**Sean Carter:** Hello, my name is Sean Carter, President and CEO of NEACH and co-leader of the Market Intelligence Workgroup for the Center for Payments™. I'm really excited to be joined today by Mike Timoney, who is the VP of Secure Payments at the Federal Reserve Bank. Mike, why don’t you introduce yourself and we'll get started with some of these hard-hitting questions on Synthetic ID.

**Mike Timoney:** Thanks, Sean. Yeah, Mike Timoney, Federal Reserve Bank of Boston, where I lead up a team called Secure Payments and our focus is really, as it implies, trying to make sure that the payment system in the U.S. is secure. Really try and cut down fraud, make it efficient, try and help the industry, a lot of the work we do is really collaborating with the industry, Sean. That's really our focus.

We're expanding into some other things now, obviously, with a lot of the newer payment types that are coming out and trying to understand the impacts from a fraud perspective in the U.S. So, I’ve been with the Fed a couple of years now, prior to that, I spent 25 years plus in financial industry, mostly in payments and product within a large financial institution. And, even fraud, I was there for 12 years before I joined the Fed. And so that's sort of why they pulled me in, they wanted a little bit of fraud experience. So, I'm happy to be there.

**Sean Carter:** Awesome. We're happy to have you at the Boston Fed, first district! So, a little shout out there.

So, the reason we wanted to chat today, I hope everyone's aware, the Fed has done a ton of work - three papers on Synthetic ID - and one of the questions I initially had was, what was the reasoning for the Fed to get so involved into this particular topic in the fraud space of Synthetic ID?

**Mike Timoney:** Sure. And actually, Sean, it evolved more from the work that the Fed was doing back about three years ago, in 2018, really doing a lot of secondary research on where we should focus. And you know, as the payment security work was evolving early, that was the time it was really getting kicked off. Where should we spend our time.

And at the time, some of the biggest things that came out was a lot of data gaps and inconsistencies across different types of payments and things of that nature, around payments fraud. And so, you probably saw that we did a lot of work just in trying to come up with definitions and things like that. But one of the themes that came out was actually, Synthetic Identity Fraud.

It came up, it raised its head more than one time. And people were mentioning it, right? And so, you know, we heard at the time that it was one of the fastest growing financial crimes. It's not well understood by the industry, that it's under reported, those types of things.

And so, we kind of felt, hey, this is something we really should focus on. Because if it's under-reported, people don't know about it, and if they're not doing anything about it, we're vulnerable. And so, that's why ultimately, we said, we need to focus on this. And as you mentioned, we've spent a bit of time and research and effort to do that. And yes, put out several papers on it.

**Sean Carter:** As you guys have gone through this process, around Synthetic ID, what do you personally, think is the most surprising thing? Is it that it is so under-reported or misunderstood? What do you find the most surprising out of the work that the Fed has done?

**Mike Timoney:** So, there's probably a couple things there Sean, but probably the one that still amazes me, is how many people don't really know what it is. And, I've been talking on it for a couple of years now. And, I'll even talk about myself just for a second.

In my previous role at a bank, I ran a fraud organization, but it was on the commercial side of the business. And really, I would hear my peers talking about Synthetic, you know, 10 years ago, or several years ago.

But I never, it never impacted my portfolio. So, I never really paid attention to it. And it wasn't until I joined the Fed and we started doing this that I went, oh, wow, this is really the magnitude of it.

So being in the fraud industry, and I wasn't even really exposed to it, because fraud is a big business. And you know, niches that you can be in, right and so, so once I really started understanding as well, it's no surprise to me, people didn't know what it is. But that's probably the biggest thing that I see today is that even after all the work we've done, I get asked to speak at a lot of different conferences, and I just did a couple in the last few weeks. And we have some polling questions in there.

One of the polling questions I have is, who knows what it is, right? It says, do you know a lot? Do you know a little? Do you know nothing? And I'm still surprised that about 25 to 30% of the time it's, “I don't know anything about it. That's why I'm here.” And then then the next largest group is, “I've heard about it, but I really don't know what it is.” I mean, they've heard the term, they maybe know a little bit about it, but not much.

So, still I'm seeing, you know, 60 to 70% of the people really don't know much about this. And, so is that a surprise? That's probably the biggest thing for me is that even with all the media that we see about it, the amount of the amount of work being done around it - is that it's happening.

The other thing that surprised me too, is it's not just in banking. It happens in all kinds of industries, whether it's insurance, automobile lending, you and I were talking a little bit about the Marine buying boats and things like that. Health care, it happens across the board. So, you know, my focus is payments. But as we dig into it, it happens across all these industries. And if you think about the last year with the pandemic, and unemployment, it just boomed in the last, you know, last year because the fraudster said, “Hey, we got a new way to go”. Right? So, they could go a different direction.

And the last thing I'll throw out there is, really that, beyond that fraud, unsettling as it is, it's also used for things like human trafficking, terrorist financing, all the things, the bad things that we also don't want to have happen. So, it's not just about the fraud, but it's about that human element that also is going on out there that, you know, again, it's scary, it's the bad part of what we have to deal with every day. Right?

**Sean Carter:** And I'm glad you touched upon that, because they're, you know, anytime we talk about fraud, right, I remember after 9/11, we would talk about payments fraud and how terrorist financing and you know, the shame that is the trafficking in this type of stuff that's happening. After completing the work with the Fed, do you feel that there's a chance for the education to be broad enough to all the industries that you just talked about, right, beyond payments? Because we all know, when the Fed gets involved, specifically, what you guys did with faster payments and bringing collaboration, do you see this as a real opportunity for the industry to get educated on the topic and maybe stop some of those negative consequences? Obviously, it'll never get to zero, but what are your thoughts on that?

**Mike Timoney:** Yeah. And so, I'll throw this out, because I didn't say at the beginning, Sean. So, you know, a lot of the opinion, the opinions here are Mike's, from the research data don't necessarily represent that of the Fed. But yes, I think it's a huge opportunity. You know, in my research, and in the conversations I've had with people in the industry, knowing that they don't know enough about it, the more we educate people, the better it's going to be.

And in fact, if I didn't feel that way, we wouldn't be doing some of the work we're doing. In fact, some of the work that we're going to be doing later this year is really trying to, again, make people aware of the problem, help them understand what it is be able to educate them, but also maybe try and put some of the tools in their hand to address it when they do start to learn about it.

Because one of the things that, you know, that I guess it's a good feeling when I do a presentation. And obviously for the last year, it's been mostly virtual, but even when I was doing them in person, you know, you'd ask that polling question, “who knows anything about this?” and not a lot of hands went up in the room?

Then you tell everybody, right? The doom and gloom story, and they all come up to you afterwards and go, “Oh, my gosh, I learned, you know, I learned something today. Now, what do I do about it?”

And I couldn't, I don't have something to literally hand to them and say, “Take this, this is what you need to use to protect yourself.”

So, with that, you know, we've been talking to a lot of people, and we're really, we want to create a way to educate people, but also try to help them as well. So, what that looks like we're still developing. But ultimately, we'd like to put some tools in people's hands to say, here's how you can teach your people what it is. And if you do encounter it, here are some of the things that you can do to help yourself.

**Sean Carter:** That's, that's really interesting. And that's good news. The Center for Payments™, we just completed a survey on online account opening, with over 500 organizations, and of the percentage that don't offer it - 65% said because of risk and fraud. And so, when you talk about having tools for people, you know, it's really important.

When you hear something like, digital account opening, people being hesitant to do that because of fraud, you know, does that kind of “juice” the work you're doing and trying to develop tools for people? Because there's so much that goes around that the underbanked and getting people. You know, even during the pandemic, being able to conduct business or open a new account and to have fraud be the reason it's not happening it must give your work that much more relevance to you.

**Mike Timoney:** Well, yeah, I mean, one of the surprising things I didn't necessarily say is that when we started digging into this, I was actually kind of surprised by how much Synthetic Identity Fraud happens in person. It's not all online.

And so, when you say that 65% are not even offering it, that's a big number in my mind, because again, I worked for a large financial institution, and guess how they do a lot of accounting opening? They still have branch, but they do a lot online as well. And so, I think a lot of people think that Synthetic is tied to online a lot, and they don't realize how much actually happens walking into a branch. You know, if I have what looks like a good social number, a driver's license, I have a great credit score, right? Because I manufactured this, this identity.

And I sit down, I have the confidence to walk in and sit in front of you, Sean, and say, “Hey, I'm looking for a loan or I'm trying to buy a house or I'm trying to buy a car or a boat,” or whatever the case may be. You run me off the credit bureaus and you do your KYC and everything all comes back good, then you're going to think, “Hey, I got a good client here” and an offer it up. And, and that to me is, If we can help people in those situations, you're not necessarily using all the same technologies that might be done on an online application in person, right? And it would, and I think just being able to understand that it can happen in person as well, is big.

I tend to not go to the branches as much, even though I work for a bank in it, you know, because that's just the way I am. My kids, I don't think my kids have been in a bank branch, to be honest. But there's still a lot of people that go to branches. And so, we do have to take that into consideration. And I would hate to think that people are afraid of fraud, and not to offer it online. Because fraud can happen anywhere. That's my point, ultimately.

But when you do it online, yes, you probably need to have some other controls in place that are different than the human element. Right? When you walk into the branch, you're at least under a camera there, you know, picking you up, maybe today you have a mask on. But you know, you have all these papers and everything. So, there are certain controls that happen in person that don't necessarily happen online. But I think what we've seen with Synthetic, is that as long as you have a multi-layered approach, to look at different elements, it can be effective. I mean, there's a lot of account openings that happen online, and they're not all fraudulent. And, and a lot of fraud actually gets stopped as well. So, you know, I think it's a mix, but we're hoping whatever we do can help across the board. So we're looking at it from both perspectives.

**Sean Carter:** Yeah, that's something that struck me as I dug into this issue, reading your papers, working with some of our FI members is the confidence it must take to walk into a car dealership, or to buy a boat off the lakes, and just use a fake identity. I mean, do you think when someone's in person, that maybe a guard gets let down a little bit? Because in the back of someone else's mind is no one would come in here with a fake? Do you think there's some something to that?

**Mike Timoney:** I definitely do. Yeah, I mean, so you know, I think about it in a different perspective. But yes, absolutely. If you're going to walk in, and, and you got to have a lot of confidence, right? If you walk in your shaking, and whatever, you know, you maybe you set off some triggers. But these guys are good, right? They know, they're confident they've done this before, and they just walk in, and they own that identity, right? So, I do, I do feel that, you know, you sit and you're sitting in front of somebody, they got all this great paperwork, their history looks good, they're confident, you know, maybe I don't know how they're dressed, it doesn't matter. But you know, you're going to look at it, and you probably do look at it in a different way.

I, for the first time, in a long time, I did actually have to go to a branch for something, and I and it was, and I had to sit down in the office of the, the bank manager, whatever. And I really feel that I could, you know, he was looking at me as an individual and my credit, and all those types of things. And maybe some of that was, he's sitting there going, I got a good customer here, right? Because he's looking at what my background is and what I do and you know, salary, and then my credit and all those kinds of things versus if he can't see me online, there's a different perspective. Right? I think image is a large part of that as well.

**Sean Carter:** Really interesting. Yeah, and I think one of the things we talked about a little bit before, you mentioned a multi-layered approach. You know, do you see AI being a way to attack this problem, or, you know, at least be one of the key pillars that an organization has in the toolbox to fight against? fraud.

**Mike Timoney:** I do.Yeah, absolutely. In fact, I just actually started some work on our team as well, looking at how AI is impacting fraud and how it's being used by the industry. And as we were writing the last of our three white papers, we talked to a lot of tech companies and folks that are using machine learning and AI and that type of thing as well. And that's really how they are solving some of the problem around Synthetic.

And really, if you think about if people aren't really aware of what AI does, it does a lot of things. But one of the things that we saw and mentioned in our paper is that, you know, KYC only covers so much, right? It doesn't validate your identity. It validates some information, *key information* we all have to comply with. Right? But it doesn't tell you that I'm Mike Timoney per se, right? It doesn't connect me.

One of the folks that we were just talking with recently, mentioned that what's one commonality that all our identities have? At some point, we all had parents, right? So, if someone comes in and is applying, let's pretend they're doing it online, and you're checking them out, and you can't find any parent path through this extra data that AI can help minute manage, then maybe you got a red flag, right?

And I'm not saying parents have to be alive. There's all kinds of reasons why things are different. But there's so many other data elements out there that for us humans, it's hard to manipulate and look for relationships and all that, but AI can really do a lot of that.

And basically, what it can do is analyze huge datasets much faster and more effectively than we as humans can, in much shorter time. And ultimately identify some relationships and characteristics that are common across it to, you know, to really try and help say, “is this Mike Timoney? Is he a real person?”

If they you know, if they go out and it's running this data? And I don't have an email address? Or maybe I don't have my cell phone just was open a week ago? Or, you know, I don't have parents, right? Or I don't have, you know, other things that I have in my life, right? Like I have a medical card I have, I have medical insurance. But if I don't show up in some data elements, other than what's just used to fill out a, you know, KYC, there's red flags there. And so that's kind of where AI can really help. It can go out and search these other systems, pull it together and say, “is Mike, Mike? Or is Sean, Sean, right?”

Or at least it can come up with something to make you check it a little bit more, right? To say,
this doesn't feel right, you know?” He doesn't have have a cell, his cell phones brand new, he doesn't have an email address, or he's got 20 email addresses, or wait a second, there's 20 people applying from that address for loans, you know, or that that social security numbers applied for so many loans in the last six months, right?

So, there's a lot that systems can do that we as humans can't get to. So absolutely. In fact, to the point, like I said, I have someone on staff now that's actually doing a lot of work around how AI can help us.

**Sean Carter:** Awesome. And so, last, last two questions here. I did see the news earlier this week. I don't know if everybody else has. But can you tell everybody why it's such a big step that a common definition was agreed to? I've been really excited to hear that. Because, you know, I think that does help.

But can you explain to folks why that's a big deal?

**Mike Timoney:** I do. And honestly, it's sort of a wall down to the work we were doing last the last year and a half around fraud classification and definitions associated with it. So, we released our model in June 2020 to try and come up with a consistent way to classify fraud and also define it because, again, if you if you can't define what it is, we've said this multiple times, I think it was our catchphrase, if you can't define what it is, how are you going to stop it? Right? You kind of need to know what it is to stop it. And so. So, when we were doing that, and we were working through it, and we got to the definition around Synthetic? Well, guess what? We came up with a lot!

There was quite a few and we came up with one when we were doing that, that we called it our generally accepted just kind of it was one we were using. And then we realized that was just an interim step.

And so, we did talk to the industry and say, you know, where do you think we should follow this up? And so absolutely, they said yes. So, we ultimately pulled together a group of experts around Synthetic - small focus group, and said, let's define it. Let's keep it simple. You know, but its got to be simple, but it also has to represent what we're trying to do here. And you’re right, we just published it last week, Sean

What we found, originally, was that a lot of the definitions went all over the place. Synthetic, I mentioned is a big industry. But we were really trying to really look at it from the payments perspective, and not just try to tie it to bust out because what we saw a lot of times it's talking about build your credit and bust out. And so we said, well, there's more to it than that synthetic identity can also be used for other things.

There's what we were thinking through is that, yes, obviously, there's a financial crime associated with it. But we found that a lot of people also tried to use it from a credit repair perspective. You know, you've probably heard of CMOS, right. And so, you know, credit numbers that are used out there to replace your social to help you rebuild your credit. It's not to say it's not legal, but it's stuff happens - but the intent there wasn't necessarily for fraud, it was to try and build your credit back. Right?

So, we were really trying to take a lot of things into consideration while we did it. We did just publish it. And surprisingly enough, I'm glad not surprising, actually, we're getting a lot of good press on that. I just read an article yesterday that actually said, it's about time we have a consistent definition. And again, that validates what we've been trying to do.

But it all comes back to - if we can't really define it, then how do we either speak about it together? How do we know we're even solving it, and then at the very beginning, I talked about it being under reported, if we don't treat it the same, or think of it the same way, we may be, you might count it one way, Sean, I counted a different way, someone else counts in another. And it's 1/1/1 instead of three, because we're not we're not looking at it the same way.

So, we're, you know, we figure that having a consistent definition, it should ultimately then allow us to really understand the magnitude of this problem, because again, at the very beginning, I said, it's often under reported.

The other thing I didn't mention around Synthetic, and if your interest or not, but one of the things that we also found a lot and this is where I think the definition can help as well, is that a lot of people currently book it as a credit loss, right?

They're not booking as I said, Synthetic, because they don't know, you know? Ultimately someone bought the car, right? They stopped making payments on it. They go to collections. They go out there to try and find “me” to get the money back or, or whatever, get to pick up the car. And guess what, I don't exist, right? They show up, there's no house, there's no address, there's no car, and they're out the money.

So, what do they do?

They book it as a credit loss because they made a bad credit decision. But ultimately, if they had investigated more, they would have found that “I” never existed in the first place. And it should have really been booked as a loss, as synthetic fraud loss versus a credit loss.

We’re trying to work through how do you define that properly, so that it gets booked appropriately, so that we have a better understanding of the problem?

**Sean Carter:** And that's really interesting, when you carry that into a payment scenario. You probably have people logging things as credit loss that are, you know, payment wasn't funded, and actually nobody was there to fund it to begin with. Now it could be rolled into something else. That’s really interesting.

With this definition you have, you're getting some good press. What are the next steps for the Fed? How do you plan to engage, let's say FIs, or maybe down market to auto dealers or places where this may be an issue? What's kind of next for the Fed as you play a crucial role in trying to solve this challenge?

**Mike Timoney:** Yeah, so I will say things like this, Sean, the opportunity to speak to a group like yours, I think it's invaluable to us to get to a group that has a diverse constituency that you can share with your group. There are other associations out there, obviously, some of your peer organizations that we'd like to talk to as well.

Getting out in the in front of people in you know, whether it's in conferences or in publication. Again, we continue to try and do that.

We're going to continue trying to push with our with our papers, make sure that people understand that. We're going to continue around socializing the definition because we just came out with it. So, we want to be able to do that quite a bit as well.

And then that other piece is really what I'm calling the Synthetic Identity Fraud Mitigation ToolKit. Now, that's a lot of words, but we'll pare it down. But really, what we're doing is we've just kicked off an effort to really talk to the industry. We're reaching out to a group of people. We'll be putting a survey together as well to get out there. And so, we're very interested in feedback when we get there. And what we're trying to do is pull together we're calling it a ToolKit.

But there's a lot of interest in how to solve the problem. And again, I mentioned it earlier, but it's really about how do I put the tools in your hand to help you with it. And so, we know, we know that the financial industry has a lot of big players and a lot of other players that are out there that need some of these tools. And so, we're actually soliciting from them, you know, what are the things that can help you here, and then we're going to, we're going to try and build this tool out.

I'll call it a “ToolKit”, we don't know exactly what it looks like, but we're hoping to have things in there that will ultimately address education, will address how to look for the problem. What to do when you find it, because very important, right? And then how do you protect yourself?

As the Fed, I can't necessarily recommend technology solutions but we're going to at least have a section hopefully on technology, that'll say, here's the kinds of things you should be looking for.

So, you asked about AI, you know, here's the kind of things multi-layer should be looking at it. Because when I think of multi-layer, I think of putting, you know, if you have your house and you put a fence around your house, then put another fence, then another fence - you might get over one fence but getting over two might be hard or getting over three, you know, you want to block them out, right? So, what multi-layer can do.

And so, again, like I said, that's what we think will be in the toolkit. But we're again, we're asking the industry what they think would be helpful, and soliciting some of that feedback so that when we build it and deliver it, it's something that's going to be used by folks,

And we expect that that will ultimately help the industry in general. I mean, our goal is to try and make us more secure at the end of the day.

**Sean Carter:** Awesome. Well Mike, on behalf of Cerner for Payments™, I can't thank you enough for taking the time. And this work has been great. I'm fully captivated by all the papers, really interesting stuff. And I know as part of this that we're going to send out to folks, we are going to link to the papers and the new definition. And so hopefully, everyone can first understand it and then we can start to challenge and fight back because as you mentioned, there's some evil side to this. You know, and that's what we all want to get after. So, again, thank you for your time and look forward to seeing you around.

**Mike Timoney:** My pleasure. Thanks, Sean.

**Sean Carter:** Take care.

**Mike Timoney:** Take care.

**Resources**

Synthetic Identity Fraud: Defined It to Fight It:

* <https://fedpaymentsimprovement.org/news/blog/synthetic-identity-fraud-defining-it-to-fight-it/>

Defining Synthetic Identity Fraud:

* <https://fedpaymentsimprovement.org/wp-content/uploads/synthetic-identity-fraud-definition-overview.pdf>

Synthetic Identity Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors (July 2019):

* <https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf>

Detecting Synthetic Identity Fraud in the U.S. Payment System (October 2019):

* <https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-october-2019_cover.jpg>

Mitigating Synthetic Identity Fraud in the U.S. Payment System (July 2020):

* <https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2020_cover.jpg>