THE PAYMENTS SHOW

http://thepayments.show

E92:
Navigating B2B Fraud with Trustmi

GUEST
Juliana Pereira
SVP of Marketing

HOSTED BY
Satwant Phull

[Important]

- This transcript was produced with machine learning and has many ***errors and omissions***

- These timestamps are for the ***audio version*** of the podcast

(00:00) Introduction

(00:00) **Satwant:** Hi, I'm your host Satwant, and welcome to this episode with Juliana Pereira from Trustmi. If you'd like to watch the video version of this podcast, or download the PDF transcript, Please either click the link in the show notes or visit thepaymentsshow.substack. com. Enjoy the show.

Juliana, welcome to The Payments Show.

(00:22) **Juliana:** Hi, happy to be here. Nice to meet you.

(00:26) **Satwant:** You too. Where are you joining from today in the world?

(00:29) **Juliana:** I am in New York city in Manhattan.

(00:33) **Satwant:** Okay. You're headquartered there?

(00:35) **Juliana:** Yes, so our company, Trustmi, is headquartered here in New York. We have an office in Midtown.

(00:40) **Satwant:** Okay. Fantastic stuff.

Well, I'm going to dive straight into it. I'll give you an intro . I think it's going to be an exciting episode.

(00:46) Exploring Trustmi's Mission and Impact

(00:46) **Satwant:** So Juliana, you're the senior vice president of marketing at Trustmi and. Your company provides end to end security solution to protect businesses from things like cyber attacks, internal collusion, human error, and ensuring payments go to the right place.

Would that be an accurate description of what you guys do?

(01:07) **Juliana:** Yeah, absolutely. That's exactly right. So we work with mostly large businesses, but really businesses of any size, but enterprise businesses really see the biggest benefit from our product to do exactly that, to, to eliminate those cyber attacks, internal pollution, protect their supply chain of vendors and avoid financial errors, which are ubiquitous within you know, finance processing business to business Uh, and that's what we do, and we ensure that they do it right, and we always talk about sending the funds to the right person, at the right time, to the right place.

Just getting it right.

(01:41) **Satwant:** Well, as someone who likes watching documentaries, I'm going to love talking to you about internal collusion. You must have some

(01:47) **Juliana:** Oh, yeah.

(01:47) **Satwant:** discuss

(01:48) **Juliana:** Yes, for sure. Yeah.

(01:50) **Satwant:** The scene for the audience to introduce your product because it very clearly states in your marketing that Trustmi, it's not just a security product.

It. Protects finance companies from payment fraud.

(02:04) The Staggering Cost of Payment Fraud

(02:04) **Satwant:** Just to set the scale of what numbers we're talking about. You've got stats showing that, 50 billion was lost on business email compromise between 2013 and 2022. That's staggering. 1 to 3 percent of companies budgets are lost every year to financial errors.

That's very high. I didn't expect that. 84 percent of enterprises were hit by B2B payment fraud attacks in 2022. And even the government doesn't escape. So I learned from your website that 247 billion was lost according to the US government accountability office for federal payment errors.

So that's a staggering amount of money.

(02:42) **Juliana:** Yeah, that was a, that was a specific story in the news for sure. And actually for the 84% uh, stat that actually I just found out last week has been updated. It's 80% of enterprise businesses for 2023, so stands at about the same amount of 80%. But also 41% of businesses suffered losses from fraud in, in 2023 of the, the companies that were surveyed, you know, so these are high

(03:09) **Satwant:** yeah. Massive numbers. Yeah. And.

(03:13) Deep Dive into Trustmi's Solution for Payment Security

(03:13) **Satwant:** Would love to talk through step by step in your solution, how, how you basically could help in all those scenarios through the, you've got a very modular solution from what I've read into it. So maybe I could pick on a couple and feel free to pick something else if you like just a couple of things that really interested me were you know, the payment approval workflow, which sounds kind of dull, but it's, it's In and of itself, but, your software helps to uncover vulnerabilities in, in the workflow detecting suspicious signals and things like that. So maybe you could talk a little bit about that.

(03:46) **Juliana:** absolutely. So, so here's where when you take a step back and you look at the B2B payment process. So when we think about it, when we talk about end to end, what does that really mean? It really means from the first email moment of communication with a vendor who reaches out to you or you reach out to them.

All the way through to building that relationship, signing a contract, you know, getting them onboarded, uploading an invoice, getting all the approvals to then release the payments to that vendor once they've delivered the goods and services, right? Like there's an entire chain that happens there in the workflow.

And so when we talk about a modular solution. Um, Really, there's all these different pieces of the solution, but you need to think about it holistically as a full solution, right? So when we're thinking only about the

approval process, that's the part where people are, there's a chain of people or different teams or people on different teams that are approving the invoice, making sure that it's approved.

That the right person is going to be paid the right amount of the right company. Now, in order to do that and to know and feel confident that you are approving an invoice that is real and that's, you're going to pay the right company. How do you know, like, what, how do you really know that it's the right vendor, right?

Like, how, how can you know from an invoice that you receive that that's the right invoice and it's not a fraudulent one and you're paying the right person? Well, what we do is with every vendor that you work with, we build what we call a baseline or a digital fingerprint. And so we look at, All the communication in the past you've had with that vendor, the, not just the tone of the communication, but the people involved in the communication.

How often are you paying them? Are the invoices being sent? What do the invoices look like? And you know, how is that being paid? Everyone who needs to approve it and, and when you have to make the payment, all of those details. I mean, it's hundreds of data points. So that if we see an anomaly or a deviation from that baseline, we can flag it.

So let's say all of a sudden someone comes in and says, Hi, Nancy, no longer works in the finance department. And now my name is Sasha. You know, and so here's my information. Two days later, Sasha sends an email saying, Hey, can you update your banking information? Because we've changed it. We now want to be paid to this bank account.

Like those. These are two isolated incidents, right? Like they're, they're two data points that individually might not seem like a big deal, but when you go tracking that and then you receive the invoice and something looks off on the invoice, the amount is twice the amount you usually pay that vendor, or the other information is different, or the formatting looks bizarre, all of those things we can flag in our system to then be able to say like, okay, you need to review this.

Because there's, there's something off here about this invoice or what's going on here. It looks like there was a business email compromise or it looks like the wrong invoice was sent or something's up. And so then we can provide that sort of surgically tell the, our, Our partners that we work with, our clients, you know, you look into this area here of this payment flow of the approval process.

But even before that, to the emails that, that led up to the invoice being sent and then being approved. So the approval payment flow is really kind of that one piece where you have all the different people involved. And so, because there's so many siloed systems, so many people that might have to approve an invoice, all of that requires some automation.

And it requires support and also visibility. So you can see who's approving and when to really make sure that that invoice follows the right process and that different controls aren't being circumvented that sort of thing. And so that's, that's everything that we can kind of see there to be able to flag if there's issues.

Right.

(07:35) **Satwant:** Yeah. So that sounds amazing.

(07:38) Understanding Trustmi's Integration and Implementation

(07:38) **Satwant:** But I want to dig in under the hood. So in typical organization where you've mentioned, you know, somebody in accounts might get an email and then. This siloed people in approvals and banking and payments, that would basically mean, according to my understanding, that you're going to have, have software agents deployed and Outlook on people's desks and on the servers and everywhere else is in addition to you hooking into that company's banking flow as well. Is that accurate

(08:10) **Juliana:** so in how we integrate,

(08:13) **Satwant:** Yeah. Because everything you said sounds great, but, but I'm just trying to think through logically how you would actually implement that.

(08:20) **Juliana:** So that, that's an excellent question. So as you, you aptly mentioned before, we are we sit at the fintech, right? So we are a, you can call us a fintech company that, you know, provides a cybersecurity product or a cybersecurity company that provides a fintech product.

We're on both sides of that. So when we have conversations with treasurers, accounts payable, finance people, inevitably we always bring in on their side, they'll bring in their chief information security officer. Because you don't just want to give up all your email access or whatever. However, if you think about it with any company, you already have a number of tools that you've integrated into your email and other parts of your tech stack to provide security and to protect it, right?

So that's not anything new. Um, So when we work with the security team to do that piece with the email handle. across the entire process. You know, we're plugging into already protocols and that they've, you know, that they've already run before like this isn't anything new. And certainly we provide the flexibility that if you say, okay, we only want you to have access to specific email inboxes, then that's great.

You can give us that access or not, you know, however much access you want to give us. So it's not a fully invasive thing, and it's also nothing out of the ordinary. This is something that you, every company has a lot of tools that are doing this already. Not like ours, but for different reasons. But that type of integration is what I mean. That's already quite common. Yeah. Does that answer the question? Oh,

(09:56) **Satwant:** at a high level. Yeah. So definitely, obviously you've got to be fully integrated with the IT team at the organization. I was thinking more of nuts and bolts um, because there's just so many parts there. I'm just trying to understand how the software. You know, certain parts are really easy to detect.

Like if you're in the banking flow, for example.

But I'm just trying to understand from the email, the business email compromise, money lost through that is huge. And I'm just trying to understand how that works actually, more than anything,

(10:27) **Juliana:** so with our system, we can have, I mean, we use it as one central location to be able to look at all that information and be able to aggregate and analyze all of that, right? Like, I'm, I'm not going to speak to the specific APIs or integration pieces, but the understanding being that there is a tech, Obviously a tech stack, and that we layer on top of that and integrating into all those pieces to be able to then connect the dots, as we call it, connecting the dots with data is what we like to call it across all of those systems, because that's the biggest challenge, is that you have systems like, it's not just the email, right, like BEC, you've got email,

you've got ERPs, you've got vendor management databases and other databases and systems, you have the payment Flow, depending on if you have a tool you're already using for parts of that all the way to the end.

Or also bank account validation tools. We also have a way that we do that, that we enable with our tool. So it, we layer on top of all of those. So think about those like they're siloed systems, but then we have a way, the way that we've built our product to be able to integrate on top of that. So that we can aggregate all of that and analyze it together, and then we use the beauty of our AI engine to be able to make sense of that and show those flags, create that baseline, and then show the anomalies and deviations.

I know that doesn't go into too much of the nuts and bolts, because I don't want to speak to the actual,

like, how things plug into each other because that really gets under the hood, but yeah.

(12:00) **Satwant:** Now that, that helps a lot more. Thank you for that.

(12:02) Bank Account Validation: Not Enough Against Fraud

(12:02) **Satwant:** And actually I want to pick on one thing you said, actually, which kind of mirrors one of the blog posts you've got on your site around, you know, why isn't bank account validation enough? Because initial thoughts would be, well, if I'm paying, you know, US steel, 50 grand a month and they change their bank details, And on the bank side, it has to verify that the new account is also US Steel, why, why isn't that validation enough? Because even if somebody else emails somebody in accounts that's fraudulent, for example, surely it would protect them on that side?

(12:40) **Juliana:** Yeah, so there's, there's so many interesting things that we've seen. So one of the cases that is really compelling was we saw a fraudster opened a bank account under the same beneficiary name, all the same details and everything, but just a different at the same bank. But just changed the bank account number and said like, hi, I'm the bank.

Yeah, or rather I'm the company and we're opening another bank account blah blah blah blah blah and Somehow they were able to get through without any questions to open this account And then they did the piece that I described before where they emailed the their client and said hi We've changed our bank account.

Here's the new information and because the company saw oh, well, it's not the same bank It's under the same name So it must be owned by that same company. You know, why would they think differently, right? So that's kind of one way you can get around Like traditional bank account validation because it's it's all the same except the numbers change But because it's at the same bank, it's under the same name.

All of that stuff is the same You wouldn't be the wiser and you'd think well How would they be able to open that type of an account at a bank, right? If they if they weren't the real person and then it turns out that the company the vendor didn't have any idea that that bank Account actually existed because it was owned fully by the fraudster Um, so there's all these nuanced ways that you can go around that and be able to kind of circumvent that callback procedure.

And even the callback procedure, like let's say someone sends you the note, like I described before, Sasha whatever vendor uh, sends you a note and says, Hi, please update our bank account information in your system and whatnot. We have an invoice that needs to be paid. What are you gonna do? Call back Sasha on her number and her signature, which clearly she's hijacked the email already.

Now you're calling Sasha. Like, you might not be calling Nancy, cause she's gone. Or at least you think she's gone. So you're gonna call Sasha, but that's the fraudster anyway, so they're gonna answer the phone. You know, so there's a lot of things about this callback procedure. And I've gone through this before, I'll be honest, where I got so nervous.

This is a past job. about um, potential fraud, and luckily it wasn't, but I went and called like three different people at the company to be really sure because I, I was a little bit suspicious that something was going on, and luckily it was fine in the end, but not a lot of people are going to go and try and call three different people they were in touch with at a vendor.

So yeah, if that answers your question, it's just, it's not so much that it's, it's not gonna work every time. Like, bank account validation is really good, I would say, most of the time. It's that fraudsters are really sneaky and there are these corners that they can take advantage of to then be able to create that bank account that can get around the traditional bank account validation.

Yeah.

(15:26) **Satwant:** Yeah.

(15:27) Tackling Duplicate Payments and Financial Errors

(15:27) **Satwant:** Another thing I wanted to touch on is how your software helps with simply... errors. So. Duplicate payments, overpayments, late or lost or wrong payments. And again, I would say, how's a company's existing procedures not going to pick up on that stuff regularly? And how does your software help?

(15:51) **Juliana:** That's a great question. The best example I'll give is always with duplicate payments because those are the most really the trickiest ones and they're the most common. So they, that stat you gave of like one to 3 percent losses from errors on budgets that most of that is actually due to duplicate payments.

And so here's what typically happens is submits payment. It gets uploaded into an ERP or the information is entered into whatever database. Then a little time goes by and maybe there's a stall in it getting paid, the vendor sends the invoice again. And it's completely accidental. They just assume, oh, maybe it didn't get paid yet, let's resend it.

And then another person uploads it to the ERP, and then suddenly you've got two invoices in the flow, you see where I'm going with this. And now both of them end up getting paid, right? And then that adds, that causes a number of problems. Um, Mainly because when you're reconciling this later, now you've got an overpayment there, right?

Now you've paid that vendor twice, like, do you take a refund from the vendor? Do you use it as a credit for the next month that they provide a service? You know, how, how are you going to be recording Right. And so then that that causes all sorts of challenges, but then maybe you don't catch it and it only gets caught at a recovery audit later.

Um, So there's all sorts of things that ends up happening like that. So duplicate payments are really the biggest one. Gosh, I'm trying to remember what the stat was, but it was really something shocking where it was uh, very high percentage of invoices are duplicates. Not that they're paid out, but that are received.

And so the way that our system catches duplicates is that we can read all of the information on an invoice, both what you see and what's underneath. And so then we can see if you upload you know, two of the same ERP within, let's say, a week apart or whatever, and they're put into a payment flow. Our system's gonna flag, like, first of all, hey, that's interesting.

You usually don't pay this vendor more than once a month. Now you've got two invoices within the course of a week. Okay, let's flag that. Like, let's just make a note of that. Maybe it's just an extra service they provided. No big deal. Maybe it's a problem. Then we'll look at the amount. Huh? The amount's the exact same.

It's within one week of each other. That's interesting. Then it'll look at the payment information and the number on the invoice. Okay. The date is the same. The number is the same. All of this other information. This is clearly a duplicate invoice that was already submitted a week ago, but then someone uploaded it twice.

Okay. So then we flag it for review and we say, okay, it looks like you have two. of the same invoice that are in for payment. Do you really want to pay these? And we'll, we'll stop it there so that then it's stopped for review and that, you know, the person in the payment approval process can take a look and see, okay, yes, these are actually the same invoice or, you know, this is, this is two separate invoices that somehow, you know, got marked incorrectly. So that's how detect that.

(18:56) **Satwant:** high level about your solution, because I would love to talk to you for hours if I could. You've got some great stories, I'd imagine.

(19:02) Overview of Trustmi's Comprehensive Solution Modules

(19:02) **Satwant:** So I'll just go through the sort of five modules. So for anyone's listening, so payment approval workflow, which I started mentioning earlier.

SOX compliance, so complying with regulations and avoiding violations. Then three and four kind of linked together. You've got vendor onboarding and vendor lifecycle management. So that's very important when you stop dealing with somebody all together, I guess.

(19:24) **Juliana:** Anyway.

(19:25) **Satwant:** And then lastly, you've got a, like a claims fraud engine, which helps your insurance customers or insurance companies that are your customers.

So that does that cover everything? Have I missed anything there?

(19:36) **Juliana:** Yeah, so those are the primary modules for sure. But like I mentioned with a bank account validation, we consider that as part of like the vendor onboarding and vendor management. When you're onboarding a vendor, you want to verify their bank account information. So that feature is included in there. Um, So we certainly do that as well.

So it's, you know, each of these I would say are buckets, which with a lot more. All right. Inside them, outside of that. But yes, that covers them, the main the primary modules. In addition to the, obviously the core product of payment security, which is the baseline, the fingerprint, the detecting the deviations and anomalies in the process, that's really our core product.

Mm

(20:19) **Satwant:** So when one of your customers has your software, do they a dashboard and I suppose different employees will be able to see different things in those dashboards. Is that kind of how it works on the user end?

(20:34) **Juliana:** Yes, so we do have a dashboard and you can see you know, you can see all of your and manage all of your invoices and payments in there and your payment cycles. It's full flexibility, so the people that you want to have whatever access to it or not and what they can see and visibility it's, you know, can all be configured and customized within the platform and the dashboard.

(20:56) **Satwant:** Great stuff.

(20:57) Addressing Supply Chain Attacks and Insider Collusion

(20:57) **Satwant:** So now the challenging bit, I want you to talk about one popular or getting more popular amongst criminals is the supply chain attack. And in case anybody listening doesn't know what that is it's where a criminal would attack another company that's supplying the target organization and actually trying to get into your company that way through the back, sort of through some kind of back channel.

And also how, how, so first of all, you know, how does your software work in those scenarios? And also kind of similar would be the insider collusion

(21:30) **Juliana:** Mm.

(21:31) Unveiling Email Compromise Tactics

(21:31) **Satwant:** You know, employees are the ones that know all the loopholes inside a company. Not necessarily all of them, but a lot of them. And again, how would your software detect that?

Yeah.

(21:41) **Juliana:** So, really, so the, the business email compromise example I gave before is, is great for that. Cause that's really one of the most common you see, is that they attack the email of a smaller agency that works with a large company, to then gain access to the systems of that company, or at least to the email conversation.

Watch the email conversation and intercept where they can, and cut out the people. That are real. And, and then, you know, the Sasha and Nancy example I gave. So that's, that's a really great example of that. And we catch that because we monitor the. Conversation you know, if they actually compromise the actual email of the employee, like a typical BEC then we can see if there's a change in tone, and suddenly there's the urgency of needing to pay the second invoice, or no, the invoice was wrong, that's actually twice the amount, and you need to upload it now and pay it tomorrow, and, and all of that, and so we can see all of those things.

(22:36) Detecting Supply Chain Fraud

(22:36) **Juliana:** You know that type of tone in the communication that suddenly shifted we can see those again deviations So that's a great way to see the supply chain is typically in the communication piece and in the invoices that they're sending So are the invoices the same? Do they look like past invoices that they've sent?

Right? Um, and And so we really look at that very closely, or our system, it, it analyzes all of those indicators and it looks at that closely. So that would be on the, the supply chain, just a couple of examples there. There's, there's certainly a lot more nuance we could go into.

(23:08) The Insidious Insider: Internal Collusion Exposed

(23:08) **Juliana:** On the internal collusion side, this gets really interesting, because it is, it is, I call it the insidious insider.

I think there's a blog post on our site to that effect. Because they are very sneaky and they are very smart, because as you mentioned, They know the systems, they know how it works, they know the process, they know that Bob is not seeing what John did and approving this without that and like, you know, they know who has access to what system.

And so, so there's a number of ways we can do that. So in this case, we can see, but because we layer into and integrate into all these different systems within the B2B payment process, we're able to see who is Who uploaded that invoice into the ERP or entered in the information? And oh look, this person over here, they came in later and they changed the banking details.

And then they changed them back after the payment went through. Like, we can see those nuances. So someone came in and did exactly what I described. Someone You know, person A uploads an invoice, then person B, the insidious insider, they come and they make a change, wait for the payment cycle to run, they come back, change it back.

And, you know, there you go. Yeah, we can, we can see that those changes happen. Then it's like, wait a minute, what just happened here? You know, they shouldn't, they're doing something they shouldn't be doing. We can also enforce controls within these different systems to be able to say like, does this person really need this much access in the system?

Should they be able to even make any changes to banking information for vendors? Probably not, you know, depending on their

level, right? And enforcing segregation of duty so you don't have one person doing, you know, everything and, and not, you know, just being able to go rogue and uh, do that off the radar.

So those are, hopefully those examples give you a little bit of a sense on, on some of the indicators that we can kind of be able to respond

to.

(25:03) **Satwant:** Yeah,

definitely.

(25:05) Audit Logs and Separation of Duties

(25:05) **Satwant:** You're basically looking at audit logs, I suppose, of some kind where you can track all of that. Yeah. Yeah. Yeah.

(25:11) Real-World Fraud Stories and Lessons

(25:11) **Satwant:** It reminds me, when you said separation of duties, it reminds me of that case. There was a lady in the States, she worked at a council somewhere and for decades, she was, she was the treasurer.

She was approving the transactions and submitting them as well or something. And basically that, That county or that town, you know, for years and years couldn't have new swimming pools or this or that for the

(25:33) **Juliana:** Oh man, yeah.

(25:34) **Satwant:** she, and only because somebody, when she was on holiday questioned it, they exposed it all, you

(25:40) **Juliana:** Yeah, we've, it's, one of the worries I saw recently is just one of those face palm moments is when you had the head of, I think it was head of internal compliance as well as like finance. You know, stealing money internally and you're just thinking, gosh, it's also the same person who's supposed to make sure this certain thing doesn't happen is the one that's also taking advantage and knows how the system works to be able to manipulate it.

So it's really, they come in all flavors. Yeah, for internal collusion.

(26:11) **Satwant:** Yeah. Yeah. You must, you must say some crazy stuff at your company. We've talked about quite a lot here in a short space of time. Is there anything that you wanted to get across? You know, for companies who really ultimately just want to sell more, convert more of their customers or reduce their costs,

(26:28) Comprehensive Solutions for Complex Problems

(26:28) **Juliana:** No, I mean, we, we touched on a lot. I really appreciate um, really kind of being able to have a conversation, looking holistically at everything is really great because one of the things we do, we Or not that I worry about or that I've seen is that often people think like, oh, we just need a point solution for bank account validation or for vendor onboarding or vendor management.

And it's like, actually, you have to think about all of it together because you can't just, because again, if you keep siloing the processes, that's feeding into the problem. So so just getting that, that point across is really great. Yeah, otherwise I mean, it's been, yeah, I've enjoyed talking about kind of all the different corners of our product that we've done, so, that we've been building.

(27:13) **Satwant:** Great. It'd be good if you could talk about some case studies.

(27:17) Case Study: Colgate Palmolive's Security Success

(27:17) **Juliana:** Two of our biggest clients that we talk about a lot are Colgate Palmolive, CNA Insurance. Certainly Colgate um, I spend a lot of time talking to them over there. We've had a long relationship with them, and they're really, really big supporter of ours and really, really smart people and very strong security team and financial processes.

And so that case study, you know, we, we uh, We started talking to them a while ago and what was really interesting was we were able to run a POC with them. So proof of concept, which is what we do with everyone that we talk to. So, you know, every company, if they We wanna be able to show and deliver value immediately.

And so we like to do a POC early on just to show them, like, let's see if we can detect any errors or issues in the past, and we can at least show you the whole story and we can show the story. Um, So we had a really great moment with Colgate where we were able to sit with the team and kind of really go through and show them the product and they could see the value immediately because, they are a really good example of a company that can benefit from our type of product, which is hundreds of thousands of vendors, thousands upon thousands of invoices, thousands upon thousands of payment cycles, but they do not have a hundred thousand people in their accounts payable department. Right.

That would be impossible. So so they could immediately see the value of saying like, you know what, we need to have a way to provide some automation and reduce the manual effort, but then also provide this detection like AI driven detection, but with zero false positives. And so that was something that really, I, I had a great conversation with their head of security there where he said he was very impressed was the fact that, you know, when we flag something, we flag something that's real.

We're not just flagging something that you check and you're like, ah, no, it's just nothing, you know, whatever. And that's really important because especially IT people, security people, but finance people as well, no one wants to waste their time looking into something that isn't real. So that's been, that was something very exciting for them.

It was like, oh, this is great. It's not going to add more time into review and all of that. It's actually going to just catch the things we need to look at. So, so yeah, so that's been a really exciting partnership and it's also been with them that they've really helped us to think uh, more strategically about how we extend the logic of our product to also address errors.

We were doing that kind of as a side thing, like, oh yeah, we deal with fraud and, and errors, you know, errors because that's easy to catch. But then they were like, they were the ones that told us, like, this is a really interesting, compelling area that you need to kind of examine more closely because that's really where.

That's where the other half of the value comes from, it's not just fraud. So that's been a big part of that case study. It has also been developing that area with them. And growing that area.

(30:05) **Satwant:** Yeah. I mean, I'd imagine with those guys, I mean, they're dealing with millions of physical items a year, shipping them all over the world. I mean,

(30:14) **Juliana:** It's a complex, it's a very complex business. And you're dealing with a lot of vendors and suppliers all over the world. I mean, that's, you know, there's high complexity there, so.

(30:24) **Satwant:** yeah,

(30:24) **Juliana:** Yeah.

(30:25) **Satwant:** Excellent.

(30:26) Getting Started: Proof of Concept and Deployment

(30:26) **Satwant:** You partly answered my next question in terms of if a customer wants to get started with you guys, how's the best way? So you, you mentioned proof of concept which is great. And, and how long would it take to deploy a solution typically with your clients, because they might do it stage by stage, I suppose, rather than go

(30:44) **Juliana:** Yeah, so, you know, before we talked about how the solution is modular so they don't have to deploy every single module. Of course, there is the core module payment security and typically all of our customers will, you they'll deploy more than one module because they'll, they'll understand the kind of end to end approach.

And so they won't just have the payment security, they'll want also payment flows, or maybe the vendor onboarding and maybe the, the management as well, vendor management, lifecycle management. So with that, like it, it's, it's whatever they want, right? We try and make it customizable and very flexible for them.

For our POC. We are very proud of the fact that we can get up and running very quickly, and so we can actually start calibrating it within a week. to start gathering data and start showing the historical data. So we get access to whatever, you know, you don't want to give us access to your, your live systems.

That's fine. Just give us a data dump in the past, the past year, past two years. We'll use that to calibrate our system to then start building that baseline for the vendors. And then we can look to see if there was an incident or where there were suspicious signals that would have indicated an incident would happen or whatever.

And then within the second week, we can already provide an analysis. So we've been able to do that for clients and it's been great because in some cases we've um, I can't name the client, but uh, where we showed them in the second week, an incident that was a fairly, large amount of money on a, an attempted fraud.

And the security team over there didn't believe us. They said like, not that they didn't believe it didn't happen. They couldn't believe that we pulled together the entire timeline. Something that took them three months as a team to pull together and be able to dissect when it happened. We were able to show it after looking at their data for one week.

Which was really great. Yeah. And so that was very cool where, you know, you have a head of security saying like, Yeah, no, we don't believe, like, this isn't possible. You must've broken into some, some computer and gotten our PowerPoint presentation to the CIO, cause this is, this is absolutely spot on all the dates and everything where everything happened, the BEC, when the person hacked the email of the vendor, when the invoice was sent, when this went through this payment cycle, like the whole thing, so yeah, so it's really great to see that we can pull that quickly, you know, and, and,

(33:09) **Satwant:** So what I'd be right in saying, there's nothing really comparable to you guys in the marketplace, because you did mention point solutions before. It's kind of the only alternative.

(33:17) **Juliana:** So you can arguably, there's others out there that are going to say they do the same thing or that they do similar things. The way I look at it in terms of our product is, We really take a full end to end approach, you know, we use that word a lot, but in terms of thinking about all the pieces and not just focusing on one or two.

So yes, there are some solutions out there that might do more than just a point solution, like bank account validation and one or two other things, or they're focused on vendor management, vendor onboarding in that piece. But in terms of really having that full view Uh, that we do, there really isn't, we don't consider there to be competition out there also because we provide such flexibility where we don't force you to change your process, so we call it your process, your way, you decide how you want to do it, you decide how you want to configure it, fully customizable.

So that level of flexibility is, is unique to the market.

(34:11) **Satwant:** And how do you charge customers? Is it typically sort of per, per user sort of seat or annual

pricing? Just at a very

(34:19) **Juliana:** Yeah, no, I appreciate that. At a very high level, we're looking at volume of invoices and payments and that area. Cause you know, you could have a hundred people that are approving things or five, but you have the same number, you know, you have Two million invoices you're paying a year or a hundred thousand invoices you're paying a year.

But the, you know, so you don't want to focus on seats, right? It's really more about the volume of payments and transactions that we are protecting.

(34:49) **Satwant:** excellent. So if people want to get started with you folks your website is trustmi.Ai. So that's trustmi.Ai.

(34:58) **Juliana:** that's right.

(35:00) **Satwant:** And I'd love to ask you, what are your company's goals slash predictions in the next six to 12 Oh, wow. Yeah.

(35:08) Facing the Future: AI and Cybersecurity Trends

(35:08) **Juliana:** So it is a really exciting time in terms of what's happening with the generative AI, right? And so we've seen, actually you'll like this, you'll like some, some sexy stories. A recent one where a company in Hong Kong, a guy in the accounting team was duped by a deep fake of the CFO. A deep fake video of the CFO.

At his company, and he ended up wiring 25 million to a fraudster who had leveraged a deepfake video. And of him, not just the CFO, but other executives. So that was a, a really big story in, in February. So, this is real, and generative AI is, is accelerating the development of it, the evolution of it.

It's getting smarter, it's getting better, and it's getting easier to use at scale. So, that means all of us uh, To say that the need for this type of product that we have and for really thinking intentionally about securing your business payments and being strategic about that is an even bigger imperative.

And so we're seeing that in the market, that there's a big interest in that from treasury teams, accounts, payable teams, finance teams there've been a couple of things that are also raising a lot of awareness about this type of solution is uh, or in general kind of AI tech. To fight bad ai, if you will.

So we had a ruling last summer from the SEC where all public companies now have a very specific way that they have to report cyber attacks and cyber incidents that happen, right? And so any sort of cyber attack that impacts your payments, obviously that would be included in that umbrella. And so. As someone in the finance team or the head of finance of one of these large companies, do you really want to have to tell your shareholders that something happened?

No. So let's be proactive and find a system that can help avoid this so we can protect that process so we don't have to worry about any cyber attacks on it, right? Also the CPA exam. is getting much more focused on technologies for finance people. And so that's another strong indicator showing that they actually changed the exam as of this year.

To focus more on kind of like technologies as a baseline that finance teams need to use. So what we're seeing in the next you know, 12, 24 months or 6 to 18 months, however you want to look at it. We're really seeing this evolution in the finance team of becoming more technologically and security focused and fluent.

Um, Where you're really going to see more of this imperative of, oh, I get it. This is why it's so important to leverage technologies, especially AI, to protect. This very vulnerable process of paying other companies, you know, paying vendors. Um, So we're really starting to see that interest accelerate. Even within the past six to eight months, people coming to us saying like, you know, we've had an incident.

Uh, We're seeing this happen more frequently. We just had an employee that had to deal with maybe not a deep fake to the level of what I described previously. But, you know, we're starting to see some really sophisticated ways that these fraudsters are trying to get people to pay them. Pay the wrong person.

So yeah, so we're definitely seeing that, that interest, but also the, the knowledge and understanding of why it's important is increasing in the market. So that's a really good sign.

(38:22) **Satwant:** Yeah, even at a personal level, I mean, if you grew up in an English speaking country like we did, the classic check is grammar and punctuation and things to detect, dodgy characters emailing you, but with ChatGPT, that, that goes

(38:36) **Juliana:** Right. But at the same time, not everyone, even a real person doesn't have perfect grammar. So, You never know, you know, how would you be able to know if that person, you know, suddenly, if they start sending an email that's in perfect grammar using all the proper syntax and everything, wouldn't that kind of raise an eyebrow too?

Because then that could be the, exactly. So there, it goes both ways. So it's very tricky.

(39:02) **Satwant:** Yeah. I did read a funny story the other day that some fraudsters that they're putting, they're copying the prompt into the scam emails so that you can actually see them. Right. They've written, Oh, please create a letter that says this. And then they, they put that in with the scam letter as

(39:20) **Juliana:** oh, yeah, that, you know, that's just working too quickly. That's sloppy work.

Exactly.

(39:29) **Satwant:** Great stuff. Is there a chance that customers can potentially meet you? You doing any conferences or

(39:34) **Juliana:** Oh, yeah. So we, we do attend a lot of different types of conferences. We will be at Courts Connect at the end of this week, early next week in Vegas. So that's a great event with really senior finance leaders who are looking for technologies that can address some They're biggest challenges. And so there's a lot of interest in B2B payments and automation, cybersecurity.

And so, so yeah, so we're participating there to talk to a lot of those folks. Um, Also there's accounts payable, procure to pay, APP2P in May from the 19th to the 21st, that's organized by IOFM and they and we'll be exhibiting there and that'll be down in Florida. So we're looking forward to meeting a lot of accounts payable people there.

(40:19) **Satwant:** There really is a conference for everything in the States. I'd never thought there'd be an accounts

(40:22) **Juliana:** know, I know, and it's, it's a, it's a really interesting conference. I mean, it's also procured to pay, but you know, it's a very niche area, which is why we're, we're excited to be speaking about AI actually for exactly this. Cause that's something we really want to talk a lot about with accounts, payable people and finance people as AI, and there's a hunger for it.

They're very interested in it.

(40:44) **Satwant:** Great stuff. Well, thanks so much. I've absolutely hammered you on this show, so I really appreciate you. Firing back the answers as you have. So I'm going to finish with something lighter.

(40:53) Closing Thoughts and Chit Chat

(40:53) **Satwant:** It would be great to hear from you, you know, some great advice you've received in your career perhaps. Or just what you're reading or watching or listening to right now.

(41:03) **Juliana:** is this related to work or related to

anything? Okay, well, well, good advice. I received, it's funny, I received it both from my sister, but then also from one of my favorite, favorite bosses in the past. Who both said to me in different ways, you know, when you're thinking about relationships, friendships, friends.

Work obviously with employees and, and managers and whatnot, or family you know, relationships are 50 50. So it's not just a two way street. We always hear that, but it's 50 50. There's only so much you can do. So if you're trying to go 80 percent and it's not working, you know, it's not always on you.

Or if you're just doing 20%, obviously it's gonna fail. So and that made me think a lot about how I, sort of the behavioral dynamics between me and, and the people around me in my life. And sort of how I build my relationships. It's like, I always think, 50 50. Are they meeting me halfway? Am I meeting them halfway?

You know, and so that was always that's been something that's stuck with me throughout my career actually as well. As for my, what I do on the side or my side hustle, I'm actually a professional violinist on the side. So I'm Moonlight playing a concert. Yes. A classical violinist. It's sort of my Zen thing that I do when I'm not thinking about payments and fraud.

So, yeah.

(42:23) **Satwant:** Amazing. Well, it's a great instrument. Awesome. Well, thank you so much, Julian. I really appreciate your time and yeah, all the best

to you in the future and to your company.

(42:33) **Juliana:** Well, thank you so much. I really appreciate it. It was great speaking with you and meeting you. Thanks for having me on today.

(42:39) **Satwant:** Cheers. Take it

(42:40) **Juliana:** Okay, take care.

Bye.