Barclay Damon Live Presents *Cyber Sip*™
Season 3, Episode 12: "Identity Theft: What to Do When You're a Victim"

Host: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Hey, everyone. Welcome back to *Cyber Sip*. You know, I have been hearing from a lot of clients and friends about how they have suffered identity theft, so I thought it would be a perfect time to talk about identity theft, what it is, how it happens, how common it is, so, you don't feel badly when it happens to you because it really is just a matter of time. It's happened to me, and I'm going to give you the top ten tips from our Barclay Damon Identity Theft Playbook that you can implement when you suffer identity theft. So let's begin. Let's dive right in. Begin with the question that you may have, which is what is identity theft? And I would say, generally speaking, it's when someone takes your information, name and address and some more personal information like an email address, driver's license number, Social Security number, and uses it to impersonate you for the purpose of obtaining credit, benefits or other funds in your name. That's identity theft in a nutshell. Someone's pretending to be you in order to get money in your name. And because we're talking about credit most often, it can be perilous because you can find yourself in debt for credit that you never applied for. How does someone get your personal information? Well, they can do it by... when you click on a malicious link, and you enter that information for them. You could accidentally download malware, which would give a threat actor access to your computer system where he can troll about and find that personal information or... and we all are increasingly you could be the victim of a data breach and we just saw report this week in Security Week July 17, Rite Aid announces that a hack impacted 2.2 million of its customers. So you and I could have our data stolen and we don't even know it because it's stolen by virtue of our being a customer of a large business to which we have provided our personal information for good reason. How common is identity theft? And here is where I think some of us are reluctant to report it or take action because it's embarrassing.

[Kevin]: We are afraid to report it because we think we did something foolish, stupid. And the reality is, is that according to the website, Identity Theft dot org, identity theft occurs once every 22 seconds. So it is happening almost three times a minute. One in three Americans has reported identity theft in their lifetime. And I think the key figure there is... the key term there is reported, because you and I both know that more people have suffered identity theft than have reported it. And it's a big business. In 2022 alone, that's the last year for which we have FBI statistics, there were 5 million reported fraud and identity theft cases. That's reported cases. Estimated losses of $10.2 billion. That's billion with a B, and that was up by about 70% from the previous reported year 2021, where we saw a $6.9 billion in reported fraud and identity theft. So it happens to you and me because it's a big business. Threat actors know that they can gain access to information, yours and mine, and then use it to obtain credit or other funds. So what do you do when you're the victim of identity theft? I'm going to walk through some... ten steps that you can take to protect yourself when you suffer identity theft.

[Kevin]: And by the way, I want to tell you that these steps come from the Barclay Damon Identity Theft Playbook, which was patented by my partner Nick DeCesare, who is our lead breach coach here and if you don't have access to our playbook, you can hit me up in the comments, but you can also go to one or both of the following sites. They provide excellent material. Much of the material you're going to hear today comes from these websites. So let me give them to you now. They're both Federal Trade Commission websites. The

first is identity theft dot gov, and it walks through in a great way. What do you do right away? What do you do later? And we're going to talk about those steps today. And the second website is FTC dot gov slash identity theft. So if you have not yet suffered identity theft, it's a great idea, I think, to visit those websites. It'll give you ten or 15 minutes of what I think is an invaluable read. And then in the unlikely event or maybe the likely event that you do or someone you know suffers identity theft, someday you'll know where to go.

[Kevin]: You can also come to this episode of *Cyber Sip* and watch it over. Watch it a few times. Forward it to your friends. I can't tell you how many times friends of the firm, clients of the firm will come to us. They're going through…they're shell shocked and they're not sure what to do. So I think preparation is invaluable and I think we all need to get our ducks in a row when it comes to identity theft before it happens. All right. So enough said about that. Without further ado, let's run through top ten tips. Tip number one if you find that you are the victim of fraud with a particular company, you're going to call the companies where you know the fraud occurred. You might have to contact them again after you complete an FTC report, which we'll talk about in a minute. But you're going to call the companies, you're going to ask for the fraud department. You're going to explain that someone stole your identity. You're not responsible for the purchases or the credit that appears on… in your name. You're going to ask them to close or freeze the accounts. And then if they do that, no one can add new charges unless you agree. This is a very important first step.

[Kevin]: And then once you do that, you're going to change your login, your password, and any PIN you have for those particular company accounts. Tip number two, you're going to place a fraud alert and get your credit reports. So when you have an alert on your credit report, a business has to verify who you are before it issues new credit in your name. So very important to place a fraud alert. You're essentially going to have that alert on your account for one year. And if you're not comfortable with just a year, you can actually purchase or place an extended fraud alert on your account, which lasts up to seven years. You can take that alert off at any time. But critical that you place one as soon as possible to prevent others from using that credit in your name.

[Kevin]: Tip number three and this is an important one. You report the identity theft to the FTC. It's very simple to do and very important. All you have to do is go to the website Identity Theft dot gov report your identity theft to the FTC and the website will create what's called an identity theft report that you can use with law enforcement. You can use with the credit bureaus, you can use with any potential debtors who may not yet understand that you have been the victim of identity theft. So it's a very easy and very important report because it proves to businesses that someone stole your identity. And then, as I mentioned, you can take that identity theft report and use it to make a report to local law enforcement.

[Kevin]: Now, a lot of people will ask me, Kevin, should I report this to the local police? Or they might come in and say, now, I already reported it to the local police and they told me they can't do anything. Well, even if they can't do anything, even if they can't undo the identity theft, the one thing they can do is create a police report. And that police report is just as valuable—"belt and suspenders"—as the identity theft report you're going to get from the FTC. So say, for example, in a month or six months, you get a letter from a creditor saying, you owe me $1,000 based on this credit card that was issued in your name. At that point, you can contact the creditor back. You can submit your identity theft report, your police report, and explain using those documents, talk about documentation later as well, that you are an identity theft victim. And those charges should therefore be reversed, and your credit should not be affected. All right. Next tip, tip number four. Correct your credit report. I don't know if you knew you could do this, but if someone steals your identity, you have the legal right to remove fraudulent information from your credit report. You just… you can do it. And there's a name for it. It's called "blocking." And once the information is blocked by the credit bureau, it won't show up on your credit report. And companies cannot try to collect a debt from you. If you have an FTC identity theft report, which we discussed just a few moments ago, the credit bureaus must honor your request to block that information.

[Kevin]: So it's very important to take that affirmative step to correct your credit report once you discover identity theft. On to tip number five, consider adding an extended fraud alert or credit freeze. Now, there's a

difference between a credit freeze and an extended fraud alert. The two main differences—so in the case of a credit freeze, the credit freeze limits access to your credit report unless and until you lift or remove that freeze and it lasts just as long as it takes for you to lift or remove it. So what's the difference between a credit freeze and an extended fraud alert? Well, in the case of an extended fraud alert, there are two more bells and whistles that I think are invaluable. Number one, if you have an extended fraud alert in place, then a company must contact you before granting any new credit in your name. So the credit freeze limits access to your credit report. But the extended fraud alert gives you that extra measure of protection. You know that no one's going to issue any more credit in your name without first contacting you. And second, unlike the credit freeze, which lasts until you lift or remove it, the extended fraud alert lasts for seven years. So an extra measure of protection, which we recommend.

[Kevin]: And in case you're wondering, well, if I have this extended fraud alert on my account and I'm applying for an auto loan or a home loan, how do I get it lifted so that it doesn't interfere with my ability to get legitimate credit? And the answer to that is when you set up, whatever it is, credit freeze or an extended fraud alert, you will receive a PIN and you can use that PIN in order to temporarily lift the freeze or the fraud alert for the purpose of getting credit, after which you can place it back on. So you have to be a little bit careful about that. And if you have any questions about how that works, you can hit me up in the comments, but that's the way you get around the problem of having a freeze or a fraud alert in place. All right, on to tip number six. Let's say your identity theft involves your Social Security number or your driver's license number.

[Kevin]: And in many cases, it does. In fact, I have to tell you, I, I don't have my Social Security card. Of course I have it...my Social Security number committed to memory. But I'm in the process of getting a new Social Security card. And you can do that, too. So when it comes to a Social Security number, know that you can go online and you can report a misused Social Security number. And if you want to prevent... you're thinking, oh, no, what if someone uses my Social Security number to try to get employment? Because that happens. In order to prevent someone from doing that, you can go online and set up an e-verify account so you can lock your Social Security number. And when... how does that help you? When someone tries to use a locked Social Security number to get a job, an employer must get more information from the applicant before they can take the next step. So that is intended to offer you an extra measure of protection on the notion that anyone who is not really you is not going to have the extra information needed to take those next steps and enter into a phony employment relationship. In addition to that, you can also apply for a replacement Social Security card if you need that, and if your driver's license number has been misused, you can contact your local DMV.

[Kevin]: Unlike your Social Security number, you typically cannot fix your driver's license card on the Internet or online, but you can go online, find contact information for your local DMV office, and you can go to that office and make arrangements there. Something I highly recommend. All right. Now we're on to tip number seven, and that is what do you do when you're in a situation where someone has stolen your identity, they've gotten credit in your name, and you don't find out about it until they are...they've used that credit to go into debt. And the debt collector, the debt collection firm or the retail store, whatever it is, is coming after you for the payment. Well, here's what you can do. First, you want to write to the debt collector or the business within 30 days after getting a collection letter. You would then want to contact the business where the fraudulent account was opened. If you haven't already, you want to ask the credit bureaus to block information about this debt from your credit report, and you want to provide them the identity theft report you received from FTC and the police report that you obtained when you reported this matter to the police. So this isn't necessarily a step you need to take right away. You only need to do it if you find out that the threat actor misused your identity in order to get credit in your name and has stuck you with the bill. But believe me, by thinking about these steps ahead of time and knowing what you need to do, you'll be giving yourself the peace of mind and the process, the roadmap that you need to address these issues when they happen.

[Kevin]: All right. So we are on to tip number eight. You've suffered identity theft and you're thinking what can I do to protect myself? What can I do to increase my information security safeguards? And here's something we recommend to everyone. First, you want to change all of your login and password information on your computer, on every account that you have, even the accounts that have not been affected because you don't want to find out when it's too late that yet another account has been compromised as a result of identity theft. So change those logins and passwords. And when you do, make sure that you use a smart password, it should not be "password123" or "1234567." You want to have a good, smart password. And if you want to know how to create one, I've got a video on just that subject or you can hit me up in the comments and we can talk about how to anonymize a password that will take hundreds if not thousands of years to crack.

[Kevin]: Number two, you want to implement multifactor authentication, which is sometimes called two-factor authentication. So some people think the two-factor authentication is login and password. That's not. That's single factor authentication. You want to add a second layer of authentication, which typically requires something you have. Maybe a token, something you know, a PIN or something you are: Your biometric information. In most cases, you can set up multifactor authentication for your personal computer, for your online accounts. It's available to you. But in many, many cases it is not the default option. So when you discover identity theft, you want to contact all of your financial companies, all of the online companies with which you're doing business and enable multifactor authentication. Finally, it's a perfect time for you to close any inactive or unnecessary accounts. We all have them. These are accounts you've had for years. You haven't used them. You're not going to use them. Get rid of them because a closed or inactive account is just as likely to create an opportunity for identity theft as an active account is. Why? Because it's got your information just like the active accounts do. So you want to close those accounts.

[Kevin]: Tip number nine: Consider identity theft protection. What do I mean by that? Well, you know the names: LifeLock, Aura, Experian, Identity Guard. There are more identity theft protection firms today than there ever have been before. Some of you might say, well, if I'm doing all of these other things that you're mentioning, Kevin, why do I need an identity theft protection firm? And you might be right, but we're finding increasingly that our clients find the extra measure of protection comforting and more effective in protecting their identities. Why? Because a typical identity theft protection firm is going to give you not only credit monitoring, but identity theft monitoring. So at the first sign of suspicious activity, you're going to know about it and have the opportunity to approve or reject the transaction. Most good identity theft programs offer $1,000,000 of identity theft protection, and many of them are known for their customer service. So you've got a dedicated representative that is going to help you walk through all the steps that we're talking about so you don't have to do it alone. For that reason we recommend it. You don't have to do it. But the key takeaway is comparison shop and find the firm that works best for you. And tip number ten, last tip for what you do when you're a victim of identity theft: Keep detailed notes and documentation. Everything you do, write down who you spoke to, when, what the subject was. If it's generated a document like an identity theft report, a police report, whatever it is, you want to keep a record of it. Why? Well, first of all, if you have to explain to a credit bureau or a business that you've suffered identity theft, you'll have the documentation to prove it. If you have insurance, you will need that documentation in order to qualify for the insurance you have in place.

[Kevin]: And having that paperwork will not only enable you to document whatever claim you may have under an insurance policy, it will make it a lot easier for you to communicate with the credit bureaus, federal and local law enforcement, and any debt collectors you might encounter along the way. So if you have suffered identity theft, don't feel guilty, don't feel like you did anything wrong because we've all suffered from it. I suffered from it myself. I lost over $4,000. Fortunately, I got it back because I was able to work closely with my credit union, but they didn't want to give it all back. And if I had had better documentation and I knew better what to do, the process would have been a lot smoother. So those are my top ten tips for what to do when you're a victim of identity theft. I hope you find it helpful. If you have any questions, you've had a bad experience or you have some ideas of how we might be able to do all this a little bit better. Hit me up in the comments, please like, comment and share and we'll be back soon with another episode of *Cyber Sip*.

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

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied.

Barclay Damon Live *podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of* Barclay Damon Live *programming is the audio file. Thanks for listening.*