea, as inconvenient as it can be, but it's even more important if your Social Security number has been exposed in a data breach, because Social Security numbers are the keys to the kingdom. You don't want your Social Security number out there.

[Kevin]: It's just that much easier for a threat actor to apply for credit, apply for tax refunds or other funds in your name. So keep that in mind. How long does a credit freeze last? Well, unlike a fraud alert, a credit freeze lasts as long as you want it to... until you lift it. How much does it cost? Free. And the difference? Another difference between the fraud alert and a credit freeze is that unlike the fraud alert, when you only need to contact one bureau, with a credit freeze, you need to contact each of the three credit bureaus to make sure that it's in place. So we've got steps one through three. Number one, lock down your accounts. Number two, check your credit immediately. And number three, place either a fraud alert or a credit freeze on your accounts. Now we're up to step four. And that is document everything. And I don't just mean keeping notes of all the steps that you're taking, which you absolutely should do. That's going to help you remember what you did. And if you need to speak to someone, like law enforcement or an insurance carrier about what you've done, you have a record. But another important step in documentation is to contact authorities. You can go on the FBI's ic3.gov website and take five minutes to make a report of the actual or potential identity theft. You can make an identity theft report to the Federal Trade Commission at identity theft.gov. You can even contact your state attorney general or local law enforcement. Why am I asking you to do all of these things? FBI, FTC, attorney general, local law enforcement...Kevin, why do I have to do all of that? It is, as we said at the beginning here. Step four documentation. Even if federal, state or local law enforcement are unable to conduct an actual investigation of what happened you're still going to have a report that you made to those authorities. And that can come in handy if you ever have to dispute accounts opened in your name. If you have to deal with banks or insurance companies for anything having to do with identity theft. So even if you think to yourself, what is the FBI going to do here? What is the FTC going to do here? My local law enforcement says they can't do anything. Don't take no for an answer. Make those reports. They may well come in handy for you later.

[Kevin]: All right, so these are all the steps—one through four—that you need to take within the first 24 hours of an actual or potential identity theft. But once you've stabilized things, once you've done these things, what do you do next? We're going to talk about that now. First idea is monitor and expand. You want to check your bank accounts, your credit card accounts, your investment accounts. Look for anything unusual. Even small transactions. Something that doesn't make sense to you. If there's any sign of trouble or even a question, you want to contact that bank, the credit card company, your investment company, and make sure they understand you've suffered an identity theft, and you're just trying to make sure that everything is okay. Next, notify key people like your employer, your financial advisor, your insurance carrier, anyone who might be dealing with you, your identity, or funds associated with an account in your name. Just let them know that you've suffered an identity theft. They may take a report from you and make sure that they note the file and they contact you if there are any questions pertaining to your accounts. And the next step you want to take, I think is very important, and that is considering identity theft protection services. You've heard of them? Experian, LifeLock, or Identity Guard. There are many different products around, but the key difference between simply credit monitoring and identity theft protection is that credit monitoring is just going to watch what happens and tell you about it when it does.

[Kevin]: Identity protection actually helps you respond. So in a typical identity theft service, you're going to get 24/7 fraud support. You will get three-bureau credit monitoring with antivirus, VPN, spam and junk mail list removal. And this is helpful: up to $1 million in identity theft insurance, including stolen funds reimbursement. Lot of people ask me, I had one of my colleagues come up to me a couple of weeks ago and say, hey, Kevin, I got one of those postcards in the mail saying that my information might have been compromised and offering me identity theft protection. What should I do? And I'll say to you what I said to him, you should definitely do it. It's free. It's an extra layer of protection. And there is absolutely no reason not to do it. Even if you don't get one of those postcards, you can get identity theft protection out in the market for as little as $10 a month. To me identity theft protection is a no brainer. Yes. It's going to cost you maybe ten bucks a month, maybe a little bit more. Some are more expensive, but balance that cost of $120 to $240 a year. I know that's not nothing to a lot of us, but balance that against the risk that someone's going to steal your name, your Social Security number, your financial account information, and then start stealing funds or opening accounts in your name. The risk far outweighs the cost. So I highly recommend it. Get identity theft protection today.

[Kevin]: All right. Now let's pivot a little bit. We talked about what you should do in the first hour, the first 24 hours, the first few days. Let's talk about why these things happen. Because that's going to be our gateway to prevention. Why do you suffer from identity theft? Well, one of the major reasons that you do is that you and I reuse the same passwords. And that means that if someone steals your password for one account, they may very well have your password for all of your other accounts. What do you do about that? One thing I would highly recommend is using a password manager. Don't reuse your passwords. Do you know what a password manager is?

[Kevin]: It's software. It helps us create strong passwords, store them in a digital vault that is protected by a strong master password. And then retrieve your passwords as you need them for your various accounts. It's a great idea these days. Many people will say, well, Kevin, is that foolproof? Couldn't a password manager be hacked as well? Sure. But it's still a strong measure of protection. And if you're looking to maximize your internet safety, I would seriously consider using a password manager. How else do we become susceptible to identity theft? Well, phishing emails and they're increasingly sophisticated. It used to be that you could tell by the language that was used, that the email wasn't coming from the United States, and that it was suspicious. Well, today, threat actors are using AI to create the perfect phishing emails. They're also using AI and other techniques to create text or smishing emails based on the SMS or text platform. And I can assure you that if you're getting a text from the US Postal Service telling you to input your login credentials, or if you get a text from the Department of Motor Vehicles telling you you need to log on and pay a fine immediately, or else your license will be suspended, those texts aren't legitimate. The DMV does not text you when you owe money, and the US Postal Service does not text you when you missed a package. You're going to get those communications another way, and even if you think it's legitimate, don't respond to the text.

[Kevin]: Contact the DMV or the US Postal Service using trusted contact information. And then you can ask about that supposed fine or that mail you didn't receive. Just need to be a lot more careful than we typically are, because the world is not the safe place that it was when we were all younger. One final thought: If your email gets compromised and this can happen. Once your email gets compromised, everything else can follow. So you want to protect your email like it's your front door. Don't click on something that you don't expect, don't open an attachment that you're not expecting. And even if you are expecting it, just take a minute or two to contact the sender using trusted contact information and say, hey, I just got this email. Did you mean to send this link to me or did you mean to send this attachment to me? More often than not, they may say no, I didn't. Please don't click. Don't open it. And if you follow that simple practice, take just an extra minute out of your day. You can avoid identity theft in that way as well. So how do we conclude this? Here's the bottom line. Identity theft is not something that happens to other people anymore.

[Kevin]: It's fast. It's automated, and it's everywhere. But the difference between a minor inconvenience and a major financial problem is simple. Do you have a plan? Do you know what you will do in the first hour after you discover identity theft? Do you know what you will do in the first day or in the first few days? If you do, I promise you, you will be infinitely safer than you are today. You will be able to manage the risk of identity theft, and you will be able to rest assured that you're doing everything you can to protect your family, your financial accounts, and your data. If you have any questions about this, or you have comments about anything I've said, hit me up in the comments. Otherwise, thank you so much for joining us. We'll be back soon with another episode of *Cyber Sip*. Take care.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, and Spotify. Like, follow, share, and continue to listen.