[music]

**Rihonna:** Hello, and welcome to Fraud Talk, the ACFE's monthly podcast. I'm Rihonna Scoggins, the Community Manager for the ACFE, and today I'm joined by Jim Ducharme, CEO of RSA, a leading technology company in the fight against payment fraud. Jim, how are you doing today?

**Jim:** Great, thanks. How are you?

**Rihonna:** I'm doing great, it's a really nice day here in Austin, so there's a lot to be thankful for.

[laughter]

**Jim:** Well, we just got more snow up here in Maine, so I'm jealous.

**Rihonna:** Oh, goodness. Jim, thank you so much for joining us today. You have extensive experience working with tech companies focused on GRC and anti-fraud work. Can you tell us a bit about how you got into the anti-fraud space?

**Jim:** Well, I've spent a lot of my career dealing with identity and authentication things like that. Over the recent years, I've realized that identity has become really the number one threat vector for how fraud happens. How people are stealing your money. It really just gives me an even bigger purpose for the identity background I have to really apply it to trying to stop fraud in the world.

**Rihonna:** Definitely. I always find it interesting how people got into the industry, either they came across fraud in their work and it lit a fire in them or they just fell into it. I think both are equally interesting to hear.

**Jim:** Yes, absolutely.

**Rihonna:** Today we're here to talk about, buy now pay later services, and how fraudsters are taking advantage of these systems. For those of us who may not know, can you give us a little overview of what these services are and how they differ from traditional credit cards?

**Jim:** Sure. You may see this if you're shopping online and in the checkout experience, you're going to see all new ways to pay. We're, obviously, familiar with checking out and then providing your credit card numbers to the merchant. We call that Card Not Present credit card transactions or CNP. Now there are new ways to pay. People are familiar with using PayPal, that looks like a credit card transaction, sometimes. Now there's these new Buy Now, Pay Later methods where they basically say things like, "Hey, pay for this transaction in three easy payments," so they break down the payments of easy installments.

We see either new types of companies like Klarna after pay and many others offering this sort of payment installment plan, or some of the credit card issues or even offering it. You might get offers from your credit card issuer to say, "Pay for this in easy installments." That's what buy now pay later is. Basically, it's the old installment plans you might have had, getting the **[unintelligible 00:03:03]** pocket fisherman for three easy payments of $33 a month.

**Rihonna:** With these Buy Now, Pay Later services, they can be incredibly alluring to people who may have poor credit history or for other reasons they might not qualify for typical credit cards, but that allure extends to fraudsters, right?

**Jim:** Well, what's really alluring to fraudsters is that there's a whole new attack pattern to steal your money. When a buy now pay, later transaction happens, and what's can be a little bit different than your traditional credit card, when you're using that credit card online, you've already established a relationship with your bank, they've extended your credit line, and they've given you a credit card. Many of these buy now pay later forms you can establish an account with them as you're purchasing something.

If you're purchasing something online and you choose one of these Buy Now, Pay Later options, you're actually enrolling, basically creating that account while you're checking out. What the fraudsters are doing is actually taking advantage of-- Rather than taking advantage of the payment fraud, they're actually taking advantage of the account enrollment part of it. In other words, establishing that account with the Buy Now, Pay Later vendor, or even with a credit card provider.

What they're doing is they basically can steal your identity to establish an account in your name, but have the goods or services delivered to them. Really, it just adds another risk factor to how fraudsters can steal your stuff. Again, rather than steal your credit card numbers, which is an established account with your bank, they can try to steal your identity open an account with one of these Buy Now, Pay Later options and complete the transaction, have the goods shipped to them. That's what's appealing to the fraudsters, is a new vulnerable spot in the payment method.

**Rihonna:** Yes, I think a major benefit of these services is convenience?

**Jim:** Right. That's why any of these new emerging payment methods really all are about providing that flexibility of pay. What you mentioned this is a new type of payment method that is great for an underserved market of people that maybe not carrying around a large credit limit. Maybe they don't have a credit card that can pay for that size purchase. These Buy Now, Pay Laters are alternate forms of ways to pay.

All of these methods whether we're talking about buy now, pay pater, peer-to-peer payments like Venmo, Cryptocurrency, they're all just providing easier ways or more choice for the consumer for how they pay for goods and services. We at RSA, look at these, and we try to identify all the different I'll say attack vectors or ways in which a fraudster can take advantage of these new methods to commit fraud.

**Rihonna:** Yes, and with that extra convenience, comes the issue of lower security checks. It's a balancing act for these companies to protect themselves without risking losing customers over a lengthy security process.

**Jim:** That's correct. The way I like to say it is whenever we see these new methods, these new approaches. The ways in which credit cards have been protected have been worked through for years, lessons learned from fraud attacks things like that. With these new methods, the fraudsters spent time finding the weak spots in the new processes. Some of these newer companies even newer processes, that's where there's vulnerability.

That's the first times you go through it, it's not as secure. As we learn from the way fraudsters take advantage of these new methods, we can then put controls in place to protect. That's really the danger in some of the new methods is, "Well, what are the ways which fraudsters can break in and commit fraud?"

**Rihonna:** What security checks are in place right now for these services?

**Jim:** Yes. Well, it depends on the company that offers it, of course. In many cases with the established credit card companies that you normally do business with, they're using some **[unintelligible 00:07:43]**. I call them traditional rails of payment. In other words, they may send the payment over a what's called the 3D secure protocol. The 3D secure protocol especially the 2.0 version, is a fairly recent protocol in the world of card not present transaction, the thing I talked about earlier. I.e. when you're using your credit card, typing in your digits on the card, et cetera.

There are some vendors offering Buy Now, Pay Later that are like your credit card companies that you would use a credit card, but the Buy Now, Pay Later happens what we call Retroactively. Meaning you pay for the purchase online and then you go into your bank and you say, "I'd like to pay for that on an installment plan." They're using a lot of the same controls that they're using to protect your credit card, i.e. the 3D secure protocol with fraud solutions like those we offered out at RSA to help look for fraudulent payments. The other piece that for some of the Buy Now, Pay Later what we call the direct Buy Now, Pay Later vendors, you got to remember it's more than just the payment that's happening at the time of checkout.

It's also the time of enrollment. In other words, you're establishing an account with a Buy Now, Pay Later or financial institution to make the payment. That's the part where you're providing, "Here's my name, here's my social security number, potentially, here's my information," they can establish that account a line of credit. Do a credit check to see, "Do we even offer you the Buy Now, Pay Later payment extensions?"

That's where new identity controls need to come into play, and that's where we see the widest spectrum of controls that are out there security controls, we see out there. How secure is that identity check to make sure that it's really you. In other words, why can't somebody else just go up to an e-commerce site and claim that they're Jim Ducharme, say they'd like to purchase this product on three easy installments, steal my identity, establish the credit and then make the transaction?

It's that identity sets of controls that really we're seeing a more of a spectrum of how ready they are for that initial enrollment, or what we call identity assurance check.

**Rihonna:** Okay. The fraudsters are more committing identity theft and these by now pay litter services are medium for profit?

**Jim:** Yes. It's really no different than, even before we had credit cards, stealing somebody's cash out of their wallet, it's just easier to do it now digitally. What's interesting about Buy Now, Pay Later is again, the fraud moves from committing fraud with somebody else's account, i.e. your credit card number, and making a strange purchase. I'm sure almost all your listeners have probably had that case of the credit card company calling you and saying," Did you just buy a train ticket in Germany," if you're in Germany, that might make sense.

If there are any German listeners, they may have gotten the call and says, "Did you just buy a train ticket in Johannesburg?" You go," No," okay, we thought that was fraud, thank you. It's anomalous transactions, that look bad. Some of the differences with these new payment methods, like Buy Now, Pay Later, the transaction doesn't look strange because you're establishing a new account. It's the fraudster that's established an account pretending to be you.

That's where it shifted, the frauds are actually happening, when they're making the purchase. It's actually happening when they're enrolling into the account. That's why the fraud pattern shift. We've got to adapt to where the point of fraud is, and that's why at RSA, we tend to look at fraud up throughout the enrollment, the pay, the management, every part of the customer journey through managing a relationship with the financial institution and making purchases online.

**Rihonna:** Definitely. I like how you mentioned, the customer journey is also the fraudster's journey? [chuckles]

**Jim:** Correct. Yes. That's what they're diagnosing to figure out where is the weakest spot, where is a spot that I can get into that buyer's journey, the customer's journey, to understand my best place to impersonate the buyer. Or in some cases, even impersonate the merchant, you think you're buying something from somebody. It's that whole journey that they're constantly looking at to go, "Where is the weak spot in the entire customer journey, where they can commit fraud."

**Rihonna:** Absolutely. Who, in the process, is shouldering the most risk with these types of frauds? Is it, the service themselves? Is it the larger financial institution behind them or the merchants?

**Jim:** Yes. Well, unfortunately, the answer to most of these things is it depends. In the case of some of the direct Buy Now, Pay Later, it's typically, the Buy Now, Pay Later company themselves, that would be liable for the fraud. In other words, the ones that the theoretical consumer is establishing the account with. I mentioned the retroactive model with credit card companies before, and that's a regular credit card transaction.

The Buy Now, Pay Later is happening again, retroactively. Those falling into the same rules that, your normal credit card liability comes into play. The great news for the consumer is that today anyway, in most parts of the world, the consumer won't be liable for the fraud. In some cases, the merchant could be liable for the fraud, as in the case of some of the credit card transactions. The issuing bank, who you get your credit card from could be liable. Or with these Buy Now, Pay Later companies, could be the one shouldering the burden of these fraud attacks.

**Rihonna:** Would the solution then be to have harder restrictions for account creation for these services?

**Jim:** Well, more secure that you said harder, right? I'm glad you said that because the propensity over time for security, is to make life more difficult for the consumer. Our goal is to have more assurance, is this person that I'm trying to do business with, actually who I think that they are? Over years, when we've tried to make security authentic, this is why I transitioned back to the original question, from an identity provider to a fraud solution, because I spent years in the identity business. Where the solutions that were out there just put more what I call stupid human tricks in front of consumers, to put the burden of proof on the consumer.

There's a tremendous amount of information and intelligence that we can use behind the scenes, to still have a function list, easy, convenient shopping experience, but at the same time, provide a real assurance that this is the consumer I think it is. What we need to put into place is those controls that provide that level of assurance that is to be sure on the other end of this transaction, really try and do, buy a tractor in 12 easy payments. True story I bought a tractor in 12 easy payments. I use that, but again, I went through that experience of signing up for an account and going through the entire process.

We've got to put those controls, that is this actually Jim buying a tractor, and are we actually delivering the tractor to Jim? That's that identity assurance the account enrollment that needs to be strengthened, not made more difficult for the consumer. Using artificial intelligence, using information, we can provide a high level of assurance that this is who we say we're dealing with.

**Rihonna:** Right. We want to add those controls without taking away that convenience for the buyer?

**Jim:** Bingo. That's exactly right. If we've done that we've failed the entire purpose of having more ways to pay, we want to make it easy. The one thing the merchants and the banks all have in common, is they want to take your money. They want you to transact. For you to transact, they want to make it really really easy. At the same time, they've got to make sure that they have the right security controls into place to ensure that it's not a fraudster robbing them off.

**Rihonna:** Can you explain how those controls work, the identity authentication.

**Jim:** Identity authentication, or what they call identity assurance now, really is about looking at data points. I wrote a white paper one time where I talked about, I saw somebody in the airport in Chicago. If you think about- forget technology for a second, think how your human brain works. If you saw somebody, a friend of yours, in Chicago, if you're not in Chicago, this doesn't help. You're in Austin? You're in Chicago and this person looks like somebody you know, but they're out of place. There's something wrong. What the heck are you doing in Chicago? I had that experience once, with our CTO.

I saw her in the Chicago airport. I'm like, "Is that actually you?" Think about why my brain did that because there was something out of place. It looked like her, but I didn't expect her to be in Chicago. A lot of these fraud solutions work in a very similar way, we look for patterns of good and anomalies against a character. For example, if I were to make the transaction online, and I showed up on an Android phone, and I've always used an iPhone, that's weird.

That's an anomaly to my normal pattern, but we establish these normal patterns to provide that verification level of assurance, how is this, this person? Likewise, we can share intelligence, for example, what we do with like the **[unintelligible 00:18:46]** global data network is we actually share intelligence where we know, "Look, we've seen this device, we've seen this network address. We've seen this geolocation be part of a known fraud event. We saw this person rip us off yesterday, over here in another bank, another merchant, et cetera."

We can take all this data about purchases, et cetera, established profiles or patterns of good, to give us some confirmation that, it looks like Jim used to say, "If our CEO showed up in a tuxedo, it would look weird because he was always wearing jeans and a t-shirt." If Steve Jobs one day, back in the day, if he would've showed up in a three-piece suit, everybody would say, "That can't be Steve Jobs," because always wore the pattern, the standard black t-shirt, and jeans. It's all of those patterns of data that we look at that provide us that level of assurance.

For us, and I would say, we call that a risk assessment, and based upon all that patterns of good and risk factors that we see, we establish a level of risk. It's also in combination with, look if I'm using Buy Now, Pay Later to buy a $10 item in three easy payments, the level of risk is lower than somebody's buying a $30,000 tractor. The risk is low because is the risk of loss. If there's truly is a fraud, they ripped us off for $10 versus $30,000. That's all goes into the computation of risk of how risky is this transaction? How sure are we that this person is who we think they are? How sure are we this is a transaction that they should be doing, and if it is indeed fraud how much are we out?

What's the damage, if it turns out to be fraud? You'll see this spectrum of decisions being made all the time online of the level of risk that are merchants assuming to complete the transaction. Again, even if they're not 100% sure they look at it and go, "Look, worst case is a $10 purchase, I'm going to let it go." Because I want them to come back again. That's the simplest way I can describe how you assess risk in a transaction. How you decide whether or not to complete a transaction or not and to balance convenience with fraud allegation.

**Rihonna:** Got you. I really like how you compared it to the airport metaphor of like, "Would I normally see this person here?" taking that human nature of us, looking for patterns and that uncanny valley effect of, "This looks slightly off, so this probably isn't right."

**Jim:** If you think about what I did in the airport is, I wasn't sure, so my assurance was looks like her, walks like her. I then did a human version of step-up authentication. I said, **[unintelligible 00:22:06]** is that you?" She said, "Jim is that you?" There was an additional interaction that we had that raised my assurance that it was her. I asked her her name, she told me my name. "Hey, it is you?" You see this in the fraud world digitally all the time.

This is why frauds just create synthetic identities or even try to do identity theft by impersonating somebody. We're seeing this all the time where people try to impersonate somebody, and they'll get the answers to all of that. They know what the answers to questions might be, or they know things that will help fake somebody into thinking it's Jim Ducharme, that you're doing business with when indeed it's not.

**Rihonna:** With the synthetic identity part, with these services being so new, and with them being catered to a market that may not have prior credit history. It doesn't seem so hard for a new account that maybe has never been served any credit to pop up one day.

**Jim:** That's correct and that is part of the problem. You mentioned it earlier with folks with little to know or bad credit history, or under service markets that don't really have that. That is the problem is there isn't enough data points in the world, in some cases, to get that assurance if you will. That's where the problems become difficult, where is this actually a human on the other side that's creating this account, and how do we verify that?

That's where it starts to get difficult, and where the challenge comes for the industry is how do we work together to provide identity assurance. That this actually is a person. Again, if you think about it as if it's a human we've never seen, we can still use a lot of those factors of, "Well, there seems to be a lot of new people coming out of this one IP address or this one geolocation. Either that's a big apartment building with a whole bunch of people that just don't have a credit history, or that could be a center of fraud."

Don't just think that I have to identify it's Jim Ducharme, I have to identify, what's the likelihood this is actually a human that is fairly new to the credit industry or as a person at all? It doesn't have to just be with credit history, it can be with just about anything. Any interaction that they have in the world in library card, driver's license? Is there any sort of fingerprint we can point to that identifies it that's actually a person. Including things like the device that they're connecting to. Is that device owned by a person with the same name or even something we can correlate.

**Rihonna:** I think that's really awesome how many like you said, data points we have available to us, what we're able to look at how you said, the location or even just the name attached to the device that they're using. With our world being so ever-expanding we are also given new data points that we can use.

**Jim:** I'm sure some of your listeners have put their tinfoil hats on at this point because whenever I talk at all the parties I go to and these all sound like horrible parties. People immediately say, "Oh my God it's an invasion in my privacy. A lot of these data points may feel like an invasion in your privacy. It really isn't about identifying, what do you buy all the time? Even things that are personally identifying, but some of this is looking for the behavior of, is this a human? Do you go places? Do you interact with the website like a human or does your interaction look like you're a burner phone sitting in a lab that was born?

The phone was turned on yesterday for the first time and hasn't moved. There's data points that we can use that still give us an assurance of, is this a human? Is this a person? Is this this person without too much invasion of privacy? That's the other piece I would say, I know we've drifted way off Buy Now, Pay Later, but it's all elements to how do we then provide that identity assurance that this is not a burner phone, this is not a bot committing fraud. We have to deal with these dimensions of fraud, in many cases, but especially in Buy Now, Pay Later with synthetic identity, identity theft, account enrollment fraud are the major attack vectors for these new convenient payment methods.

**Rihonna:** Wow, I think that covers my questions that I had for you. Jim, is there anything else you'd like to touch on?

**Jim:** I think we covered a lot of ground, I think I've drained what I can today.

**Rihonna:** Thank you again, Jim, for joining us today for this podcast, I really appreciate you taking the time out of your day to chat.

**Jim:** Absolutely. Thank you so much for the time, it was a lot of fun.

**Rihonna:** Thank you for listening. You can find this podcast along all other episodes of Fraud Talk on acfe.com, Spotify, iTunes or wherever you listen to your podcast. This has been, Rihonna Scoggins, signing off.