Where Do We Go From Here?

Thursday, October 13th, 2022

SPEAKERS
Erika Bailey, Seth Rudan

Erika Bailey 00:04
Welcome to Reinventing Banking, a special series of The Slant podcast brought to you by Bank Director. This 12 part series, sponsored by Microsoft, focuses on innovative companies and thought leaders in the financial technology space. Hi, everyone. My name is Erika Bailey, research analyst for FinXTech, at BankDirector, part of my job is to live in the FinTech space, soaking up all the information I can either by vetting, researching or interviewing bank-friendly technology companies, and even if not the primary focus of their product. So many of these companies highlight their fraud prevention measures and tactics. In today's episode of Reinventing Banking, I talked to Seth Ruden, Director of Global Advisory for the Americas at BioCatch. Now, BioCatch is a behavioral biometrics company that helps financial institutions fight fraud, among many other things. We talk about what it means to proactively fight fraud, the evolution of the crime, how data analytics grew to be an invaluable resource and what banks are actively protecting their customers against today. And to start things off, we couldn't help but to revisit our love of classic rock and roll. We hope you enjoy today's episode and thanks for listening. The first thing I do have to say, when we chatted on Tuesday, I know kind of went on a Zeppelin rant, and started listening a little bit more and I I slept on Zeppelin too I think I did I did because it's got the first album sound but I think does, but I mean like how do you skip over Moby Dick Or Heartbreaker? A whole lot of love is that intro.

Seth Ruden 01:43
It's so much more bluesy. They really do that more of that like "bluesy-Americana" thing where I think we were talking more about like how they were bluegrass and kind of has the folk-y or sound later on. But yeah, Led Zeppelin 2 and even 3. I mean, the first 3 I think are are good. That could have been a whole band.

Erika Bailey 02:03
Oh, absolutely. And it was a very specific errors were like 69 to 72 or something like that. And then like you were talking house graffiti or physical graffiti, excuse me, and then HOUSE OF THE HOLY. All these different things, but you speaking of like Pink Floyd, you don't seem like a folk person?

Seth Ruden 02:20

Oh, no, for sure. I know. I so my dad's from New Jersey. And he's like Ian Anderson, Jethro Tull, Neil Young. And the my mom is from Venice Beach, California. And so I got like, my fill of the dead and between the two they they really gave me a really deep education and Crosby, Stills Nash and Young Buffalo Springfield and, and all that stuff. Like there's just really fun things to play on guitar, and around the campfire. So I got a on Saturday, my friend throws an annual and she's got a band, her friends of bands, and we all get together in her backyard. And and we just carry..what's what's the word? Where you just like, have an extension cords up your extension cord? And, and oh, I'm Jerry-rig it. Yes. I know. Yeah, we'll we're all going to, you know, it's like it's like supposed to be acoustical, we'll plug in our acoustic guitars, throw a bunch of pedals at them. And that'll work. And that'll totally work. Oh, does every time. I mean, I can't believe her. Her electrical system tolerates it, but we do this every year. And right as like Oregon descends into its rainy season, or last days of sun. And we have a really fun jam with like, 30 people on guitar. And yes, it's a really, really great time. And so that'll be all folk music, and, blue grass all that stuff.

Erika Bailey 03:44
You would have done. Excellent. So our company we do a Giving Campaign every year. We pick a few charities we do this thing. This year, partying as part of the committee, we decided to have a decade's theme. So we did 60s 70s 80s 90s 2000s. One of the games was kind of like "Guess That Tune" situation. I think you would have killed it. Yeah, absolutely. I embarrassed myself pretty bad. I talked to big talk and couldn't walk, unfortunately.

Seth Ruden 04:10
You know, give me a give me a question real quick.

Erika Bailey 04:14
Oh, I mean, do you know Simon and Garfunkel pretty well? Yeah, great. They had, um, there was a song is the box, something like that? Or "The Boxer?" And, and we were planning what the heck is this thing? And then one of our co workers. I mean, she slammed it. She knew instantly I was. I was flabbergasted to be honest with you. And then all of us are like, Oh, no, it's this other. It's others. Simon and Garfunkel tune No, she was absolutely right. She got it in like five seconds.

Seth Ruden 04:45
I wish I was better at Simon and Garfunkel. I don't know "The Boxer" so you're probably right that's that's a that's a deep cut, I think. And that's from Bridge Over Troubled Waters, which is one of their better albums Right? Absolutely. But I don't I'm not that thorough. I've got all my folks records and we listen to them on the regular but I don't have I don't have bridge. I've got Graceland.

Erika Bailey 05:10
Okay, um, you majored in economics? Is that right? finance? Finance? Okay. Did you go straight from graduating college into the bank space?

Seth Ruden 05:21
I did. Yeah, I was a technique. I was a mechanic for so many years. And, and my first gig was in compliance and at HSBC. And that's where I got my start.

Erika Bailey 05:34
Got your start.. And then I know, we talked about what your credit union for a little bit and then, and then was it BioCatch right after?

Seth Ruden 05:41
So I did a bunch of consulting after that. I was with Fiserv working on card fraud rules and strategy. And then we went to Asia. And I started doing consulting on online banking, fraud detection solutions, and came back to the States did kind of the same thing, just consolidated it card, and online banking, to make like enterprise. So you can see between the card side and the online banking, if somebody was doing cross channel attacks, and then then I got into, I mean, my credit union needed me. So it's time, time for me to lead the team and take everything that I've been doing for so many years to to practice. And so we did what we needed to do with the credit union; turned that ship around in turn, I got them healthy, and then I get to go back to my, my safe space – vendor land.

Erika Bailey 06:39
I'm in college, I mean, did that finance degree...How did it prepare you for getting into the fraud space, because a lot of that, I feel like you learn on the job?

Seth Ruden 06:50
Well, you learn a lot of key concepts that are really important to understanding how it all fits together, you know, you, there's no education. There is now but at that time, there was no education in the fraud space. There was no specific capacity to learn how to manage card fraud rules, which is kind of where a lot of the other disciplines have emerged from. So card fraud was was the first space that we needed, these prevention controls that were like working in flight and putting those declines so that you can have that experience in the shopping center checkout line, where you get to decline and get embarrassed. And well, the card worked this morning, you know, but now, we needed to take those principles and apply them to online banking space, and then apply them to P2P channels, like Zelle, and apply them to, you know, every other channel. Yeah. So that didn't quite exist. But you know, when you get a finance degree, you learn the language of, of money. And, you know, you have to know these kinds of things in and understand the nature of investing in the technology, or a sunk cost or an opportunity cost and, and be able to leverage that language, that vernacular, to make the case to any other stakeholder in the enterprise that you're working with.

Erika Bailey 08:17
Sure, I'm thinking about when I was in college, so I did criminology as my major and that I mean, focuses a lot, a lot of different fields. But it's all you know, fraud, or, or FEMA, or Homeland Security, or all these different things. And me graduating with that degree, I would not

be anywhere near ready to take on a gig like that, or get into the actual fraud space, because it's just so let's glance over it. This is kind of some of the language but you're not living in it.

Seth Ruden 08:46
Well, I don't know if that's accurate, I think you probably are addressed meaning where you can apply that in, in this space. You know, there's a lot of different verticals and segmentation opportunities for you in fraud, you know, we we need people who understand the law, and we need people who understand criminal intent. And we need people who understand how those two dynamics intersect. I think what you're sensing is that I've got a very technology-focused perception of how to organize a business in creating rules and controls and and develop a operation. But when you take an individual with your discipline, and you apply that to the nature of how do we manage process, how do we manage compliance and legal elements? How do we get, you know, elements around a court case, and the handling of evidence and all of these bits These start really create a lot of reliance on individuals who have that discipline and are able to pull from that. Sure, it takes, it takes all kinds. And you know, in the fraud space, I would tell you that if you're trying to grow emerging talent, some of the best places that you can start in is math and science. If you've got a real strong data science background, or you're very good at at math, then being able to use data analytics will serve you incredibly, and that's where we're really needing a lot of new talent to emerge and to be brought into the space. So right now, if you're a math or science major, and you want to do this data science thing, and you know, let's be honest with you, fraud is really hot, everybody really thinks that fraud is a great place to be no one's gonna be bored, talking fraud with you at a dinner party, there's always there's always an interest. And you're going to have to be a little quieter more often than not about what really happens. That's a great place to enter the field and become a, you know, a real niche operator and in a place that has a remarkable growth opportunities. I don't know if this is the direction you want to take this question.

Erika Bailey 11:20
It's perfect. I did want to kind of touch on throughout the conversation, data science, the evolution of it, and you bring up this really good point, I mean, you're never going to be bored. Because what was true yesterday is maybe not true today.

Seth Ruden 11:35
It's such a circuitous route. If you would have told me, you know, 20 years ago, that I'd be sitting in a chair, having a conversation upon a podcast, somebody be interviewing me about my banking job, I would have told you that that's imaginary, that that's not a future that's going to occur. But there's a lot of ways to get into the space. And there's a lot of opportunities to grow in it. And there are many mechanisms where you can find yourself really engaged all the time. And never bored. I think. I can't quote the individual. But I remember hearing somebody somewhere, say, "If you're passionate about the work that you do, you'll never work a day in your life" or something to that effect.

Erika Bailey 12:25

When you were in the banking space, did you find that to be true as well, in terms of banks, needing folks with data analytics backgrounds, or folks interested in that? It's obvious that's probably true working at biosketch, or working in this technology space. But was it true back then at a financial institution? And are you seeing that today in financial institutions?

Seth Ruden 12:46
It's much more true today than it was in the past. And in the past, it was valuable. I think one of the things that I was able to create as a differentiator was the ability to start developing metrics early on, and start to recognize the ability of data analytics as a science to be able to acquire success criteria, and to know what would be good targets. And that became a repeatable thing. And I think I wrote that quite a ways to be able to realize those reliable, repeatable valid outcomes, and have those be consistent and help many clients across different geographies around the world, realize positive outcomes and a better and more secure environment. So if somebody wants to start in this space today, they're going to be better than me at this kind of thing. Because they have all these new tools, and they have all these new skills, and they've got all this discipline that they can bring to the table that you know, we had to acquire early on with no background or nothing. Yeah. Or guidance. Yeah. Just working through it. Yeah. Yes, solving solving new and complex problems. So yeah, start there, for sure. That's, that's the place where, where you'll be able to really benefit.

Erika Bailey 14:10
Sure. I'm obviously not specific conversations in specific banks. But can you tell me a little bit about what type of conversations you're having with financial institutions today?

Seth Ruden 14:23
Well, we have conversations about crises. You know, everyone's got an exposure somewhere. And a lot of the conversations I had are how do we resolve this business problem? Some of these problems are heavily around scams at the moment. So you have a lot of really bad actors who are making outbound contacts either via SMS, text message or voice messages, you know, contacting people telling them that you know, the FBI has this found this problem for you. The DEA tells you that drugs have been shipped to your house, or, you know, you get a call from Amazon's fraud department. And you know, you've had a transaction, you know, somewhere crazy. So that's one. Emails come come regularly to you as well, phishing emails. And, you know, all of these have a way of pulling you into a scam at the moment. And they're really effective, you know, they don't need to have a high penetration rate to be able to be effective at meeting their economic goals. So they send out enough of these, and eventually somebody will take the bait. And I think that these have become plague proportion, in recent years. And we're not that great overall, at getting a handle on it because of how sophisticated, complex and challenging it is to resolve some of these things. And the banks are the ones who are frequently taking it on the chin, as there's a big push on the consumer protection front, to be more aligned to the needs of consumers and ensure that we protect them as much as possible. And globally, there's a big push to reduce their liability. And so banks are starting to take on more of that, and is pushing the responsibility for that protection to the banks. And as a result, they need to be acquiring more technology, more capability, more sophistication, and being able to respond to

these events. And I think that's one of the reasons why I decided to join BioCatch, having user technology in the credit union that I used to manage so efficiently, that we were able to do things that were really interesting, and protecting our members, and and ensuring that they had positive outcomes.

Erika Bailey 17:01
So, you talked a lot about, you know, banks taking on the chin, so they are now taking more responsibility. And as regulation changes, and the shift is happening, so we're almost in a transition. wWhat you were talking about earlier is a lot of reactive things of "this happened and now we kind of have to deal with it." Or as a company like BioCatch are working on proactive of "let's just not even have this be an issue." Do you think because banks are trying to get to that state of let's work with this company, because we're going to get these proactive algorithms, analytics, and we're going to stop this before even happens, versus now we're so reactive in a lot of ways?

Seth Ruden 17:44
It's a big transition, you know, we just didn't have the technology well-deployed. And we were in a generation of technology solutions, fraud prevention, technology solutions that were limited in terms of the data that you could acquire. And along comes new methods and mechanisms for acquiring data elements that looks at things that we didn't conceive of before behavioral elements, endpoint risk, cross channel activity, you know, that you logged into the session, and you had potentially transactions occurring in a channel that you couldn't conceive of. And now that we're starting to recognize the totality of the attack surfaces, something's what we call it, you know, that you've got cards, and you've got online banking, and you've got branch and, and all these fintechs that tie into it, it's created so much complexity in the environment, that there's no longer much of an excuse, or even a reason to sit when all these attacks are occurring. And we need to do something about it. So I think, you know, as, as the old cliche goes, necessity is the mother of invention. Now, we've created situations where we need to be far more engaged and proactive in bringing the fight back to the the attackers. And the right posture to take is an aggressive one. It's not welcome at my institution, and I am going to do things that create better outcomes for my organization and my customers.

Erika Bailey 19:27
It's a hard job, what banks have, because you can only protect what, you know, could happen, if that makes sense. And as new forms of fraud emerge, and granted, we talked about how the environment has to be there in order for that fraud even happen, so it's not like they're going to create a new environment that banks automatically are going to be plugged into so the banks have to create this new thing or technology has to and then fraud will follow. But how do you know what type of fraud is going to follow if you've never had it before? That's a hard job.

Seth Ruden 19:58
It's a challenge. Yeah, that's it. challenge that, you know, you can't manifest this crystal ball, which tells you that they're going to start socially engineering people for multifactor authentication codes. But what we know is that, and exactly to your point, when you when you

create a new channel, you create a new platform to be exploited. And what you have to do is attribute the areas of exploitation that occurred a day to the potential exploitation that could occur on this new attack surface. And so I know that there's going to be mobile pay fraud, you know, the, the mobile wallets, I know that that exists is an attack service, I know that there's account takeover. So now I gotta marry these two ideas, where does account takeover exist for the mobile pays? And are there ways that online banking risks can be manifested to a channel that is diverse, like these mobile pays, because if you try to think in silos, that everything is going to occur within card, and nothing else out of card is going to affect card, and everything online bank is going to effect banking. No, we need to be less naive about how we compartmentalize risk. We need to look at the totality the user journey, and fraud use cases and how they can manifest from different channels. And look, you're never gonna get it 100% right, and I don't think that's the expectation. I think the thing that you need to focus on is being agile enough to be able to take down the emerging risks when they start to come up, and to be able to put down an emerging crisis before it becomes a catastrophe.

Erika Bailey 21:47
Sure, do you think that most customers would leave if a huge breach happened?

Seth Ruden 21:56
Turn is real. We did a study so many years ago, at one of my former organizations, where the question was, if you have a card fraud event, and you're expecting that the way that the event was handled to be better, or that, you know, you have too much loss, or there was never detected, you know, something along these lines, your expectations weren't met. We found that 20%, one in five, cardholders will will find a different bag, they'll leave. And you know, that's, that's a big number, especially when customer acquisition cost is so high. That's a big number to get wrong. And I think that when you have like a complete total account takeover event, I think that number is even higher. And so it's pretty critical to have the detection that you need in that space. I think that one of the things that was really valuable for me, when I was leading a team was when I would get the feedback from a customer, and the customer would say "you found it before I did," and in the discussion with that customer, I would sometimes hear stories of "you know, well, here's what we identified" and "here's the things..." And they were really impressed. And they were very pleased that we were upfront. And that created a greater stickiness and retention.

Erika Bailey 23:21
I mean, how I don't envy the position of a bank of being like, hey, so all of your accounts have been hacked, and we're so sorry, we'll get back to you soon. I can't even fathom having to be put in that position, and then not only do you have to announce that, then you have to individually handle all the calls, all the emails, all these things, which is what a person wants. If my account was taken over, I want somebody to say, "Hi, Erika, this thing happened and we need to find a solution. We're on it." It's a community thing, you know, your bank is supposed to protect you. And specifically, I mean, we want to go into the conversation of community banks, or, you know, you worked at a credit union, this sense of community is so large, but community has evolved. My community bank could be in Oregon, right? I actually bank in Iowa still. I have a

little community bank up there that I've been with since you know, my parents took me in at six years old to open a checking account. That's just where I bank. I would hope that they would personalize that or reach out to me as a customer that they care about.

Seth Ruden 24:38
It's really hard when when you're a smaller entity to be able to acquire that kind of sophistication. And, you know, there are solutions out there. And, you know, I don't want to brag too much on mine. But there are solutions out there that allow you to raise your sophistication and scale like the big banks do with technology that allows you to ingest and work like a more sophisticated entity. But I want to go back to one of your points you were making the beginning of that line. Yeah, God bless the investigators, God bless the specialists who, who really put themselves in a challenging position every day. I saw that firsthand, and I'm grateful that they were so...it's a it's a major sacrifice. I'm grateful that they're so resilient in the face, because yeah, you're dealing with with people who have a hardship, and have a very vulnerable moments. And they go on an emotional roller coaster every day with them. So, for all the bankers out there, send flowers to your fraud ops teams, they're doing some really important work to try to help people in a very compromised position.

Erika Bailey 26:01
Well, and let's think about it this way. So when I was a case manager here in Tennessee, who is the suspect? Who did this? Well, I can tell you who did this crime? Yeah. Who hacked into my account? Sometimes? You don't know. Yeah, that's hard.

Seth Ruden 26:17
It is. It was very limited my career, the number of times we ever had an arrest. I got I have one.

Erika Bailey 26:27
One goldstar.

Seth Ruden 26:28
Yeah, it a was a guy from Bulgaria that was awarded a trip to Guam. And those was brought in from there. So that was, that was my one notable takedown of a bad actor. But it's so infrequent, you know, and law enforcement, they don't have the resources, they don't have the scale to be able to address all of these. And so they gotta go after the big efforts.

Erika Bailey 26:57
Absolutely. I encourage you to talk about BioCatch. You know, you just said you don't you didn't want to brag about your solution. First of all, I'm sorry that I didn't start with this. But can you take me through? What's a day to day in your role? Obviously, I'm sure it's changing every day, you're looking at the space you're in? But can you kind of take me through what your role is at BioCatch? What do you do every day? Who do you talk to?

Seth Ruden 27:21

I'm usually talking to leaders at other financial institutions, individuals who have a problem, individuals who want to solve very complex crises, who are or who anticipate that they'll need something to manage the threats of tomorrow. And really, what I do is I try to share with them my experience and help them understand how I was able to leverage this technology to create favorable outcomes, and protect institutions and then their customers. So what BioCatch does, which is unique and and gave me that advantage, is it no longer looks at just a transaction in isolation, like historical fraud detection, instead. They only looked at a transaction as it was being implemented, and maybe a handful of other elements that surrounded it. Now we're looking at the totality of user journeys. And the second that you log in to your online banking account, we start really collecting a lot of information about that session, about the device, about the navigation, about the engagement about the behavior of the individual on the back end. And this allows us to build a pretty comprehensive picture of the relative risk of the session, and be able to identify the potential that the session is high risk, and has elements in it that we need to address either with a decline on a payment transaction, or if we need to do an investigation because we have elements that we want to alert on. So I'm not gonna go too much into detail about how we how we went the secret sauces, because this could be at a wide audience and mindful of a bad actor who's trying to listen in.

Erika Bailey 29:18
I love how you guys make data colorful. You know, not to go into stereotypes, you growing up data was math, it was numbers. That's not always the case. I mean, of course, if you're gonna put it in a spreadsheet, you do have to, you know, assign it to a value. But you're talking about behavioral analytics of how do I log on? When do I typically log on? How long do I usually stay? These things that create a story, which is so much I love putting math to story. I think it's so fascinating because, going back to music, I mean, music is math. Music tells a story. It's all these different things that you can then use to say hey, this is not EriKa, this is not Seth. Something is wrong. And then I'm sure if you look at the big picture, you can say, Oh, this is happening to many people at the same time. I wonder what's happening? If you had to boil it down to a sentence, is that how you're, you know, quote on quote "reinventing banking?"

Seth Ruden 30:16
Well, what I would say is that we're looking at the totality of the user and their behaviors, and as an end result, their behavioral biometrics. And we're ingesting novel elements of that behavior, to help develop risk signals. This data science, this comprehensive activity that we start to ingest is novel in that we didn't have that capability from a fraud operations capacity when I started on this journey, and that's what's really different about it. So yeah, does it tell a story, we record a story. And we develop the data elements that allow us to compartmentalize these things, and the threat indicators and the genuine indicators that allow us to be better at segmenting, when a journey, or user story demonstrates that there's elements that we should be paying closer attention to. And it really has allowed us to get so much better at differentiating and creating the better outcome for those parties who have a signal that we need to be paying closer attention to.

Erika Bailey 31:43

What do you think is next for you? What makes you excited about what's next?

Seth Ruden 31:50
I love that we're starting to get to a place where we're automating a lot more. And we're beginning, we're starting to get far more creative, and opening our minds to the consolidation of these things. So BioCatch is one technology that allows you to get some visibility across channels, right? So we're historically would say, okay, well, that's a wire transaction; itjust lives in the wire vertical. And then you've got an ACH transaction that lives in the ACH vertical. BioCatch allows you to get between them and say, okay, well, you interacted this way between wire and ACH and that's important because...But now we're starting to say, well, we're going to integrate this thing, the BioCatch, to an another enterprise fraud solution. And we're going to integrate this other thing, which is like a check database, and we're going to bring that into the other solution. And we're going to bring in all these other threat indicators, all these other models, all these other data elements from new channels, new perspectives. And that all gets filtered into one potential risk engine, and executed on. And for me, this is something that I think is is really powerful, that is starting to really be realized today. It's the place where I set my technology roadmap when I was running the team. I think that, once that's fully realized, we're going to make it so much harder for bad actors to engage in illicit activity, that we will hopefully reduce the potential that they have as much opportunity in the real world. Because we've been on the backfoot for too long. We've been trying to respond so many times to emerging threats and risks, that we've been plugging the holes with our fingers in the dam so many different ways that we were always on the defensive. I think this new kind of integrated, API-driven, everything's in the cloud capacity, where we can just send the signals to the destination in real time, finally creates the right kind of mechanisms. And then we automate it with with machine learning models, where we don't have to be awake and having those pillow thoughts of what am I missing? Where am I gonna get hit next? Is this a problem? No, I can relax. The machine learning is in the automation will do what I needed to do and I'm not going to wake up to a crime scene the following morning.

Erika Bailey 34:25
When you were just talking, I had this relevation. Gosh, whenever I think of algorithms and data analytics and things, I really just think of the technology. I don't think about the people behind it that really are having those pillow thoughts of "Oh my gosh, you know, like what did I miss? What did I miss? What did I miss calculate? What is going on right now that I'm not seeing?" God bless that team. Oh my gosh.

Seth Ruden 34:51
It's hard and you know, these these guys are, they're putting in the work. You know, it's not just the the risk inventory and assessment, it's about keeping the systems up and fed and maintained and upgrades, and all of these things that that they have to take into consideration. That occupies so much of your time, right? And you want to have people working on strategy and just strategy and focus there, right? But, we get pulled in so many different directions, because, you know, we're so frequently resource-deprived, and you're only one person? Well, I mean, the team at large. We're not a revenue center by the conventional sense. There's your

finance degree. We're not a revenue center. So we're a cost center. And everyone wants to limit the spend that goes to the cost center. I'd like to invert that thinking, though, and say, well, actually, we're a recovery center, and the losses that already went out, or the ones that we prevented, contribute to the revenue. So, that's a way that we can invert that kind of thinking and maybe get some more of those resources applied to fraud and financial crime students.

Erika Bailey 36:02
What you said earlier about churn rates and the cost of customer acquisition, you lose those folks. Right? I mean, who's to blame?

Seth Ruden 36:11
Yeah, well, it goes all around. And you know, here's the thing, everybody who's... this is a fun topic, I love this topic...everybody who's in a marketing or in a account, acquisition role, or, you know, consumer lending or credit, you know, everybody's got these assumptions that they create, and a spreadsheet that exists. And that says that, well, based on A, B, C, and D criteria, we're going to be anticipating that we're going to have X number of new customers for this product that we're rolling out. And X number of receivables and X number of, you know, whatever - rewards points, and you know, all of those things that go into the the arithmetic, right. What they don't recognize is that fraud can really take the wind out of those sales. And they get that wrong, and they go for the acquisition side. And they do adoption without concern for exposure, for financial crimes exposure, and all that profitability metrics goes right out the window, if you get that wrong. All you need to do is bring in too many fraudsters, we've really created an environment right now, where we've got a lot of synthetic identity or identity theft, with all the breaches that exist in the world today, where that can be really painful to that hard earned credit arithmetic. You need to be looking at it from the lens of "alright, do we have the right controls in place on the backend to prevent new bad actors from trying to establish accounts and and ruin our profitability?"

Erika Bailey 37:54
Yeah, it's almost like the value of these teams. You can't even speak to value. Because it's everything at the end of the day, you lose your customers. Like you said, the probability goes out; the marketing doesn't matter.

Seth Ruden 38:10
Bless your heart, Erika.

Erika Bailey 38:12
Thanks, I do not envy you. But we can help you.

Seth Ruden 38:17
You know, we're standing up these technologies that will allow organizations to be able to go ahead and see things from an account opening perspective, and understand that there's risk there, because bad actors still act the same way relative to bad behavior. They use devices and they have journeys, and they have familiarity with data that regular customers don't. Then they

don't have familiarity with data that real customers do. So the same methods and mechanisms that we use in our account takeover solutions, and our money, mule solutions, and our scam call solutions, we can invert some of the paradigm and say, well, "if good if good people are profiled to act like this, then that people who are opening accounts will act like that." And we use that kind of technology to begin our account opening journey. And that allows us to have high detection and prevention rates relative to bad actors who are intent on using synthetic identity or identity theft, or even just opening accounts in their own names. We can recognize the behavior of a good person versus the behavior of a person.

Erika Bailey 39:34
Yeah, and you bring up a good point, because before we leave, I do want to kind of put first of all myself and our audience kind of at ease in terms of, you know, fraud is something to absolutely be aware of you have to be, but it's not hopeless. Banks can get in front of this.

Seth Ruden 39:54
Yeah. It's about setting up good models. And it's about creating good governance and it's about are setting realistic expectations with the business on what is acceptable and what are the business operating targets and parameters. So, establishing the guardrails, here's how I want you to operate, here's what's acceptable loss when the loss isn't acceptable, here's what we're going to do about it. Creating those kind of operating mechanisms, creates reliability. Ultimately, that's what we're trying to do here. There's no one has any foregone conclusions that fraud is going away permanently. If anything is going to get worse. Right? And it has.

Erika Bailey 40:38
Well, look at the evolution of what's going on. What's the next ecosystem? What's this next marketplace? What's this? Yeah, of course, it's going to evolve, it's going to grow. But you were just talking earlier about, you know, we have a chance here to maybe get on the offensive side, not necessarily defensive. You always will be playing defense, I fear that you kind of have to do that. But we're finally going to get this chance to get in front of this. Or certain models of it.

Seth Ruden 41:08
So, we had a very unique experience in the last three years in stimulus. We gave out nearly a trillion dollars in stimulus. And I think that maybe a quarter to maybe slightly less than half of that went to bad actors. I know. When the movie gets made, you know, I'd love to have William Defoe play a bad guy. Right? So, sorryWilliam, loved you in "Forrest Gump." But you create these ecosystems and the actors who engage in them, and they don't go away. They now have car payments and mortgages. And these guys, they'll continue until we take away the cheese, right? And we don't have too many opportunities to squander on making the right kind of investments because they're already coming. And so it's not a good thing to sit back and wait for the next attack or to feel as if the pressure is on you to be making the right investments in standing up people processes and technology to find those right outcomes. The right thing to do is to set up governance systems and the right kind of business models that allow you to anticipate and accept fraud as a, and everyone will say this always, you know, a cost of doing

business. But, can you make it a tolerable and have an appetite for that cost, rather than wait for the crisis? Because when the crisis hits, it's already too late.

Erika Bailey 41:46
I want to put Brad Pitt in the mix there. That's who my mind wants you. Yeah, that's when FEMA comes in. No, that's great. That's absolutely great. I've really enjoyed speaking with you again, I've learned so much more. And thank you so much for coming on and speaking with us. Really appreciate it.

Seth Ruden 43:11
Cheers. Thank you so much. I really enjoyed this as well, and hopefully you guys can have me back.

Erika Bailey 43:14
Oh, absolutely. Absolutely. We'll get you back. Awesome. Thank you. My pleasure.