Bill: Okay. Brett, I want to welcome you into the show.

Brett: Hey, thank you for having me. I appreciate it.

Bill: So this is going to be a fun one for everybody. I think this is... so, we're in a very interesting world today. And I think, I told the story recently, this is a company we're working with today, that is actually a sub company. We're working with the parent company and this [00:00:30] is a sister company that's recently acquired, but it's big. It's a 2,000-person company. And so they know, the parent company didn't just shove the security team onto them and say, "They are the new security." Like, there's a lot of politics and so, we weren't essentially representing them, although the parent company really wanted us to. Well, it just so happens that this company, this sub-company now is 2,000 users completely haven't been able to work for a week due to [00:01:00] ransomware compacting-

Brett: Gee.

Bill: Taking down the entire business.

Brett: So, 2,000, 2000.

Bill: 2,000, yeah. And so, this is the significant business outage, and so, I think we're at this point where businesses are being taken down, hospitals are being taken down. And I want to talk about your unique expertise, which was developed in this amazing way over time and maybe we could start with your [00:01:30] story and what do you do today? And let's talk about what got you there?

Brett: Sure. So let's talk about what I do today because as you know, Bill, I tell the story a lot, I do. Today, I'm a public speaker. I keynote a lot of conferences. I'm also a consultant. Now, what do I consult with? I consult regarding cybersecurity, cybercrime identity and theft. I'm highly regarded, at least as [00:02:00] a good guy. I was highly regarded as a bad guy. I mean, the way I got my experience was not really from a book. It was from being hands on the United States Secret Service. They call me the Original Internet Godfather and I was recording my podcast last night. And I said that and it got me. I sat there for a second and I just paused. I was like, "Man, think about that for a second."

Bill: Let's put that in the frame of what year did that come out where the South Carolina made [00:02:30] that statement? What year was that?

Brett: That was 2005.

Bill: 2005.

Brett: 2005.

Bill: So, essentially, you built an essential first dark web, where essentially replicated with the Godfather. We've done kind of physically and kinetically and metaphorically in New York, Philly, Boston, you did that online?

Brett: Yeah. What happens is before, the group that I built is called ShadowCrew.

Bill: ShadowCrew.

Brett: [00:03:00] As you mentioned, it was called, it was precursor to today's Darknet and Darknet markets. It kind of, well, it not kind of, it did lay the foundation for the way modern cybercrime channels still operate today. And the way it works is, before ShadowCrew, there's actually three websites: There's Counterfeit Library, ShadowCrew, and CarderPlanet. CarderPlanet was run by a guy named Dmitry Golubov, Ukrainian national. I ran and built both Counterfeit Library and ShadowCrew, me and two other guys did. [00:03:30] What happens is, is if you're looking at engaging in cybercrime before those two websites come up, the only real avenue you had to do that was an IRC chat session, because rolling chat board, you didn't really know who you were talking to. If you could trust them, if you could buy an item from them, whatever. So, you were getting ripped off all the time. Anybody could come on there and claim they had anything and you had no idea.

What ShadowCrew did was it provided a trust mechanism that criminals could [00:04:00] use. So, now you had a large communication channel, a forum. You had a forum, all of a sudden, that people from different time zones could engage in conversations. They could learn from conversations. They could talk with somebody that had posted something a month ago or three weeks ago or three years ago. You knew by looking at someone's screen name what the person's skill level was. If you could trust them, if you could learn from them, if you could network with them. We had vouchers in place and you mentioned it a second ago, if [00:04:30] we bounce back then, it's pretty much the same now, but it was based on that type of gangster vouch that you see in The Godfather movies. Someone vouches for you. If I vouch for you that means-

Bill: Social proof?

Brett: Yeah.

Bill: It's like a social proof.

Brett: Absolutely. I take complete responsibility for you when I vouch for you. If you go off and you rip someone off, if you steal money from another user, it's my responsibility to make that complete for you. All right? That's the seriousness we took with it. We had escrow [00:05:00] systems in place. We had all these things in place, so that a criminal, who doesn't know another criminal, who will never see or know the real name of another criminal on the other side of the planet can engage with that person and trust that person because what you're dealing with, with cybercrime, three things have to take place for that crime to succeed.

You have to gather data. You steal the PII. The bank accounts, the credit card numbers, whatever, so you gather the data, then you have to commit the crime with that gathered data, with that [00:05:30] stolen data. So, you have to hit the merchant or retailer for the MacBook Pros, you have to file claims with the unemployment office, since this is COVID-19 year or whatever that crime is. And then finally, you have to put cash in pocket. So, you gather data, commit a crime and cash it out. And I'm no different. The problem with that is, is that a single criminal, he's not good at all three things. He's good in one thing, sometimes two, very rarely all three. And that's why you see [00:06:00] these forums, these marketplaces, these dark web and surface web groups, they exist so that that one specific criminal can network with other criminals who are good in areas where that one guy is not. And that's the basis of what we see today with cybercrime channels.

Bill: So, it said, you essentially partnered with other folks that had different skill sets, so we often say, well, one of the ways [00:06:30] that a hack can happen is someone clicks on a link, it infects the server, and then it's quietly there and there, someone in another area of the world then sees that there's an outbound, there's a heartbeat there, and then establishes a remote connection. Okay, but that's just one skill, that's just one skill. And it's a very technical skill and essentially, you could create essentially a botnet of these listeners waiting for heartbeats to open up in a corporate network. But then what happens next?

Brett: [00:07:00] Well, think of it, we have mentioned ransomware a couple of moments ago, right?

Bill: Right.

Brett: So, you've got someone who builds a ransomware. They coat it and everything else like that. Now, as that person, now, he's very good about doing that. That falls into the gathering data area that you-

Bill: Sure, sure.

Brett: You've got a product. All right. Can he deploy the product? Maybe not, maybe not. He can build the hell out of the product...

Bill: Got you, yeah.

Brett: ... but he may not be able to deploy, so he has to rely on someone else to deploy it, so a good social engineer. [00:07:30] Some of us may be using Unicode domains or maybe he's coming in and maybe drops the thumb stick out of the parking lot or whatever that is. Maybe the router, because we've got 41% of all routers on the planet have the default password, maybe the router is compromised. Whatever that may be, I don't know. All right? But you rely on that second guy to do that.

Now, ransomware exists so that criminals can profit. If they can't profit by that at the end of the day, why even build it, why even try to deploy [00:08:00] it? So what's the chance of person A or person B, knowing how to launder money? Maybe not, maybe not. That's why we see in a lot of cybercrime channels now, you have somebody that is able to steal, get wired out $3, $4 million to a bank account that he has set up, all right, but they can't cash it out in time, just because it's wired out of one account into another, it doesn't mean that you've stolen that much. That means that you've just got that much wired out. You need to know how [00:08:30] to do that properly, how to get the money out quickly and effectively and anonymously. So, you rely on a bunch of money mules or laundering mechanisms that are already part of that platform of whatever cybersecurity group or cybercrime group that you're a part of.

Bill: Okay, so that's really interesting, so you not only have the technical skills to build the piece of malware, but then you have the social skills to [00:09:00] either withdraw from USPs or somehow social engineer looking at LinkedIn or whatever that may be. And then you have the financial, not just the financial skills, but you have to know the mechanisms to move money within, it seems like a big part of this is anonymity.

Brett: It is. You have to remain secret. And let me give you another example. And Lord knows, I've talked about this a lot in my presentations. Do you want me to talk about Tesco or you want me to talk about unemployment? You tell me.

Bill: Well, unemployment. We can talk about elections, too.

Brett: We can talk about elections, [00:09:30] too because I complain a lot these days. So, unemployment, for example, the Nigerians hit Washington State for a billion dollars. Okay?

Bill: A billion, okay.

Brett: A billion dollars in unemployment fraud, so how does that happen from the bad guy's side? Well, the way it happens from the bad guy's side is the Nigerians, first, we have to realize that cybercrime is not rocket science. It's not sophisticated. We have this perception that attackers are really sophisticated computer geniuses, they're not. More of them are just social engineers. Now, that doesn't mean that you [00:10:00] don't have a lot of highly capable attackers out there that understand computer systems and understand those high-level attacks, but you don't need a lot of them. All right? You just hit a few of them because of the way the system works.

So, unemployment works, because that fraud was successful, because the Nigerians, they said to themselves, they had an idea. They were like, "I wonder if you could file fake unemployment claims?" So, they tested it. Now, they already had the information [00:10:30] because everyone's information, everyone's PII is already compromised. Just look at the year before last, we had 1,500 just reported breaches. Of those 1,500 just reported, 2.6 billion records compromised, just then, and that's on a yearly basis, we see numbers like that. So, everyone's information is already available, so they had the data. Okay? They had gathered the information.

How do you commit the crime? Well, it turns out that the only thing it took to file for those benefits was someone's social, [00:11:00] the name and address and a phone number. That was it. As long as you inputted that in, if no one else had already filed for that individual, you were getting those benefits. So, the Nigerians, they test it, they see that it's not only successful, but wildly successful, so they start following the claims. Now, here's where the failure happens. They actually get a billion dollars wired out to Nigerian banks, a billion dollars. Now, did they get to keep a billion dollars? No, they [00:11:30] didn't because I guess they didn't expect that level of success. All right? They got to keep $200 million, but they lost $800 million because they couldn't get it out of the bank in time.

That's what you see all the time. You talk about business email compromise, it's extremely easy and that's a social engineering attack. Extremely easy to trick a payroll department and switching banking information, maybe get a couple of million dollars wired out to bank account. That doesn't mean that you get to keep that money. That means that you [00:12:00] had it wired out. All right? That's what typically attackers, they're more concentrated on committing the crime, and not following it through to the end game. And the end game, if you can't put the money in your pocket that becomes a problem. And I'm fortunate enough, I get to speak at Quantico twice a year these days, but the FBI as far as reclaiming business email compromise funds, it's about 85% successful in that. And it's highly effective and it's simply because criminals don't [00:12:30] follow through the end game.

They don't really look at it. They're more concentrated on stealing the money and don't realize that just because you get the money sent out, it doesn't mean you profit anything at all and that boils down to what we're talking about of understanding these three compartments, these three necessities of cybercrime. Each one of them have their own import there, so it's very important that you gather data, that the data is valid. It's very important that when you're gathering the data, that you're not [00:13:00] identified. Same thing with committing the crime. You want to be anonymous with that. And then finally, cashing out if you can't put the cash in the pocket, if you can't do it without being identified, look at all these idiots that are using Bitcoin, so if you can't do it without being identified, what's the point?

Bill: Yeah, and I think or you finding that the anonymity on the Bitcoin side is probably a lot better than just wire transfer of U.S. cash, correct?

Brett: It is. So, you can move massive amounts [00:13:30] of value with cryptocurrency, right?

Bill: Yeah.

Brett: And if you're using Monero or one of these anonymous coins, at least they used to be anonymous, if you're using one of those, it's very difficult to track it, especially if the criminal has any understanding of the way that Blockchain works at all. We're seeing now, there's been a lot of effort recently, from security companies and global law enforcement to be able to track those anonymous crypto tokens, specifically [00:14:00] Monero. There's been a lot of headway that's been made in that. All those coins are short lived as far as anonymity goes right now.

Bill: Okay. Yeah. I fear it's only a matter of time before those crypto keys are going to be compromised with law enforcement, so a big part of your story is you're not just coming into this from an academic approach or graduated from college with a degree in [00:14:30] Computer Science. You came at it from some dark places and were very successful on the other side. Maybe you can talk about when did you first get exposed to criminal behavior versus "I'm going to go mow 10 lawns and make $50 per lawn or $10 per lawn" as a child. You were exposed to some of this early on. Maybe you could talk a little bit about that?

Brett: Sure. I'm from East [00:15:00] Kentucky. I mean, that's part, that's the start right there. I'm from Eastern Kentucky. Eastern Kentucky, it's kind of like one of these areas of the panhandle of Florida, parts of Louisiana that is very poor. It's very poor. If you're not fortunate enough to have a job, you may be on the government draw, you may be involved with some sort of scam, hustle, fraud, whatever. My mom, and I say this, and she calls me, I guess last month, six weeks ago, cussing me out because [00:15:30] she had finally after four years, she finally sits down and listens to one of my presentations, so she calls me up. I mean, threatening to kill me, everything else. My mom was basically the captain of the entire fraud industry, and I mean, no crime, too big or too small. This is a woman who at one point, she steals a 108,000-pound Caterpillar D9 bulldozer.

Bill: That's a huge machine.

Brett: It's huge. It's gigantic. [00:16:00] All right? She steals this thing. Another point, she takes a slip and fall in a convenience store. She tries to sue the owner. We had a neighbor, she used to pimp out. This is my mom. My dad was not like that. My dad, honestly, my dad was a good guy. He was, and in Eastern Kentucky, it's hard to get away from that type of hustle or criminal mentality because of the poverty levels, so my dad had that in him, but he was a good man. I mean, he would work hard. This man would work hard, [00:16:30] just trying to provide for family. My dad's problem was is he loved my mom so much, that he became the enabler in this relationship.

Bill: He enabled, yeah.

Brett: So, it was if she came up with an idea to commit a crime or whatever, he would support it. If she wanted to abuse people, me and my sister or him, he would let it happen and she was abusive. I mean, she could be physical and she was physical. She was physical up until the point, I don't think I talked about that in my podcast or maybe Denise did, but Denise, [00:17:00] she was beating Denise with the buckle of a belt. Denise, for no reason, no reason and Denise caught the belt and kicked her and kicked her through a closet.

Bill: Wow.

Brett: And that was the last time that mom ever touched us physically at that point. Like I said, she could be physical, but where she excelled and abused was with the mental, the verbal, the negligence, all that and [00:17:30] she used to bring men home in front of my dad. And my dad would sit there and just beg her, "Carolyn, please stop. Don't do that. Don't do that." And he'd cry and she would do it anyway, and she finally leaves him. We were in Panama City, Florida at that point. I told you my dad worked hard. My dad was working at that point as a midnight clerk for 7/11. He was making $140 a week, it was what this man was making.

Bill: Wow.

Brett: And she leaves him. We moved from Panama City. Me, my sister [00:18:00] and my mom moved from Panama City back to Hazard, Kentucky and she was a nurse, but she never really worked as a nurse. She would work long enough to see whatever man she was seeing off of work and she'd go out and party, and she kept up with those party anyways, so she would leave. I was 10, my sister Denise was nine. She'd go out and party and she'd leaves us at home for days at a time sometimes and she used to tell us, she used to look at us and say she'd [00:18:30] given up her life for us, that she was going to leave and not come back one day that we'd find her dead in a ditch or behind a building someplace. And that was my mom. So, when you're a kid, Billy, you take that shit serious.

Bill: Yeah.

Brett: But you do. You take that serious. When your parent tells you, so I think that's what a lot of people don't understand is when you're a child, you want to believe in anything your parents says, so.

Bill: They're your God.

Brett: Yeah, they are. They are.

Bill: They represent [00:19:00] the be all and end all and so, for sure.

Brett: I was a kid that thought mom wasn't coming back sometimes. I'd post up at the window, look outside to see if she's coming home. I'd walk out on the streets to see if she was driving down the street. Denise wasn't like that. Denise was the kid who was just angry. She's just anger, anger. So, this one time, mom had been gone for a few days, we didn't have any food in the house, Denise walks in and she's got a pack of pork chops in her hand. And [00:19:30] I'm like, "Where'd you get that?" She's like, "I stole." And I'm like, "Well, show me how you did that." So, we go over to A&P and she shows me how she steals food and I'm like, "Hell, that's a good idea. Let's eat."

So, we start stealing food. We get to the point that we wanted to make sandwiches and you can't stuff a loaf of bread down your pants because it's going to get crumbled, so we had to have something to put the loaf of bread in. There was a Kmart across the way, so we go over there and we still a hoodie and stuff the bread down the sleeve over [00:20:00] the shirt, over the hoodie. And then that becomes, once you get by with that at Kmart, well, they've got toys and games and clothes. So, we started doing that, stealing all that stuff.

Mom comes home finally and she sees all the stuff we've been stealing. She's like, "Where'd that come from?" And I stand up at 10 years old, "We found it." She's like, "No, you didn't find that." My sister stands up and Denise was always like that. Denise stands up, she's half proud, she's half pissed off. She's like, "We stole it." My [00:20:30] mom looks at my sister, and she's like, "Show me how you did that." And I'd joke about it, but she started running as a shoplifter. If she wanted something stolen or distraction or whatever, she ran as a shoplifter. She goes to get her mom, too, so it's her mother, her, me and my sister. We used to take these road trips to different parts of the state shoplifting. They'd go in J.C. Penney's and steal clothes and jewelry. I'd go to bookstore and steal books because that's the guy that I am.

[00:21:00] And I say this and I really made this, I don't want people to think I'm blaming my childhood on my choices as an adult, because that's not true. I mean, my sister had the exact same upbringing that I did, other than that one shoplifting experience, she doesn't break the law anymore. She goes off. She's a teacher. She's a great parent. She's a good citizen.

Bill: Sure.

Brett: I'm just the guy who kept on going. And as I kept going, I got more and more involved in the types of frauds and scams and crime that my [00:21:30] mother in that entire side of the family committed. I mean, my granddad used to sit down on the bottom of the porch, underneath the porch and people would walk up to him with whatever item they had stolen that day and they'd come with a VCR and try to give him some story. "Well, Paul, this is where it came from." And he'd looked at me and say, "Whoa, whoa, whoa. I am not an FBI agent. I don't care where it came from. What do you want it for?" So that was my granddad.

But I mean, it was forgery, it was charity [00:22:00] fraud, insurance fraud, it was drug trafficking. I mean, anything that you could possibly imagine as far as basically training somebody if they decided they wanted to career in crime later on which of course, I decided that. I ended up branching off on my own and mid-'90s, faked a car accident to get the insurance money to get married to move from Hazard, Kentucky to Lexington, Kentucky to go to university. So, I go [00:22:30] there, and I'm the kid. I was raised and I was scared that the people and it was my dad and my mom. I mean, my mom instilled that in me. My dad was scared of losing the people that he loved, so that's what I do. I mean, I'm scared of the people that I love leaving.

Got married. Told my wife. I was like, "Hey, don't worry about getting a job. I've got it. I'll work. Don't worry about that." And told my wife, "Don't worry about the cooking and cleaning. You just worry about going to school. I've got this." So, here I am, dumb Brett. I've got a [00:23:00] 50-hour a week job. I've got an 18-hour class load. I'm trying to do all the cooking and cleaning. You can't do all that. Something had to give. What gave was the job and well that proclivity toward fraud I already had, well, you got to make money somehow don't you? I didn't really know how.

And one day I find eBay and it was evident. I mean, you knew when you looked at eBay that that was an environment where you could profit. I didn't really understand how. I didn't understand online [00:23:30] crime yet. One night though, I'm watching Inside Edition. Bill O'Reilly used to host that thing. They've got a show on Beanie Babies.

Bill: I remember the Beanie Babies. Yeah.

Brett: Yeah, the $5 thing, right? Mid-late '90s, $1,000 Beanie Babies. There's one where the profiling was Peanut, the royal blue elephant, right?

Bill: Yeah.

Brett: He was selling it for $1,500 on eBay. I sat there watching that show like, "I need to find me a Peanut." Next day, I skipped class to go around all the Hallmark [00:24:00] stores. This is how naive I was. I thought they had had one hidden in a base, in a bin someplace at a Hallmark store. So, I start going to Hallmark stores. I sneak over to the band. I'd start rattling through the Beanie Babies and finally, out of despair. I'd go up to the customer service desk, "Hey, have you guys got any blue Beanie Baby elephants?" And they had looked at me like I was an idiot. So, after five or six of those shops, I was like, "Well, he's not at the shops because they're selling for $1,500 on [00:24:30] eBay."

So, they did have these gray ones, these gray Beanie Baby elephants for $8. So I'm sitting there going, "Okay, buy a great Beanie Baby elephant for $8." Stop by Kroger on the way home, pick up a pack of blue red dye, go home and try to dye the little guy, put him in a bucket, water.

Bill: Oh, my.

Brett: [crosstalk 00:24:55] in there. So, you're sitting there because he's trying to float, you're stuffing him down in the water and you can get him [00:25:00] out, and you realize after 10 minutes of this that he's made out of polyester. He doesn't hold dye very well. Get him out of the bath. He looks like he's got the beige. You sit there going. I ended up, my first cybercrime, that was my first one. I ripped the lady off of $1,500 dollars.

Bill: Now, on eBay, and then, how did the social proof is a big part of that platform, maybe this was just super early and they didn't have those mechanisms built in, but if someone saw, didn't receive the value from [00:25:30] their purchase, because you dyed it in dye, and it wasn't the blue Beanie Baby, how did you then pivot, so that you could do that again and again?

Brett: So, back then and ShadowCrew ends up forcing companies like PayPal and eBay to change, [crosstalk 00:25:46] proper security. It didn't happen until ShadowCrew actually forced their hands in that way. All right?

Bill: Okay.

Brett: So, back when I started this stuff, it was the Wild West. There were no security protocols on eBay. You could [00:26:00] get their real name easily. They had their full email address, their contact phone numbers, everything else. It was just right there for you. So, what you could do is you could post an item like what I did was I found a picture of a real one. Posted it. She thought I had the real thing as soon as she wins the bid. I take the conversation off eBay platform. Actually, as a matter of fact, eBay didn't even have a platform at that point. They didn't have the instant messaging implemented that they do now. All right?

So, I sent her an email and then the email was basically that's where the social engineering kicks in. So, what you see time and time again, [00:26:30] I don't really care what the scam is, if it's a romance scam or if you're doing an account takeover, or what have you, at some point, social engineering has to kick in. All right? So she wins the bid and that's where social engineering, for me kicks in. I sent her an email. An email says, "Hey, I've never done any business with you. I don't know if I can trust you. What I need you to do, what will protect both of us, is you sending me a United States Postal money order. It's guaranteed by the United States government. Your money is [00:27:00] protected. I'm guaranteed to get my money. Everyone's happy about that."

Well, she believed that without really thinking it through because that's the way scams work. You try to get people away from objective thought. You just get them to a knee-jerk reaction. That emotion is what you're wanting to do. So, she believed that. She sent me a two U.S. Postal money orders. Now, what I knew was that there was no way for her to cancel those orders and I also knew that I could take them into U.S. Post Office and get [00:27:30] them cashed right there. So, I did that. After I cashed those money orders, I sent her this blue thing and immediately I get a phone call. Because at this point in time, I was doing this under my own name. So, I get a phone call on my phone and she was irate. She was like, "I didn't order this. You're trying to rip me off." And my response was, "Lady, you ordered a blue elephant. I sent you a blue-ish elephant."

And what happens is, is this is where a lot of people, a lot of criminals, you [00:28:00] learn the same lesson, somewhere along line, somewhere early along the line that if you delay a victim long enough, if you rip someone off on, you're saying you got a camera or this year, you're saying you got a PlayStation 5 or an Xbox X, you rip them off of $5, $8,000, they start complaining about it. Even if they may know your real name, they start complaining about it, but if you keep putting them off, "I'll send your money back. I'm sorry. You didn't get what you wanted to. I'm sorry. I'll make sure you get your money back." You just keep putting them off, sooner or later, they get exasperated, they throw their hands [00:28:30] up in the air, they walk away, you stop hearing from them.

And very few people, very few ever complain to law enforcement. That's why you see this year, specifically with PlayStation 5 and Xbox Xs, you see people all over the place that are selling these systems that they don't have, and a lot of these scammers will get to keep the money because people just give up after a while. They figured, "Who am I going to report to? Am I going to port to local law enforcement? Well, they're not. Am I going [00:29:00] to report to the jurisdiction where I sent the money? They're probably not going to do anything. It's his word against mine, this whole thought process is. FBI, the dollar amount tends to be so low, they're not going to really look at it." So, that's typically what happens, so.

Bill: So, what type of money are we talking about, Brett? Like when you early on, it's very entrepreneurial in many respects.

Brett: Sure.

Bill: It's just the dark side of entrepreneurship, but it's the same thinking pattern. It's like you're probably trying to generate as much money in your pocket as possible, [00:29:30] like over a 10-year span, like what did that look like that you-

Brett: So, 10-year span, so I got to the point that an eBay account, because I would set up an eBay account and I would also set up a bank account to cash out the items that I wasn't selling, so an eBay account would profit, it'd be $12,000, roughly for each eBay account that I set up and typically, I would run one of those a week, so I was profiting, at one point 50K a week, 50K a month. All right? Now, as ShadowCrew gets built, [00:30:00] we transitioned. So, these whole platforms start out as PayPal fraud and eBay fraud. It transitions over to credit fraud once we hook up with Dmitry Golubov and the Ukrainians, okay? So-

Bill: So, they had the ability to get the credit card numbers [crosstalk 00:30:16]-

Brett: They had all the credit information in the world. And this goes back into this idea that I talked about, the three necessities of cybercrime: Gathering data, committing crime, cashing out. So, the Ukrainians could gather the data all day long. They could even commit the crime [00:30:30] to a degree. The problem the Ukrainians had was cashing out because in the Eastern Bloc of Europe, at that point in time, every single card had been shut down. There had been so much fraud already that even if you were the legitimate cardholder, you couldn't run your card over there.

Bill: No way. Right.

Brett: So, all of a sudden, the Ukrainians have all the credit information in the world. No way to put cash in pocket. They have to rely on somebody else. The only game in town because Dmitry got his idea from the ShadowCrew group, so the only game in town was us, [00:31:00] so he comes and we partner at that point. And that's where the genesis of modern credit card fraud takes place is with Dmitry Golubov, Roman Vega, guys like that.

So, you start out on eBay fraud, roughly $12,000 per false eBay account or fake eBay account. Credit card theft, you're looking at, it's not a whole lot of work back then because you didn't really have ABS or anything like that in play, so a credit [00:31:30] card thief could profit $40,000 to $50,000 a month fairly easily. All right? If he knew what he was doing, he could profit that. It takes a little work, but 40K, 50K. I got to the point, because I'm the guy that I was doing all that stuff, and then I got to the point where I happened upon or I hate to say the word invented, because somebody would have done it if I hadn't, but I started this thing called tax return identity theft. So, the reason everyone's tax returns are delayed every single year [00:32:00] is the SOB Brett Johnson.

I had access. The first PII database I had access to was the Indiana State sex offenders' registry. So, you could go on there, and it had all the sex offenders in Indiana. It had their social, their mother's maiden name, their driver's license numbers, their dates of birth, I mean everything. So, I'm sitting there. I saw that and I'm like, "Huh." And my idea, what I started doing was I would open up bank accounts, [00:32:30] in the names of these sex offenders and I would commit the crimes under their name, and my thought process was, "Who's going to complain that a sex offender is being victimized?" Nobody. So, I started doing that and used that so much that Indiana starts removing that PII from that database. First thing that left was the DOB and the SSN then it goes from there.

So, the next database I had access to was the Texas driver's license database. And then finally, I ended [00:33:00] up with access to the California State Death Registry. So the idea was I had access to that and I was like, "Okay, how does the federal government know you're dead?" And the way that works is before 1998, it took the family to file a social security death benefit, so you've got a state death index, you've got the federal death index, the only way the federal government knows someone dies is a Social Security death benefit has to be filed [00:33:30] for that person.

Bill: Sure.

Brett: Okay, prior to 1998, it took the family to do that. After 1998, the hospital, the funeral home, a group like that could do it. So, I'm sitting there, I've got access and I've researched it enough. I find that out and then my first thing was, "I wonder if I could file for Social Security benefits on these people? That would give me an incoming check every month." So, I started trying to do that and the answer was no, because the number had been dormant for so long, [00:34:00] they wanted you to come in for an in-person interview. And that was no, because here I am at 34 and I'm trying to pass myself off as 63, 65, something like that.

So, the next thing was, "Well, I wonder if you could file tax returns on people like this." So, the way cybercrime operates the high tier attackers and I don't care if it's someone that's a computer genius or a very good social engineer, it's all about doing as much research [00:34:30] as you can. So, you read white papers. With me, I ordered this big ass book on tax law and you just read through every single thing. I pull up all the indictments that I can regarding tax fraud to find out what's going on, how people are doing it, everything else. And then you start doing, you put your operation in play. What does it take in order to try to defraud the United States government? So, you basically over prepare and it doesn't matter what it is.

Bill: Sure, or by learning [00:35:00] about, reading this case, like why they were caught and what they were doing?

Brett: Exactly.

Bill: Okay.

Brett: You do as much preparation as you can and then when you start to try to launch the crime, you overdo things. So, when I started filing these fraudulent tax returns, I was using proxy addresses. If the guy's name was Brian Johnson, I would find a real Brian Johnson and correlate the address between the two. I would use payroll software to make sure that the figures were completely correct. I would come up with the different [00:35:30] amounts for each, each victim everything else to file for.

So, you start out doing like that and then you find out then you start cutting corners. Once it works, you figure, "Okay, how can I make this more efficient? What can I cut out that it will still work fine?" I got to the point that I was able to file a tax return manually once every six minutes. So, I would file, I'd work Sunday through Wednesday, file roughly 180, 200 tax returns a week, 80% of those would tend to fund and I would cash out at about $160, [00:36:00] 000 a week at that point.

Bill: Wow.

Brett: So, I would file Sunday through Wednesday. Thursday, I would take a road trip. Plot out a map of ATMs. Friday and Saturday, I would cash those cards out then come back Sunday.

Bill: So, these would come in as cards ? They would come as-

Brett: Actually, so the problem is when you're looking at that type of thing, how do you have the money deposited? You don't want checks sent to you, because that leaves a paper trail. Back then was when we first saw prepaid debit cards [00:36:30] start to hit the market.

Bill: Sure.

Brett: So, that's one of the things that you see time and time again, is a new product comes on the market. It's a great product. The consumers are going to love it, but some engineer somewhere has not really figured out that, "Hey, fraudsters will love this stuff, too." So, they don't really think about the fraud aspects of things. So here I am, we start to see these payroll cards, basically prepaid debit cards, I'm able to order 200 a week sometimes, so you order [00:37:00] 200 a week, you have the tax returns deposited onto that, you take a road trip, and you spend 40 to 50 minutes at an ATM sometimes just feeding one card in, pulling out $20 bills, stuffing it in the backpack.

I would come back on a Sunday. I was in Charleston, South Carolina. I had a spare bedroom, $150,000 in $20 bills fits into a backpack. I would open up the bedroom door, chuck the backpack in there, then one day, you wake up, you open that bedroom door and you're like, "Got to do something [00:37:30] with all those backpacks." And that's when you learn how to launder money.

Bill: Yeah, I was going to say that that's a great, great point, because I don't think you can't just show up at the bank and say, "I want to open a bank account with $120-"

Brett: I remember because I was... and a lot of it, and criminals are like that. They're good in one area, but they're naïve in other things.

Bill: You're like Blacklist. You ever watched the show Blacklist?

Brett: Yeah. It's a good show, it's a good show.

Bill: And then, I mean, it's very, very interesting. But okay, I mean, I stopped you, but you-

Brett: No, you're fine.

Bill: For the launder part.

Brett: [00:38:00] Yeah. So, criminals, they'll be good in one area and they're naïve other places. They don't really understand and it's a process of learning it when you learn it. All right? So me, I was stealing all this money, so I've got all these $20s and I've got. "Okay, I'd like a jet ski or I'd like a boat." So, here I am, idiot that I am. I walk in with a satchel full of $20 bills and I'm looking at the jet skis. I'm [00:38:30] like, "Which is the best ski you've got?" They point out this four-seat Yamaha ski, and I'm like, "That's the best one?" They're like, "Yeah." I was like, "How much is that?" And I think it was like 14K or something, but I was like, "You take cash?" And he was like, "What?" And I was like, "Do you take cash?" And he was like, "Yeah, we take cash." So, I'm like, "Let's go."

So, here I am, middle broad daylight, counting out stacks of $20s. Bam, bam, bam, bam, bam. I got three people counting. The guy, who owns the power [00:39:00] sports store. He was in the back. He finally comes up front, and he's like, "What are you a drug dealer?" And I'm like, "No, I'm a cyber criminal." And he was like, "Yeah, you are." I'm like, "Right. It's funny, right?" But I mean, that's part of it, you do stupid stuff, you do stupid stuff. That tends to be what gets criminals caught is this not understanding what's raising flags a lot of the time.

ShadowCrew goes [00:39:30] on to make the front cover of Forbes, of course, August 2004. It was a headline, "Who's stealing your identity?" It was about ShadowCrew. It was about how the FBI, the Secret Service was investigating those sites that were up at that point. October 26, 2004, United States Secret Service arrested 33 people, six countries in six hours. It was a Sunday that happened. And I was the only guy publicly mentioned as getting away. [00:40:00] A couple of other guys had gotten away, no one talked about that, but they picked me up February 8, 2005. For you to turn your life around, you got to hit rock bottom.

Bill: Sure.

Brett: It took me a long time to hit rock bottom.

Bill: This is classic Joseph Campbell hero's journey, that descent into hell?

Brett: I love him. I love Joseph Campbell.

Bill: You've seen that?

Brett: The Hero with A Thousand Faces, Power of Myth, all that.

Bill: [00:40:30] Yeah, yeah, Power of Myth.

Brett: Yeah. So, I had been married for nine years, had lied to my wife, my first wife, the entire nine. It took really three years to find out that I wasn't just a criminal, just a criminal. And once she found that out, the next six years were me telling her that I'm going to stop or I have stopped or I will stop, finally getting mad and telling her, "Hey, you're spending the money, too." She leaves and the way she leaves, [00:41:00] I guess she understood that at the end of the day, it was the only way that I would break off with her is if she cheated on me. So, she did and I found out about it and of course, that would end it, so she leaves. And that fear I had of being abandoned, that became real. I mean, I caused the thing, but it became real.

So, I'm in Charleston, South Carolina, I just cried every day, walking around in a daze, getting suicidal. And [00:41:30] I mean, it's kind of like a comedy, so I've realized I'm getting suicidal and I'm like, "I got to do something." Go over, grabbed the Yellow Pages, opened it up to psychologist, and I'm flipping through psychologist and there's criminal psychology and I'm sitting there thinking, "Well, shit. I need that." And so, I'm like, call. I'm crying to the psychologist. I tell her everything and she's like, "Come in today." So, I go in and I just, I spill guts. I have the conversation, "If I tell you stuff, are you allowed to report law enforcement?" She's like, "Not unless you're actively [00:42:00] committing crime." I was like, "Well, I'll just leave that point out."

So, I tell her everything and I saw her for about four months, and she was trying to get me to quit breaking the law. Trying to get me to go into real estate and me, being an asshole that I am, I'm like, "Real estate. What, is there a difference?" But what happens is, I was 34 and I'm the guy because my mom was a drug addict, I had never used drugs, never drank or anything else like that. I started drinking when I was 34. And [00:42:30] so, I saw this psychologist for about four months and one night I get lonely and the little libido is acting up a bit, so I'm like, "I've never been to a strip club. Let's try that."

So, I walk into a strip club, 34 years old, had never done that before and that naiveté pops in again. It's not like you're a criminal and you understand everything. No, I was very naive. So, I walked in and I'm that idiot. I literally, literally, the first stripper that I saw [00:43:00] is the one I fell in love with. She walks by, I'm like, "That one. That's the one." So, I ended up moving her in my house. After I moved her at my house, found out she was addicted to cocaine, not only addicted to cocaine, but was prostituting herself to support that habit. And I guess, I adopted. I've got on my cape and goggles and played superhero. I figured if I could save her, everything would be all right.

Bill: Sure.

Brett: And I make a lot [00:43:30] of that, Bill, but that's a lot of the truth there. A part of me felt that if I could really, really save her that we would love each other and it would be all right. And I mean, I was head over-

Bill: Isn't that what your father did?

Brett: Yeah. Same thing. The exact same, the exact same, exact same.

Bill: I mean-

Brett: I mean, you could look back and say, "Yeah, that's where he got that from. That's where he got that from." Yeah. I mean, you could read me like a book on that, so she didn't know I was a criminal either, of course, because I was a [00:44:00] liar. I lied to everybody.

Bill: Sure. Sure.

Brett: So, here I am. It's like ShadowCrew gets busted and I got it to my head, her name was Elizabeth. I got it in my head that I could keep her mind off drugs by giving her whatever she wanted, whatever she wanted, I did. So, that quickly became, you'd spend $300, $500 a night at dinner. It'd become I'd withdraw $11,000 [00:44:30] on a Friday and on a Monday morning, not have anything left, nothing. I had no idea what happened to it. So, I quickly went through, I'd laundered all my money over to Estonia and I quickly went through everything in the U.S. side.

Meanwhile, ShadowCrew gets busted. Now, I had stepped aside of ShadowCrew at that point. I was doing the tax return fraud. I had stepped away from that and by this point, I was engaged to Elizabeth because [00:45:00] I kept thinking if I just keep investing, everything will work out. So, I didn't have any money, all of a sudden. ShadowCrew gets busted. I can't do tax fraud because tax season's over. I can't go into credit card fraud because the Secret Service has shut all that down, and you have no idea who you're talking to anymore. So, it was paranoia through the roof. She's like, "What are you going to do?"

So, I had always preached to people never, never run counterfeit checks and that's what I started [00:45:30] doing. I started writing counterfeit checks, and knew that the end was coming, knew it. And I get picked up running that. By that point in time, I didn't have enough money to buy the engagement rings for us, so she wanted Tiffany rings, of course. So, I defrauded two people out of those via eBay. And then she wanted Tiffany wedding bands, and I certainly didn't have enough money for that, so defrauded [00:46:00] more people out of that, and that's where I got picked up was at that point right there.

Bill: What do you think the skill is most important or do you think is most prevalent now with what's happening with cybercrime? Do you feel, do you think it's more of the technical skills like-

Brett: Technical?

Bill: Or is it this social engineering part?

Brett: So, it's both. Social engineering, without social engineering, [00:46:30] cybercrime ultimately fails. Now, you can build the best ransomware in the world. You can have whatever program you've got out there, but if you can't deploy that, if you can't put it on the system, it's useless to you, so they work in conjunction. I would argue that social engineering is more important, but it boils down to getting someone to trust you enough that they do what you want them to do and the way you get people to trust you, if you're a criminal online is by using technology tools [00:47:00] and then finally, social engineering. So, we've got a cell phone, we've got a laptop in front of us, we tend to trust that tech. We don't really understand a lot of it a lot of the time, but we trust it. We trust the stories that come across. We trust if a number comes across on our cell phone that it's the number that it says it is.

We don't understand that criminals can use tools to manipulate that technology, to spoof a phone call or spoof a location or something like that, so it's technology and tools lays base levels of trust, but then finally, it's whatever [00:47:30] that social engineering looks like. Is it the phishing email? Is it a Unicode domain? Is it something like that that's being used to finally trick the person into giving whatever you want them to give, information to access data or cash?

Bill: So, when you're working with someone these days, we're going back to how you turned your life around...

Brett: Sure.

Bill: ... in a moment. But when you're working with a customer now, with a company, what is your superpower that you [00:48:00] most often see that you're able to help them with in your engagement?

Brett: Sure, I am extremely good at knowing the vector of which a company will be attacked. So, if you have-

Bill: Because you could see it through a different angle? You can see it.

Brett: Yeah. I know what criminals are looking at, I know how they're going to do it, and typically, I can either pull up enough data that shows that, "Hey. I'm not the only one that knows this. Criminals have been talking about you for a while," or I'm very good at, I've been extremely good, since I've turned this, turned the curve [00:48:30] and I'm this good guy now. I've been extremely good about anticipating different types of cybersecurity or cybercrime trends that are coming up. So, on the merchant side, you've got this thing that's eating merchants alive this year called friendly fraud. It's basically a refund fraud is what it is.

So, I was talking about that five years ago. Synthetic Fraud was one of the first people that started talking about that period. Told them it was a problem. Now, it's 80% [00:49:00] of all new account fraud. It's the fastest growing form of financial crime on the planet, so it's-

Bill: Synthetic fraud.

Brett: Synthetic fraud. It's weird. It's this thing where you can... so, the Social Security administration, they randomize social security numbers in 2011. They did that to combat identity theft because if I know the last four of your number and I know the state you're born in and the year you're born, it's very easy for me to get the first five. It's an algorithm. It's very easy to pick that out. [00:49:30] So the Social Security administration, they randomized it to stop that fraud. It did, but when they did that, it now allows criminals to either fabricate numbers or to use a child's Social Security number, build new credit profiles, and then cash out at that point. Extremely, extremely effective from a criminal point of view.

So, it's very easy. It's not very easy, but I've got the skill level where I'm able to kind of gauge the pulse of the way the cybercrime community is going and I guess that's [00:50:00] where I was on the ground for developing and implementing a lot of these crimes. Nowadays, we've got a couple of channels like Discord or Telegram that are really setting the tone for the way cybercrime is going to go into the future. Those types channels and communication areas, but that's my primary skill is that. I'm very good about being able to, instead of, I can be technical, but I prefer to not. [00:50:30] I think it's very important that we be truthful about things. You don't have to make things highly complicated, especially if you're talking to a manager at some place.

We've got this perception that that attackers are these computer geniuses, these specters. We see that. We have 7,000 security companies and a lot of them are snake oil salesmen and there's a lot of them that sit there and it's easier to scare a potential client into thinking that it's a computer [00:51:00] hacker that you're never going to be able to track down and he's able to get into your system whenever. The problem with that is that it's not really true. The problem is not that they're specters. The problem is, is that typically, it's the company is not doing what they need to. You've got 92% of every breach uses known exploits.

Bill: So, why are we going after, why are the bad actors going after medical records now? Why [00:51:30] are hospitals and the medical system, why those records are so much more valuable on the dark web versus like a credit card data?

Brett: Well, it used to be. That's the weird thing. It used to be that and when I was running things, you would have somebody that would come in with thousands of medical records and not be able to sell them. I mean, they had no value whatsoever. Okay. You'd typically have this person that's criminal to come on and say, "Well, what will you give [00:52:00] me for them?" They would be begging for something and then finally, they'd just start giving a lot of stuff out free.

What was found out over, and that's because it was very easy at that point in time to launch a phishing attack and you could ask all of this PII and the victim would fill it out. They weren't educated enough to know better than that. Nowadays, medical records are a primary source for information. You could get all the PII in the world, a lot of [00:52:30] credit card information is there, you can get the medical history, but it's-

Bill: That's why it's so much more valuable.

Brett: It's crazy. The amount of data that you can get from that is absolutely crazy and it's very easy to hit. You've got HIPAA, but I want to tell you, there's not a criminal in the world, who really gives a damn about HIPAA.

Bill: Right. Yeah. And, it's not really, it's not useful and it does anything. It just identifies broad scopes of what to [00:53:00] do and not do. It's not very poignant and pointed about how to structure your defense.

Brett: But it gets worse than that. I mean, I do believe in training or cybersecurity training for compliance, but it has to be done properly and I believe in doing it for effectiveness as well. When I see, and I'm in Birmingham, Alabama. And Birmingham, they've transitioned from that iron steel town into a medical town. And I'm fortunate enough, [00:53:30] my wife, at one point was a medical practice manager and typically, what you're seeing is with their HIPAA training, is the employee's sit down during lunch break and they watch a video and that's it. And then, there's a couple of questions they have to answer after that and that's it, so it there's no retention at all about on top of the training.

Bill: So, what do you think the best training is?

Brett: It needs to be hands [00:54:00] on. It needs to be, I think-

Bill: But you do a lot of this training. I watched the video where you were doing something with AARP.

Brett: Right. Right. It needs to be hands on. It needs to be personalized. I was talking because hopefully, hopefully, we're getting ready to launch some training video, but sometime in the next year. I was talking to the guy and he was like, "Well, why you? Why are you going to do that?" And I was like, "What do you mean?" He's like, "Look," he said, "there's all kinds of training videos out there. You need to do something [00:54:30] that someone is going to remember, make it basically the Forrest Gump of cybersecurity awareness training. Someone is going to engage with that. It's going to be entertaining, but it's going to be something that they remember."

Bill: Storytelling.

Brett: Storytelling. That's what it's all about. If you could just, if you're preaching at someone, they're not going to retain that.

Bill: No.

Brett: That's typically what you see all the time with cybersecurity training. You get some guy that's on electropod and he's lecturing.

Bill: You see, that's what you got to do is just tell stories. You have all these little stories on your podcast. [00:55:00] You could take those as a prelude into the actual training. People will be glued to it.

Brett: We're hoping, we're hoping for something like that.

Bill: So, let's wrap this up, but I want to wrap it up with tell us how you started to get things back together on track. And so, that return to the hero's journey descent into hell, and then comes out with a story to tell, so essentially to teach everybody.

Brett: I went to work for the Secret Service. I was arrested. They let me sit a week at the county [00:55:30] jail in Charleston, South Carolina. And when I say sit a week, it was in the holding area for a week. I slept on a table. Okay? On a steel table because it was that crowded. There was not room enough. You could not sit down or anything else, you just made the best spot you could. I was week there. Secret Service flies in from New Jersey. They pulled me out of the cell. They look at me said, "We got your laptop." I'm like, "Yeah." They're like, "You got anything on your laptop?" I'm like, "Yeah." They're like, "You're going to be charged for whatever's on it." And [00:56:00] I'm like, "I figured." And then they look at me and they say, "Hey, is there anything you can do for us?"

Well, they arrested me three weeks before I was supposed to be married to this Elizabeth girl, and I was head over heels with her. I looked at them and my exact words, I still remember that to this day, my exact words were, "Hey, man. You let me get back with her. I will do whatever you want me to do." They looked at me and said, "We're going to get you out." I'm like, "Yes." They let me sit there for three more months [00:56:30] to get a taste of it. Finally, they get me bonded out. They reduce the bond from $327,000 cash to $1,000 cash. My sister pays the bond.

My first phone call isn't to my sister, it's to Elizabeth. "I'm out baby." During that three-month time, she had visited, I don't know two three times, had taken two or three calls, that was it. So, I tell her I'm out, she's like, "I'll be there." It's midnight. She had a friend that ran a limo company. [00:57:00] She pulls up in a limousine, me and a Secret Service agent are standing in the parking lot. She pulls up and limousine, pops the trunk, gets out, gets these two plastic storage containers with my clothes in them, drops them on the parking lot, comes over hugs me, "Call me later." Leaves. I'm sitting there and I start crying like a baby. Secret Service guy, he looks at me. He's like, "Is that your fiancée?" And I'm like, "Yeah." He was like, "Dude, I am so sorry." I'm like, "Yeah." But [00:57:30] I was so convinced that, he had to pay my hotel room that first night.

Bill: No way.

Brett: Because I didn't have a house anymore. He paid my hotel bill. I had $30 to my name. Soon as he leaves, I walk because I didn't have a vehicle. I walked to Walmart, buy a prepaid debit card, so I can start back in tax fraud.

Bill: Wow.

Brett: I then call Elizabeth and begged to get back with me. She does, and for the next 10 months, I break law while working for the Secret Service often from inside Secret Service [00:58:00] Office. They find out after 10 months. Like "Yeah, you knew they were going to." They find out, I take off on a cross country crime spree.

Bill: Wow.

Brett: Yeah, steal $600,000 in four months. I'm in Las Vegas, Nevada. The night before, I had stolen $160,000 out of ATMs. Woke up the next morning. A friend of mine, Max Butler, was running a website [00:58:30] called Carders Market. I signed on to Carders Market, there is my name U.S. Most Wanted beside it.

Bill: No way.

Brett: Yeah, yeah. And I joke about it, saying that's not just an aha moment, that's one of these aah type of things. So, I actually sat there for a few minutes, looking at that. Clicked on it and it was linked to the Secret Service. It had my information on there and I'm sitting going, "Okay, Brett. What now?" Because [00:59:00] I was planning on bugging out to Brazil. I had found a house in Florianopolis. I was going to live down there and start my fraud ring up again.

So, I'm sitting there looking at it. I'm like, "Okay, Brett. You've made the United States Most Wanted list. What do you do?" And I said it out loud, I'm like, "I'm going to Disney World." And that's exactly what I did. I went to Disney World. It lasted about six weeks. The Secret Service, they came and got me, arrested me, sent me to prison. Six weeks into prison, I escape.

Bill: Wow.

Brett: Yeah. I escaped prison and [00:59:30] they caught me a few weeks after that. And they sent me to a real prison at that point out in West Texas, and what happened was, what gets me turned around, Bill, I had three things. It starts with my sister. My sister disowned me because of my relationship with that stripper.

Bill: Right, right.

Brett: She knew I was a criminal, but she could not handle that, so she disowned me and she didn't talk to me for over a year. During that year is when I get arrested, go to prison, escape everything [01:00:00] else. So, after the escape, I'm in a county jail in Lexington, Kentucky, my dad comes to visit and he was like, "Can I do anything for you?" And that's where I'd hit rock bottom right there. He's like, "Can I do anything for you?" And I'm like, "You could tell my sister I said I love her." Dad gets on the phone, calls Denise. Denise is seven and a half hours away, pregnant with my niece, and he tells, Denise gets in the car and she drives those seven and a half hours to come and see me for 10 minutes to [01:00:30] tell me she loves me.

Bill: Wow.

Brett: And it took two and a half years, it took two and a half years behind the fence for me to realize that the reason I was in jail wasn't because I told myself, "I did it to help my family, my wife, my stripper girlfriend." No, it took two and a half years for me to realize that I did it because I chose to do it. I chose to hurt people because that was my decision. A hard pill to swallow when you start accepting responsibility for hurting people, so I got out [01:01:00] in 2011. No taste for breaking the law whatsoever.

Bill: And how long was that timeframe? Like-

Brett: I spent a total of seven years in prison.

Bill: So, the two and a half year mark was when you really felt the shift, and then-

Brett: That's when I came to terms with things, it started.

Bill: And then finished up the balance of that, okay, at the prison.

Brett: Right. So, I got out in 2011. No taste for breaking the law whatsoever. I was under three years' probation. Could not touch a computer. I wondered why. I had job offers from Deloitte, from Nova 4, a couple [01:01:30] of payment processors, didn't take them. It got to the point I was trying to apply for fast food. No, that payment terminal, that's a computer. I can't take it.

Bill: You can't do that.

Brett: So, then it's like, "Well, what about a waiter's position?" Well, no, that's computers and credit cards. You're an idiot, so I literally could not get a job. That's not what a lot of people don't understand. I mean, you can't get a job selling cars, nothing else because you stole money. There's a big difference between hiring someone who dealt drugs or something like that compared to someone [01:02:00] who's an embezzler or someone who steals money.

Bill: Sure.

Brett: So, you can't get a job. I was under. I was bumming money from my dad and my sister. I had a roommate that was taking care of half the rent. I was on-

Bill: It's probably you were better taken care of in prison than you were when you [crosstalk 01:02:16] out.

Brett: Much better, much better.

Bill: You easily had food. You had regular, yeah. I mean, a lot of that.

Brett: I actually got to the point, I told my dad at one point, I wish I was back in. At least there, I knew the way there.

Bill: So, that was real rock bottom is coming out?

Brett: Yeah. [crosstalk 01:02:31] [01:02:30] And it keeps going, though. I mean, I'm the guy, so I was on food stamps, everything else. They tell you to find something you care about, you may not recidivate. I had a cat, that's what I had. I had enough money to feed my cat and I didn't have enough money to buy toilet paper. So, first crime I committed, go to the dollar store, buy the cat some food. On the way out, they had a kiosk with toilet paper there and I stole toilet paper. I didn't want to get back [01:03:00] online and commit crime.

Bill: Sure.

Brett: So, I shoplifted and what happens is, is my wife now, Michelle, she ended up finding me about the same time. I didn't find her, she found me. I ended up moving in with her about two months later. Finally, I get a job. The only job I could get was pushing a lawn mower. That was it. That was it and had to beg to get that. But I started pushing a lawn mower, busting ass doing that. What happens is, is once [01:03:30] it gets cold, the job ends. You can't mow any grass.

I talked about motivations of cybercrime, it's ideology, status, or cash. With me, it was cash, but it's what you can do with it. With me it was, I'm the guy who buys love. It's never enough. It's never been enough for me to show love in a healthy way in a relationship. I have to buy gifts. I have to go overboard all the time, so the job ends. I don't have any money coming in. I'm like, I've got to do something. I've got to show it to her that I'm worth it [01:04:00] in this relationship. She's the only one working.

So, I get it in my head, "Well, at least I can bring food in the house." So, idiot Brett gets on the dark web, buy stolen credit card details, starts ordering food, starts stealing food online, and I get caught. I go back to prison for 10 months. I had my sentencing. The probation office, prosecutor, U.S. Marshals, the judge, and Michelle. Michelle stands up and she's crying. She tells the judge that I'm a better dad [01:04:30] to her kids and their father is. I'm sitting there crying like a baby. I get 10 months and go back. What I find out is, is that that entire time Michelle didn't need me for what I could give her. She just wanted me for me.

Bill: Sure.

Brett: And I'd never had that before, so I get out after 10 months. I'm off probation at this point, so I can touch a computer now. Start looking for work. Nobody's going to hire you, man. You're the guy who steals money. No one's going to hire you. [01:05:00] And I know what my triggers are. I know I'll go so far before I start doing it again, so I looked at Michelle and I was like, "Let me see what I can do." So, I go and of all things, I signed on to LinkedIn, is what I did. And I reached out to this guy named Keith Malarsky, FBI agent out of Pittsburgh. He was involved. I mean, he'd been involved in some of the people that I knew that had been arrested. I mean, just FBI super cop, this guy. And I sent him a message and the message was, "Hey, I respect everything you did. I think you did [01:05:30] a great job, no hard feelings. Just lots of respect for you. By the way, by the way, I'd like to be legal."

And I sent him that message, and he responded within two hours, and he gave me advice. He gave me references. He does that to this day, that guy does this. He's retired from the FBI now, but he does that to this day. From there, it was the head of the identity theft council, took me under his wing. [01:06:00] The head, the editor of the CMP group, [inaudible 01:06:03] group, she hires me for a paid speaking gig. Microsoft comes in and hires me once they hear about it. And it kind of went like wildfire. Today, things shut down because of COVID this year, but I typically keynote somewhere between 50 to 70 conferences in a year.

Bill: Wow.

Brett: I consult. I'm working on a book, a couple of TV shows. I've got two podcasts.

Bill: Are you really [01:06:30] a theater major in college?

Brett: I was, I was.

Bill: Okay because you've got a voice. You've got a theater voice.

Brett: Yeah. Honest to God, I used to be conceited with that, but I'm scary good on stage when it comes to theater.

Bill: Yeah, yeah. I noticed that. Your presence is very strong.

Brett: Yeah. No. I used to be conceited, I used to be a really conceited guy with that, but it took a lot of time to get humility, but yeah, I was-

Bill: But that's quite a powerful [01:07:00] kind of coming from that zero state and that continually pummeled. It's a powerful, people don't understand how hard it is to change your first 10 years of your life.

Brett: It is, and-

Bill: That programming if you don't get that, if you get it right and you're perfectly parented, you're golden. If you don't get it right, you've got a whole set of challenges, but the thing is-

Brett: It's a problem.

Bill: Yeah. It's a powerful thing to redo it and-

Brett: With me, and I [01:07:30] want people to understand that, what really separates me, the reason I'm not back in prison right now for 20 years, it could have been easily Brett Johnson back for 20, the reason I'm not is that I had enough people out there who took a chance on me. The people I had, the identity theft council, Keith Malarsky, the FBI, Microsoft, all these groups, they didn't have to do that. They put their necks [01:08:00] on the line to give me this chance.

Bill: We talked about the power of mentors, Brett, the power of who were the average of the five people we surround ourselves with, and we talk about that quite a bit in the CIO Innovation Forum and you're a perfect example of that. If you had to look at your five closest friends 10 years ago and your five closest friends today, the people, it's just complete-

Brett: Huge difference.

Bill: You rise to the level of that click, that cohort, [01:08:30] that group.

Brett: You do, you do. You truly do, you truly do. And I lead a blessed life that I don't deserve, but man, am I thankful for it every single day of my life. I get choked up thinking about it. I truly am thankful for the opportunity I've been given.

Bill: Well, at the end of the show notes, I'm going to put links for everybody, so they can connect with you on LinkedIn.

Brett: Sure.

Bill: You're a very strong presence [01:09:00] on LinkedIn and your podcasts and ways that they can engage with you. I imagine whether it's speaking or whether it's consulting with organizations that the mind that you have is a very unique gateway into what people are trying to protect right now.

Brett: Thank you. Thank you. I appreciate that.

Bill: Yeah. So, I wanted that one. Thank you for sharing your story. It's powerful and I know people are going to be glued to it.

Brett: [01:09:30] Bill, thank you for having me. I do appreciate it again.

Bill: You're welcome. You're welcome.

Brett: Stay safe out there.

Bill: Yeah. It's a pleasure. Thank you. Have a good day.

Brett: Yeah. That was-