Help! My Domain Name Was Stolen (And 3 Ways to Recover It) - With David Weslow

Watch the full video at:
http://www.domainsherpa.com/david-weslow-domain-theft/

On this show we tell you exactly what you can do if your domain name is stolen. AND…what could happen if you buy a stolen domain name. Sherpa Network, today's show is an important one.

I have three sponsor messages before we get into today's show.

First, if you're buying or selling a domain name or portfolio and you want an estimate of it's value, Estibot.com is the place to go. Just like you'd visit Zillow.com to get an estimate of a house value, Estibot.com provides key information about the most important statistics so you can make an informed decision based on data.

Second, whether you are buying, selling, brokering or financing a domain name you need an escrow company that is properly licensed, bonded, insured and audited. That company is Escrow.com and they have been doing it since 1999. Escrow.com – it's about trust.

Finally, are you tired of being up-sold and cross-sold when you buy or renew a domain? Then try the newest registrar being built from the ground-up with a beautiful interface, competitive pricing and 24/7 support. Uniregistry.com will surprise and delight you. The right domain name can change your life: Uniregistry.com.

Michael Cyger: Hey everyone. My name is Michael Cyger, and I'm the Publisher of DomainSherpa.com - the website where you come to learn how to become a successful domain name investor and entrepreneur directly from the experts. It seems like we cannot go a month without hearing about some sort of online theft. Whether it is hackers stealing millions of MasterCard and Visa credit card numbers directly from those organization or cyber attacks from other countries targeting technologies or pharmaceutical companies, hacking is on the rise, and the costs of operating businesses are growing too

in clean up of hacked information, security software and protocols, and additional employees.

The domain industry is not sheltered. Wherever you have something of value to others, you are going to have theft. If you have a domain name stolen, you may find yourself alone. You may think you are alone in trying to deal with it. Your registrar may disclaim all liability, your local law enforcement agency does not know how to even handle a cyber crime, and you are left feeling like there is no one to turn to.

Today we are joined by a past Sherpa, David Weslow, a partner and attorney at Wiley Ryan, who specializes in domain name and intellectual property law and has successfully handled domain name theft recovery, and he is going to explain exactly what you can do and how to do it. David, welcome back to the show.

David Weslow: Hi Michael. Thanks for having me back.

Michael: My pleasure. I want to start this interview by asking a bit of a personal question, David. I hope you do not mind. I notice you got a little bit of a shiner on your left eye there. Is one of your kids taking mixed martial arts and caught you unexpected with a right hook?

David: I wish it was something that interesting. It was me playing soccer and a little bit of a collision. And hitting the ball is no longer allowed for kids below a certain age, and I learned that maybe hitting the ball should not be allowed for people over a particular age as well.

Michael: That must have hurt, because that is a pretty fragile area to be headed by somebody with a thick head no less.

David: It is on the mend, so not too bad right now.

Michael: All right. Well, I think it is more endearing to have an attorney that is willing to throw blows and heads as the case may be in soccer, so you get my vote.

David: I appreciate that.

Michael: Usual spiel before I get into this show, which I do not do on all my other shows. Although David is a practicing attorney and we will be discussing legal topics in this show, you should not take anything said during this show as specific legal advice for your situation. Every situation is different. Every domain name is different. Everything is different. So, you need to contact an attorney for your specific case. This show is meant to educate you on all of the major aspects related to domain name theft, how to protect yourself, how to prevent a domain name from being stolen, and then your options for recovering it once it is - hopefully never - stolen.

David, it is sad to admit, but if I lost most of my investment domains, I probably would not even notice them gone. Why is domain theft such a big deal?

David: It is interesting, Michael. As you said at the outset, I really think it is indicative of increased hacking across the board. So, you gave some great examples here on a weekly basis of credit databases being hacked, eCommerce sites being hacked, and you are exactly right. Where there is something of value, there are people on parts of the Internet and places around the world that want to steal it. They have discovered the value of domain names, much like others. So, particularly where you have got domain names of value, there will be attempts to steal them through hacking, just as with any other type of database. Whether it is credit card database or personal information database, or anything else that is accessible online, there are going to be those people that try and steal them.

Michael: Yeah. And so, what is an example of a domain name theft that you have dealt with recently that highlights this situation?

David: Yeah, as you have mentioned, I have handled a number of cases recently, both in court and that have been resolved short of going to court. One was fairly high profile. It involved nine three-letter and number .COM names. The domain name owner woke up one morning to a notice from his registrar that the names had been transferred to a new account. By the time he

contacted the registrar, they had then been transferred from his account to another account and then out of that account to another registrar.

The registrar happened to be in China. The losing registrar tried pretty hard to get them back, but the gaining registrar in China would not cooperate. Really left us with no choice but to go to court and pursue a court order that the domain names be returned. We ultimately got that court order and the registry and registrar were very cooperative in returning those names.

Michael: Nice, so you were able to successfully return those domains.

David: That is right.

Michael: We have talked on Domain Sherpa about the value of domain names and we talk about it in DN Academy as well. LLL, three-letter domain names like ABC.com. Well, not that one exactly. Like XQW as well as three numbers. Those are high-value domain names usually in the tens of thousands, sometimes even in the hundreds of thousands, or if it is a word in the millions because they are so short. So, those short ones have a liquid value that people can immediately. If nobody knows it is stolen, they could immediately get tens of thousands of dollars for it. That is the real drive here. Those short numerics and acronym-type domain names.

David: Yeah, that is exactly right. I think those are the most common, though any domain name is susceptible to theft. And we have also seen premium generics or category terms that are being used by eCommerce sites, for example, being stolen and sometimes even being held for hostage or ransom for a payment to have them returned because of course when the name is stolen, that shuts down the eCommerce site, but you are right. The most frequent names that I have seen being stolen are those short numeric, short few letter names that are very often stolen, transferred, and then sometimes flipped pretty quickly to subsequent sellers.

Michael: Yeah, so you bring up an example like an operating business, whether it is online and eCommerce business or just a consulting business, where customers are coming there and they need to do email. You lose your domain name. You lose not only your website access. Maybe documents that

is stored on the server. Access to those documents as well as all the emails that are coming in. And somebody that steals the domain name could put a catchall on for every single email and then look through them.

So, it is not just stealing the asset. Not just making the asset unavailable for use in the business, but also proprietary information might be revealed by looking at it. So, tremendously important that domain names are not stolen in a lot of different cases.

David: That is right, and yeah, you raise a great point about the ability to configure the name to receive inbound email traffic in particular. There have been cases where domain names have been stolen. They have been configured in that way for the purpose of stealing the other intellectual property, so the trade secrets of the company or the know-how of the company because they are then in that position to receive all of the inbound email traffic as well as everything else you just mentioned.

Michael: Yeah. All right, so in this interview, we are going to tackle two main objects. First, we are going to talk about six best management practices that our audience can do today to prevent a domain name theft. And then, once we get through those six best management practices, we are going to talk about if a theft happens, three things a domain owner can do to get the domain back, to recover the domain name.

All right, and I want to make it clear. We are not going to talk about just good management practices, like putting your domain name in your name as the WhoIS registrant and making sure your domain name is in your registrant account at your registrar versus your webmaster. We are not going to tell you things like make sure it is on auto-renew so it does not expire. Those are all straightforward, common sense practices that I would hope everybody would know. We are going to focus on domain name theft, how to prevent that theft and then how to recover a domain name once it has been stolen. So, that is the purpose of this interview.

So, let's get into the six ways to prevent domain name theft. Number one is secure passwords. David, what is an insecure password?

David: Password. I think the word itself is the most patritional, most insecure password.

Michael: I think it is the number one password ever used around the world. Password.

David: That is right, and the easiest to guess. So, obviously you want to make it a complex password. Uppercase. Lowercase. Different characters. Ideally not a word. A lot of this, a lot of the cases where people come to me, the password is something that can be guessed or the password has some relation to the WhoIS data that is out there, and we are going to talk about that as well, but you want it to be something that is not going to be easy to guess, it is not going to be easy to crack, and it is also not going to be easy to social engineer if someone were to try and trick you into giving out the password or trick your registrar into giving them access.

Michael: Yeah, and a lot of people will tell me. Well, I have heard a couple of people tell me yeah, my domain registrar account at so and so - GoDaddy or whatever - was hacked, and I said well, did they guess your password. Was it a real word? And they were like yeah, it was a real word. So, that brute force type of hacking. It cannot be done when you are using a complex password with numbers, symbols, capital letters, lower letter, not a real world, a mix of different characters, and there are simple programs out there.

For 30 bucks, you can buy a program that integrates with Chrome that uses encryption that allows you to store every single password up to 15 characters mixed together. I use 1Password. I know plenty of people have used other software programs like LastPass that worked just the same way. So, it is easy to do that. It is syncs up over the cloud with your phone, all encrypted. Definitely something you should invest in. Get secure passwords. Number one.

Number two is multi-factor authentication. What is multi-factor authentication, David?

David: All right, so you are in essence going to be requiring some second or even a third step so that a transfer of the name requires that additional step.

Different registrars have different options, but there has got to be something other than just the login and the password. So, that could be a text message for confirmation. It could be an additional password. It could be a secret answer. It could be a phone authorization. There are lots of different ways to achieve it, but the concept is there has got to be some additional step beyond mere that login and password.

Michael: Yeah, and that is an important one. And I know I mainly use GoDaddy and it texts me a six-digit number every single time I try to sign in to my account, and then I have to enter in that number. Uniregistry I think uses Authi, which is on my phone, so somebody has to have my phone in their possession and then get into my phone in order to view those. So, there are authenticators out there.

So, that is the multi-factor or two-factor authentication. Some other independent way. And I also know at Uniregistry, when I try and push a domain name from my account to somebody else's, after I am already signed in, it will ask me for my password again to initiate the push. So, those are the kinds of things that you want to look for as a domain name investor or domain name entrepreneur with valuable domain names. You want to make sure that you are using a registrar that has these kinds of multi-factor authentication processes in place.

David: Yeah, that is absolutely right. And occasionally I hear from people well, that slows things down or makes it more complicated, but you really do have to weigh that against the risks. And as you alluded to, theft is rampant. I get a call I would say at least once a week of someone who has had a domain name stolen, so you just have to weigh that risk against yeah, it may slow things down or occasionally be a bit of an annoyance, but it is really giving you the protection you need in the current environment.

Michael: Yeah, that is amazing. Once a week, and you are just one attorney out how many attorneys in the world that specialize in intellectual and domain name law?

David: Fair amount.

Michael: You are the best, right, David. I am sure you get the lion share of all of the calls, but yeah, that is amazing. Okay, so that is number two. Number three is email monitoring and protection. Why is email necessary for maintaining domain name security?

David: So, as we will talk about when we get into the nuts and bolts of how some of thefts actually happen, reputable registrars will trigger an email to you when there are changes. They will absolutely send you an email when there is a transfer out to another registrar. Some registrars will also send you an email when there is a push to another account or what is called an intra-registrar account transfer. So, that is how you learn about that there has been some transfer of your names, and the earlier you learn about it, the better position your registrar is going to be in to help you out and to do the work for you and to keep that name from transferring or to get it back. So, it is really important to make sure that you are reachable so that you can learn when something happens.

Michael: Yeah, so you want to use pretty much your main email address not necessarily on the WhoIS of the domain names you own, but for the account information at your registrars, right? You do not want to use an email address that you only check once a month or once a quarter that you use for your promotions and coupons and things like that where somebody requires you to sign up. You want to use the one that you are checking every morning when you wake up on your phone and in the middle of the day when you are taking a break or whatever. You want to make sure that if somebody is sending you a notice for a domain name that you own at the registrar that you get it and see it as soon as possible.

David: Yeah, that is right. I have been on the phone with people who have discovered their name has been stolen because it is an eCommerce site and the site is down, or if they are an investor, they have gone to sell the name and it turns out that it is no longer in their account. And as we talk through the issue, we will talk through well, how did you not receive notice and very often it is that there was an obscure email address on file. The person will login to that account and there will be all these notices showing that there was pending transfers or account changes. So, that is right. It is really

important that you are going to get those notices because you are in a much better position to stop it the sooner you learn about it.

Michael: Yeah, so that is the email address associated with your registrar account, like a GoDaddy or a Uniregistry. It is not necessarily the address that is public information on your WhoIS domain. So, that is number three for email monitoring and protection. Number four is phishing. What is phishing and what can happen with it, David?

David: Right, so we have all gotten these emails that could be generic spam or they could have links in them, or there is some attempt. Basically phishing is some attempt to obtain personal information from you. A lot of times it could look like an email from your registrar. It could be the WhoIS verification email, where you hover over the link, you see it is actually going to another page, or there could be some other link or some other offer. What these emails are, are attempts to get your personal information or some small piece of information that lets them ultimately socially social engineer their way into your account.

So, one email may pick up one piece of information. Another email may get another piece of information. So, you really want to be careful about emails coming in to you. Be careful about what links you click on and make sure you know who it is you are dealing with so that you are not giving up information by itself, or when pieced together with others could be used for someone to gain access to your accounts.

Michael: Yeah, great advice, and I know that I have received emails while I am out and about from GoDaddy, where some of my domains are, and the phishing emails purportedly from GoDaddy and those were phishing emails asking me to sign into my account and verify my information or something like that. And when you are on your phone, you cannot hover over a link like you can when you are on your browser on your laptop or your desktop. So, I recommend if you get the email and it looks like it is phishing and you cannot quite tell if it is real, then wait until you get back to your laptop. If it is an email saying a domain was just transferred, clearly that is something you do not want to wait on. You can call your registrar directly right then.

And even once when I tried to like press on the link in order just to see where it was going to go to, the browser on my phone just automatically went there. So, be careful when you are on your phone. Do not click on the links because clicking on them logs it on the phishing site's website as well. They know who is clicking on them, that the email got through, that you clicked on it, and that it is a valid email address, so be careful about those emails coming in.

One thing that I appreciate about Escrow.com emails, because they are financially related with escrow going on, is that they never put a link in their emails, so you physically have to go to a browser and type in Escrow.com and then sign in. So, that is one way that they prevent those types of issues from occurring related to their business.

So, number four is phishing. Let's go to number five. The fifth way to prevent domain name theft: WhoIS privacy protection. What is WhoIS privacy protection, David, and how can it help?

David: Sure, so privacy or a proxy service can either conceal your information or substitute the service provider's contact information for your so that your personal information remains confidential. It can be a good idea so that you are taking one other piece of information that might be used by someone who is going to steal or try to get into your account and steal your domains. Your address, your phone number, etc. will not be posted.

With one caveat. I do think it is important that if you use a privacy or proxy service, it is a reputable service that you can count on that any communications will come through to you. You will be reachable. I generally do not recommend using third party services that have no relationship to the registrar or that may be offshore somewhere or where you are not one hundred percent confident that all communications are going to come through to you. But assuming you find a service provider that you trust, it can be worthwhile to consider using that so that you are keeping those additional pieces of information private. It takes one other thing off the table in terms of how thieves might try to gain access to your account.

Michael: So, I understand instead of having Michael@DomainSherpa.com listed as public WhoIS information associated with my domain name, DomainSherpa.com, I might have it at Uniregistry using privacy and it might be Privacy-Link with a number at Uniregistry.com. So, then if a phishing company sees that, one, they may not try and email me because they can determine that it is under privacy, but if they send a phishing email through that email, it is still going to come to me, right?

David: That is right, and I think theirs is a great service so that the Uniregistry privacy service you know that you are going to receive any communications. I believe there is a specifically identified email address that is unique to you so that that is what you should be looking for. You will receive emails, but what you have done is, by using their privacy service, your address is not published, so that is one data point that the thief does not have. So, if they are going to try and gain access to your account, they do not know your physical address or they do not know your phone number or your actual email, so they cannot use that to try and build their profile of you or to try and guess. Do you have your street address as part of your password? It is just something else that you are taking away from them.

Michael: Got it. Makes sense. All right, so that is the fifth way to prevent theft. And the final and sixth way are what we call locks, both at the registry and registrar level. What are these locks, David, and how can they help?

David: So, both the registries and registrars provide additional locks that prevent the names from being transferred. You can have a registrar lock that is an additional step. Sometimes some registrars require you to pay an additional fee. There are also registry locks that prevent changes in the registry record, often for an additional fee, but that is another level of security. It can be another step, but again, if you are talking about your most valuable domain names or the name that is used for your business, it makes a lot of sense to incur that small, additional step to give yourself another level of security.

Michael: Yeah. So, for example, if I was operating a business that was making multi-million, tens of millions, or hundreds of millions of dollars, I could actually go to VeriSign, who is the registry for .COM, and pay them an

extra fee. I think it is probably on the order of a few hundred dollars per year. I cannot remember the exact number. And they will lock it down at the registry level. So, even if somebody gets into my GoDaddy account or my NameCheap account and tries to transfer it, VeriSign will not allow it to transfer. Is that correct?

David: That is right, and the same could be true with the registrar lock or an additional lock at the registrar level.

Michael: Now, if you are a domain investor and you have value domain names that you are looking to sell, that could be a pain to try and manage through when somebody really wants the domain name quickly or you want to close the deal quickly.

David: Yeah, it certainly could be, and I think with the list of the six items you have just walked through, the idea is that it may not make sense in any particular circumstance to use all six, but these are options that are out there for people to review and to implement where it makes sense. And you may decide, looking at well, I have implemented five of these. The sixth - the registrar or the registry lock - really is not necessary because I feel comfortable, I have done everything else, and that may make sense. In another case, you may decide not to use privacy service because you are comfortable that you followed all the other steps, but you really want to be reachable and it is important for you to show that you are the owner of that name, and that may make sense in that particular instance.

Michael: Yeah, and that is a great example and that is actually what I do with all of my domains. I want to show that they are available. People want to look me up that way in the telephone directory, the WhoIS directory of domain names that they can find me. The one that I will throw out personally on that registrar lock is that some of my domains are at GoDaddy, and because I have over four hundred domains there, they set me up with a premiere account and they use a service called Domain Transfer Verification Service (DTVS), where if I try to push or push a domain to another account holder at GoDaddy or transfer a domain name out of GoDaddy to another registrar that they will prevent that happening until somebody calls me on the phone on a phone number that I have specified and I give them a special passcode that

allows them to transfer the domain name out. So, that is one that they provide at no charge, but you have to have a certain number of domain names at the registrar for them to offer you that service.

And I find it to be tremendously valuable. I wish most other registrars would do something like that as well because I know it gives me a high probability that the domain name is never going to be stolen. A high assurance that the domain name will never be stolen.

David: That is right.

Michael: So, those are the six ways to prevent domain name theft. Secure passwords. Multi-factor authentication. Email monitoring and making sure you are using an email address that you use all the time. Preventing phishing attacks. WhoIS privacy protection in the appropriate cases. And then locking the domain at either the registrar or the registry. So, six ways there, David.

Now, David, International Corporation of Assigned Names and Numbers (ICANN), the organization that is responsible for how domain names are implemented around the world, has tried to stop domain name theft by mandating a 60-day lock. I am not sure if it has another name. I know most people just refer to it as the 60-day lock. What is that lock?

David: Yeah, the rules are that once a name is transferred between registrars or the registrant field is changed, there is a mandatory lock the registrar has to impose against further transfers. So, that is what is required under the rules. 60-day lock if there is a registrar transfer or a change of the registrant. Now, different registrars add on to that rule and interpret it a little bit differently, so you will encounter different practices if you change the address field or if you make a change to the registrant name that is not necessarily viewed as changing the registrant. You will encounter different practices and different registrars, most typically in relation to account changes and how those are treated.

Some registrars will treat an account change as a transfer of the registrant that requires the 60-day lock. Other will not. It will depend on what is in the WhoIS record when the name actually is changed.

Michael: So, why 60 days? What is that supposed to prevent?

David: The idea I think was to give everyone enough notice and to prevent the flipping of the names to a series of subsequent purchasers and to cut down on really the laundering of stolen names. And it does limit the ability of a thief to continue to transfer the name. Now, of course thieves can be pretty creative, so my experience they are constantly looking at those differences in the practices, particularly on account changes and how different registrars treat account changes or push transfers so that they can get the name away from a reputable registrar in as few steps as possible.

Quick break from three sponsors of today's show:

First, if you're buying a domain name from a private party and want to know what else they own, DomainIQ.com is the tool you should be using. View their entire portfolio, filter by Estibot value and be a better investor. $49.95 for 250 queries per month. Visit DomainIQ.com/portfolio to learn more.

Second, Efty was built by domain investors to increase your inquiries, sales and profit. Forget spreadsheets and archived emails — manage your entire investment portfolio in one place using a secure and completely confidential platform. Learn more at Efty.com, that's e – f – t – y, Efty.com.

Finally, If you're struggling with how to buy, sell, and value domain names, you need to check-out DNAcademy.com. Published by me, Michael Cyger of DomainSherpa, and trusted by Uniregistry to train their new employees, you too can learn using the DNAcademy accelerated learning system for domain name investing. Learn more at DNAcademy.com.

Michael: Yeah, those thieves are wiley. So, in preparation for this interview, I wanted to understand what leading registrars are doing to try and protect those of us who have a lot of domain names at their companies. I personally use GoDaddy and Uniregistry. I think they have great management teams in place, and so I wanted to dig in. If I go to their website and say what is your policy for this or that, you may not find it, so I reached out to their staff and I asked them because I think one of the wiley ways, one of the creative ways

that domain thieves have figured their way around is that they will go into somebody's account, they will push the domain name to another account, so nothing is changed on the registrant, but it is in somebody else's control, and then they will transfer it out or maybe they will change the information once it is there.

But anyways. Being able to push it was one of the holes that they found in the system from account to account at the same registrar. So, I reached out to GoDaddy and they said that they notify the losing account holder whenever a push between accounts happens, and they lock the domain name for ten days. All right, so it is much like the 60-day lock. They are going to send you an email because the domain just left your account and they are going to lock it for ten days to make sure that you see that email and you can address it if there is an issue.

Similarly, at Uniregistry, they are implementing some systems in place. They do notify the losing account holder as well and they are implementing a transfer lock on those domain names as well. I do not have an exact period of time for which the domain is locked, but they are implementing that right now.

So, those are important things to know, David. I think a lot of people think that every registrar operates the same way, but have you seen that in your practice?

David: Yeah, it is wildly different between registrars, and those steps that you just mentioned really are best practices for registrars that they all should implement. As you said, this is a loophole that thieves are exploiting and continue to exploit pretty regularly. It makes a lot of sense to me for registrars to implement some kind of lock, even on an account transfer or push transfer, but there are many that do not that once it is into a new account, you are right. That is the way that the name is then transferred out, particularly to a registrar that may be less reachable and that is not going to be very cooperative in sending the name back.

Michael: Yeah, and it just occurred to me. You push the domain name to another account. You change the DNS. You put in a catchall for the email

address. You update the information. You get the email. You approve the transfer out. The process is a lot easier once it is in their control.

So, I bring this up because I want to make it clear to people that are watching this show that not every registrar operates exactly the same way. We look at them and say well, I register a domain name. I point my DNS where I want it to go. I renew the domain name. That is all I am really concerned about. But that is not all you should be concerned about. You should be concerned about their policies and practices in place in protecting your valuable assets, these domain names. So, ask them. If you are not sure what their policy is, send an email to support at the registrar that you are using and ask them what their policy is around locking domain names that are pushed between accounts and find out. And if it is not up to par, think about one of the two domain name registrars that I just mentioned.

All right, so those are the six ways to prevent a domain name from being stolen, but let's say that something happened. A theft is discovered. You may notice that you are not receiving emails like you used to or the website may not resolve or the landing page that you are using may not resolve. The WhoIS information might be different. There are three things you can do to recover the domain name.

Number one is called registrar retrieval. What is that, David?

David: The first and best thing to do when you discover a name is stolen is contact your registrar. They may have a particular form they want you to fill out. They may ask you to submit your driver's license or other pieces of information to verify who you are, but your registrar really is in the best position to either stop the transfer if it is in progress or to negotiating with gaining registrar to have the name come back.

Now, if everything is above board, you are the legitimate owner of the domain name, you submit the documentation and you have got a reputable registrar, they actually can be pretty successful in having the name returned assuming that gaining registrar is also reputable and really willing to work with them. Now, my experiences the last few weeks to a month, in a number of cases it may take some time. A week to two weeks, but the registrar very

often can have the name sent back, where it is clear that it has been stolen. So, that is the best. First option is to reach out to the registrar and really give them all the documentation they want to see if they can help you out.

Michael: And how should you reach out to the registrar? Is it as simple as just going on the website and looking for a support telephone number or an email address?

David: Yeah, I would start with support. Actually some of the registrars do now have dedicated domain theft teams, so if you go in through the regular support line, they may give you a particular email address or put you in contact with a team of specialists who are accustomed to dealing with domain name theft issues, and they are really used to that process of working with the gaining registrar to try and figure out who the rightful owner is. But in the first instance, going through to support and really advocating they are your registrar. You are their paying customer. Really advocate that they help you out as best they can.

Michael: So, should I feel pretty confident that I have got 60 days from the point that the domain was stolen? So, if I go do a WhoIS lookup and I see that the domain name was lasted updated five days ago and I contact my registrar today and they start to look at it, should I feel pretty confident that I have 55 days in order to get this resolved before it goes some place else?

David: Yeah, that is a tough question because in the instance let's say it is an account transfer within your registrar and then from the second account it goes out to another registrar, and that registrar does not have a hold period on account transfers, which many particularly based in China do not, when the domain name arrives at that gaining registrar in China, it may be sold again and again through account transfers within that registrar. So, you may still be within that 60-day lock period, where it cannot go from that gaining registrar to another registrar, but it could be sold over and over again within that registrar.

Michael: And then just pushed from account to account within the same registrar, and we often see that. If you go to a discussion forum or you go to Flippa, it says the domain name is at. And not to point out that these two

locations are doing anything not reputable, but it will say the domain name is at this certain registrar and the transfer will happen by push because they may have updated the account information and that is the only way that they can actually sell the domain name and it might actually be legal.

David: That is right.

Michael: Yeah. Once you contact your registrar and you provide the documentation and you ask them to retrieve it and they start their investigation, is there any sort of lock that they can put on the domain name or is it only if the current registrar, the one that received the domain name agrees to do that?

David: Yeah, really depends on where it is in the process. If has already gone out, if it has left your registrar, then they are not in a position to add a lock at that point. Now, the gaining registrar, if they are being cooperative, they certainly can implement a transfer lock so that they could actually stop the subsequent transfers through push transfers within their registrar, and that is absolutely a good idea to ask for while your registrar, the losing registrar, is working with them. That gaining registrar should implement a lock while the two registrars are trying to figure out who the rightful owner is.

Michael: I understand. So, if I get an email saying that a domain name is being pushed from my account to another account at the same registrar and I call up support and say hey, hold up. I have got an issue with this. They may actually lock it at that registrar until they can resolve it. But if it is already transferred out and the gaining registrar has it and they do not want to cooperate, then it could actually continue on down the line.

David: Yeah, that is right, and that is where you get into the situation we will talk about your legal options. But where you have got a gaining registrar that is not willing to cooperate, then you really have no choice but to pursue legal action.

Michael: Okay, and so we are talking about these three ways to recover the domain name, and they are pretty much in this order that you should pursue them. So, number one is the registrar retrieval. It is just reaching out to the

registrar and asking them for their support. It does not cost you anything except for your time to do it. And knowing that if it is currently at the same registrar, you can ask them to lock it, and if it has already gone out to another registrar, you can ask them to lock it and maybe that gaining registrar will lock it until it is investigated and hopefully returned back to you, but if not, then we need to go down the next path, which is the legal one.

So, number two. The second way to try and recover the domain name is to actually file a uniform dispute resolution policy (UDRP). What do you call it? You file a UDRP case I guess.

David: So, it is an administrative proceeding. Also, there is a registrar transfer dispute resolution policy, but that policy does not allow for you, as the domain name owner, to file an administrative proceeding. So, that policy is part of how your registrar would interact with the gaining registrar and ultimately your registrar actually has the ability under that policy to file a complaint with the registry or even to file its own administrative proceeding, but that is what is going on behind the scenes under step one when you are advocating that your registrar do what it can to try and get the name returned.

If they do not have success in having the name returned, as the domain name owner, you are not in a position to invoke that policy. That is only available for registrars. So, you then could consider the uniform dispute domain name resolution policy that you have had lots of shows on, Michael. Traditionally, the policy was created to address cybersquatting, which is use of a domain name to exploit someone else's trademark with bad faith in brief. The UDRP in certain circumstances has been successfully invoked to allow for the return of a domain name that has been stolen, but there have also been panelists that have said this kind of this is really outside of the scope of the policy. The policy is only intended to deal with cybersquatting. This is not cybersquatting.

So, it is really going to be case specific. The first hurdle is going to be were you using the domain name in a way that qualifies for trademark rights. If so, then it is worth considering because the second element of the UDRP is lack of rights or legitimate interests. Someone has stolen the name. You should be able to show they do not have any rights or legitimate interest. The third

element would be whether or not they have registered and used the domain name in bad faith. So, if they have stolen it, you have got a good argument there as well.

The challenge is going to be, again, some UDRP panelists will just say outright although this is wrong what has happened, it is outside of the scope of the policy. You could also run into issues where the name has been sold to someone else. You have got someone who could appear and defend the UDRP and say I did not know. I paid good money. This happens all the time. They are the second purchaser. The third purchaser. They had no idea that the name was stolen, in which case this is a dispute over the title of the domain name. Clearly that is going to be outside the scope of the UDRP. Panelists probably is not going to want to get into that dispute. The result would be the panelists saying you really need to take this to court.

Michael: Yeah. All right, but if, for example, somebody got into my account and stole DomainSherpa.com, I have a trademark on it. I can file a UDRP and immediately, as soon as a UDRP is entered, that locks the domain name so that it cannot further transfer or change ownership. Is that true?

David: Yeah, that is right. So, it is absolutely necessary. It is worth considering because you are right. If you can file quickly enough under the UDRP rules as they were updated last summer, you file with the service provider. The service provider notices or gives notice to the registrar and the registrar then locks it in place even before that UDRP complaint is sent to the new owner. So, that is a good option in that scenario because you can lock it, and if you have got the original thief and you have got a trademark, you may be able to invoke the UDRP. Clearly the UDRP is going to be less expensive than the next option, so it is worth considering.

Michael: And will it actually prevent? Will that lock from a filed UDRP actually prevent the domain name from being pushed from one account to another account?

David: It should.

Michael: It should, yeah. Okay. All right, so that is the UDRP. The first one is the registrar retrieval. If that does not work and you have a trademark, you can make an argument for a UDRP and try to lock it and get it back that way. Clearly you need a trademark. It likely cannot be a common law trademark. It needs to be a filed trademark with USPTO or a similar type of government institution in another country, right, David?

David: Well, the same rule would apply to any UDRP. You could theoretically establish common law rights. You just would need to establish them. They would need to provide sufficient evidence to the UDRP panel. So, for common law rights, you are typically talking about sales figures, marketing figures, and things to show the way you use the name really did rise to a level of an unregistered common law trademark. So, that is going to be case specific. If the name was not used as an eCommerce site or in the trademark context, if it was just an investment name, that may be an issue because, again, when it is not a registered trademark for UDRP purposes, you really do need to establish through evidence that you are entitled to trademark rights.

Michael: Yeah, okay, so that is the second way to try and retrieve a domain name that has been stolen. And the third and final way down this ladder of increasing cost and resources is a court action. What would you actually do in that case, David?

David: Right, so you would file typically a U.S. federal lawsuit. Depending on the way the names were used, you have a couple different federal laws that you could invoke. Again, if the names were used in a way that gave rise to trademark rights, either registered or unregistered, you could file under the U.S. Federal Anti-Cybersquatting Consumer Protection Act. Whether or not you have got trademark rights, you can also invoke the U.S. Federal Computer Fraud and Abuse Act because in the vast majority of these cases there has been some hacking, either into your email address that then allowed them to gain access to your registrar account or a hacking directly into your registrar account. So, that action of gaining unauthorized access to a protected computer and then causing injury is a violation of the Computer Fraud and Abuse Act.

There are other laws state specific that can be invoked. Conversion is possible and other things along those lines. There are a number of legal grounds that you can use to pursue a transfer order from the court. Now, ultimately it is really going to depend on is there a live person that you can identify as the thief or do you need to file what is called a John Doe action or even an in rem property action asking solely for a court order that the names be returned. So, there are a lot of variables depending on how the theft was undertaken and how the domain name has been used since the theft, but there are absolutely legal claims that particularly U.S. Federal Courts are willing to entertain, and I have had multiple cases where judges will order the return of stolen domain names.

Michael: And so, most of the highest value domain names use the top-level domain of .COM. And the registry for .COM is VeriSign, which is located in the United States. Will a court order to return a .COM domain name actually happen because VeriSign is located in the U.S. even if the current registrant, the thief or the person that is in control of the domain name is outside the U.S.? Will that work?

David: Yeah, that is right. So, U.S. Federal law allows for an in rem action in the location of the registry or the registrar, so you are right. VeriSign is here, just outside of Washington D.C., in Northern Virginia, so .COM and .NET domain names can be subject to a court order and an in rem or property action from the Federal Court, Northern Virginia. Same thing for .ORG. Public Interest Registry (PIR) is also in Northern Virginia. NewStar for .BIZ is also there. That particular Federal Court has handled the vast majority of domain name cases over the last 15 years.

So, that court can issue an order directing the registry to implement the change. And because then that is implemented at the registry level, you are over the registrars. It does not matter whether or not the registrar is non-cooperative. It is going to be a registry-level change. They will move the domain name to the registrar that you ask the court to specify, and then that registrar then changes the WhoIS information - at least that is how it works for a .COM and .NET - back. The registrar then changes the information back to you as the lawful owner.

Michael: And is true, like the UDRP, where the domain name is locked as soon as you file that action? In a court action, can you also lock the domain name from further transfers or account changes?

David: Yeah, that is right. So, generally, once you file the lawsuit, your lawyer that files it for you will reach out to the registry or the registrar to let them know that court action has been filed and to ask them to implement either a registry-level or a registrar-level lock. The vast majority of registries and registrars will do that voluntarily. If not, you can ask the court to order the registry or the registrar to do that, and courts readily issue those types of orders.

Michael: Okay. And so, I know somebody that may be watching this, thinking I just had my domain stolen. I am going to read the transcript. Figure out what my options are. But at the end of the day, it comes down to dollars and cents. Does it make sense to actually pursue one of these options? Assuming that the owner of the domain name that had the domain name stolen from them has a trademark and wants to go down the UDRP path, what would be an order of magnitude cost associated with pursuing that with an attorney so that you make sure it is done right, because if the domain name is only worth say ten thousand dollars to them, it is a hard pill to swallow, but it may cost them ten thousand dollars to try and recover it?

David: Yeah, that is right. So, a UDRP action, the filing fee is going to be in the ballpark of 15 hundred dollars depending on the administrative service provider that you use. You could probably count on for a reputable attorney's fees a multiple of that by a few times at least. Particularly if you are talking about a common law or unregistered trademark, you are going to have to put in a lot of evidence because you need to satisfy that standard. You cannot file and just include a statement that I own a trademark. That is not going to satisfy the test. So, there is a fair amount of work there.

Going to Federal Court, you do not have that high filing fee to file a lawsuit in Federal Court. It is only a few hundred dollars, but you are obviously looking at a lot more work. A UDRP is a single filing with the opportunity potentially for a supplemental filing. If the case is defended in Federal Court, you are going to have to establish to the court's satisfaction that you are

entitled to the relief. Many Federal Courts insist on hearings in person, particularly in Northern Virginia, the court that hears a lot of these cases. They will want to see your lawyer. They will want to talk through all of the allegations, so there are going to be hearings. It is a decent amount of legwork. So, I cannot give you a fee range because it is going to highly case specific, but obviously it is going to Federal Court. It is not an inexpensive endeavor and you do really need to weigh what that is going to cost versus the value of the names that have been lost.

The case you and I talked about at the outset. Nine three-letter .COMs that were stolen. Obviously the value there of those names, it makes sense to go to court and get an order and get them returned. I have had other cases. A three-number .COM, where it was the name of an eCommerce site. Makes sense there. You have to go to court to get that returned because otherwise you are out of business.

Michael: Yeah. So, just from an order of magnitude perspective, UDRPs are probably going to cost you around ten thousand dollars all in. Maybe it is 20 thousand. Maybe it is eight thousand. It is an order of magnitude. Is that fair, David? I do not want to pigeonhole any lawyer into that.

David: I think that is a fair estimate, sure.

Michael: And it is probably going to be for a court case that requires going to court and going through all of that, that you just mentioned is probably going to be tens of thousands of dollars.

David: Yeah, that is right. When it goes to court, it really comes down to whether or not the case is defended. If it is a domain theft case, it might be decided by default. Might not be defended, in which case it is much more efficient. But again, if you have got a stolen name that has been flipped over and over again and there is someone out there that has paid a lot of money and did not realize it was stolen, that is going to complicate the case.

Michael: Yeah, all right, so I am going to ask you about that, and we are coming close to an hour point, so I just want to summarize. Those are the three ways you can get your stolen domain name back. Number one is the

registrar retrieval. Call up the registrar. Tell them the domain name was stolen. Get transferred to their specialist that deals with this. Provide them the information. Ask them to lock it down if it is at the current registrar. Ask them to lock it down if it is at a gaining registrar and maybe they will work with them, but that is your first, cheapest option and fastest option.

Number two is if you have a trademark, to go the UDRP route. Make the argument. Get it locked. Try and get it back that way. Talk to a lawyer in that case because it is going to have a lot of different factors that are specific to your case.

And then the final way is a court action. It is going to cost you the most. It may be settled quickly, but if the current registrar tries to defend it for any reason, then it could go up. But clearly in that first case, those domain names were probably worth half a million or more dollars. It is going to make sense to defend it and try and retrieve those back for 30, 40, 50 thousand dollars because that is half a million liquid, like today. And if they held on to them long-term, it could be two million dollars worth of domain names.

So, you brought up a great point, David. If my domain name is stolen, moved to another account, transferred out to another country, and then sold from that thief to some unsuspecting domain name registrant, some other person that just thought it was a great domain name and wanted to invest in the domain name, buy it or whatever, they are buying stolen property. They did not know that. I know that if I go to a pawn shop and I buy a stolen watch, for example, paid good money not knowing and they find out it was stolen, it can be taken away from me and I am out my money that I paid for it, and I have to then go try and recover my money from the pawn shop who sold me stolen goods. Is that similar case in domain names?

David: Yeah, that is a great analogy. It is not dissimilar with the important caveat that there are not that many domain name court rulings addressing title involving stolen domains and there is some disagreement particularly from courts in different parts of the country applying different state's laws and viewpoints on what a domain name is, but I would say the more common position of courts would be that if the domain name is stolen, not unlike your pawn shop example, there can never be valid title to be passed in any

subsequent purchasers. Even if the subsequent purchaser has paid a lot of money and had no idea that it was stolen, the title can never be valid because it was stolen.

So, that is the more common view, but by no means is it universal. So, what that means, how that translates practically is if you are in this situation, you clearly want to think about taking action sooner rather than later so that you can stop the potential for those subsequent purchases because while you would still have a legal claim and you might ultimately win, again, because there can be no valid title that is transferred, it is clearly going to complicate it and you do not want other people to be out their money, not knowing that it is a stolen domain name.

Michael: Yeah, great advice. And for those that do not understand the UDRP process, David has been on the show multiple times in the past, talking about that. I suggest you click on David's profile down below this interview. You can watch his other interviews as well, where he talks about the UDRP. And I have also done a program on due diligence. If you are buying high-value domain names, it is upon you. It is your responsibility to go look and make sure that the WhoIS history of that domain name shows that the person who is selling it has the right and the title to sell it. If it is recently changed, over the past few days, that could be an indication that the domain name could have been stolen and may not be the rightful property of the person who is selling it.

David, you have provided some phenomenal information here. If somebody has watched this show and they want to contact you to discuss their specific situation about a domain name that might have been stolen or was stolen, what is the best way that they can contact you?

David: Sure, the easiest way is DavidWeslow.com, which redirects to my law firm, WileyRyan.com's website. My contact information is there. All of my background information, including information about cases in this area that I have handled.

Michael: Great. And if somebody has a domain name stolen, I would probably be freaking out. Should I call you or should I email you?

David: Either is fine. I am happy to talk to people. As I mentioned, I get a lot of calls and I am happy to talk to people even when it is not going to result in me needing to take the case because, again, if there is a way that you can encourage your registrar to help out or otherwise negotiate to get the name back, I think that that is a win-win for everyone, so I am happy to talk to anyone if the situation arises.

Michael: Fantastic.

David Weslow, Partner and Attorney at Wiley Ryan. Thanks for coming on the Domain Sherpa Show, explaining how to prevent and then recover a domain name if you could not prevent it in time from theft, and thanks for being a return Domain Sherpa.

David: Thanks, Michael, for having me once again. I appreciate it.

Michael: Thank you all for watching. We'll see you next time.

Watch the full video at:
http://www.domainsherpa.com/david-weslow-domain-theft/