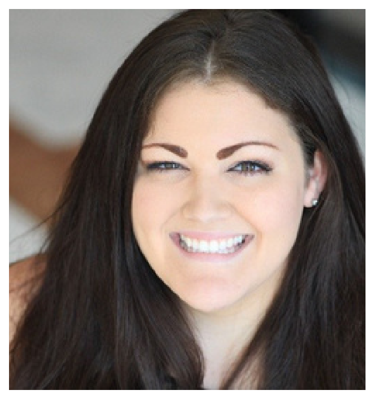
THE PAYMENTS SHOW

http://thepayments.show

E83:
IDOLOGY: HOW TO VERIFY YOUR ECOMMERCE CUSTOMERS WITHOUT COMPROMISING SECURITY OR CONVENIENCE



GUEST

Heidi Hunter

Chief Product Officer

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

[00:01:02] IDology Overview: Identity Verification and Fraud Management

[00:01:02] **Satwant:** it'd be great to hear from you and another part of the GBG organization in terms of what you're doing in payments. So welcome

[00:01:09] **Heidi:** Yeah. Thank you so much.

[00:01:11] **Satwant:** and where are you joining from today?

[00:01:13] **Heidi:** So I am in GBG's Atlanta headquarters. So I'm from Atlanta, Georgia, Stateside, US, Eastern Seaboard.

[00:01:22] **Satwant:** so it's an interesting setup with the organization. So you're pretty global, which is nice to see.

[00:01:26] **Heidi:** We are, it's a really interesting organization. The company's headquartered uh, London, we're traded publicly on the stock exchange. The company's made some really great acquisitions over the years. My colleague, Justin, comes through Locate, which was a location service, very, very adjacent to the work that we do in identity.

[00:01:43] I've Came from a software acquisition of a company called Ideology, who provides identity verification services in over 35 different verticals, very similar to GBG's UK business. So we're very comparable in the types of offerings that we provide and collectively we provide the ability to verify any individual globally in the world through some method of verification.

[00:02:05] **Satwant:** Okay, great. Well, actually kind of nicely introduces to what you guys do. And I liked your tagline, which is nice and simple on your, LinkedIn profile company page, actually. It said ideology provides solutions to drive revenue by removing friction and fighting fraud.

[00:02:20] So I liked that it was very simple and straight to the point. And like you said, through a combination of solutions such as. Identity verification, fraud management, et cetera.

[00:02:29] Statistics on Business Fraud and Data Breaches

[00:02:29] **Satwant:** So I just want to set the scene and talk about some, some crazy stats that I read, which were provided by your organization, and then we can talk around how those can be addressed with your solution.

[00:02:41] So one interesting stat was 55% of businesses have suffered fraud attacks in the past year, [00:02:47] and

[00:02:47] **Heidi:**

[00:02:47] Mm hmm.

[00:02:48] **Satwant:** That was from the Global State of Digital Identity Report. And then there's another stat that says 83% of businesses are seeing multiple data breaches over the same period of time.

[00:03:00] And that was from your own organization's report. And we've all been subject to data breaches. I think I get so many emails from my password manager saying, oh, this has been involved in a breach. That's on the dark web. This is out there. So yeah, it'd be great to sort of understand

[00:03:15] **Heidi:** how

[00:03:17] **Satwant:** your solution attempts to address these problems because you're the chief product officer ideology. So I guess you can see the whole suite of everything you offer and explain where they fit in.

[00:03:30] **Heidi:** Yeah, that's exactly right.

[00:03:32] Exploring the Sophistication of Fraud Attacks

[00:03:32] **Heidi:** So they are some troubling stats, and if I'm honest, I think they are a little bit, I think they're likely worse than that, because I think oftentimes, you know, in a large organization, you find these things out after the fact, right? A lot of times data has a sense of curing, right, almost like a salted meat, where it's, you find out later. And the, the attacks now are so sophisticated. These guys have gone from, you know, there's, there's different types of plays. There's, there's fraud plays that are you know, heavily digitized bot level activity. They just spam. A system, whether it's, you know, they're going to have different types of gains.

[00:04:09] They're trying to find a weak, vulnerable point to pull data out. Whether it's spamming an organization cause there's some type of incentive, like a a kickback, you know, in the gaming market, you know, you might hear like you get a player bonus for making a bet over a certain level retail. I mean, these guys will do anything.

[00:04:26] So there's brute force types of attacks. But I think the most shocking thing for me over the last four to five years has been this immersion of the long, The Long Strategy, where these guys are actually willing to create culture and cure identities over a period of time and build a worthiness level of them financially, and then they'll utilize that and just and just bastardize it across different financial services providers for the gains that they want to make.

[00:04:51] The Role of Technology in Fraud Prevention

[00:04:51] **Heidi:** So from our perspective, right, Everything, if you're gonna drive a low friction experience, the best thing to do is with relative to that is to really try to leverage technology to your benefit the best way that you can. And I think we're in a very interesting time in the world where things are so heavily digitized.

[00:05:11] Everything is Amazon, like checkouts, right? We want, you want to, you want things quickly. There's a lot of information.

[00:05:17] Impact of COVID-19 on Digitization and Fraud

[00:05:17] **Heidi:** The Internet's made it so that if you're looking for a particular type of financial product, there's a thousand options, right? And digitization, I think it had begun prior to COVID, but COVID just absolutely rapidized all of that, right? Because the types of interactions you could have in person were greatly limited to almost non existent. So, people that were holdouts on tech, Adopting tech as a consumer suddenly had to take the digital path and now that they're able to actually use these, these solutions, they've become accustomed to that.

[00:05:52] So from their perspective, right, I feel like Sat there, it's a crowded market. There's a lot of options. It's easy to get information. And so consumers are looking for a really great experience, right? With technology can bring you those types of things. And on the fraudster side, there's more opportunities than ever because there's just an abundance of these things out there.

[00:06:15] The Importance of Data Collection in Fraud Prevention

[00:06:15] **Heidi:** So from our perspective, our solutions are heavily baked into technology and the utilization of, of, great tech that's available, but also data and information. So in order to go a low friction path, you want to collect the right amount of data. And I tell people that a lot. We need, we need to collect the right information.

[00:06:35] We shouldn't collect data we don't need. But our solutions are built around taking different information about an identity. So you've got the core pieces, which is always name, address, date of birth. Here in the States, you've got this, you know, SSN in Canada, that might be the SIN, you know in Mexico, it's the CURP, but taking those attributes and verifying them for the purposes of meeting some level of compliance, right?

[00:06:59] Challenges in Asserting Ownership of Data

[00:06:59] **Heidi:** So our tech can deliver that, but that's not sufficient in this world in order to assert Ownership of that identity, ownership of the device that it's on. These, you're going to need to look at that for many different aspects, right? You need to make sure that you're meeting compliance by verifying this person is legitimate, exists, they're not synthetic, but you also need to be able to assert some type of ownership of that data, which is very challenging to do in a non present environment.

[00:07:26] So looking at things like the email that they registered with, the mobile number, do they have some kind of ownership of that? Looking even at things like their IP address, right, to try to get a sense of where the traffic's coming from, information about the device. Our solution will factor out To those different data points and pull back as much data as it can, it generates information that then can be run through decision matrices to come with the next step type of outcome.

[00:07:53] So, can they be on boarded cleanly? Do they need to do some type of deeper authentication? Whether that be here in the States. We've got a concept of knowledge based authentication. There's some places where that's applicable. Doc verification can also be part of this process, right? So scanning of a photo ID, but by leveraging that tech, you're able to really get into the detail of the data you've been given, the data you've been able to collect by, you know, the mobile device and what's going on around it.

[00:08:21] And you can get a really good sense that, yes, this really is Heidi. In Atlanta, on a mobile number that she's owned for 12 years, she's, she's safe to transact, right? Versus, yes, this is Heidi's data and it's clean, but it's coming from maybe California. Heidi's never been in California. She's on a mobile number that's a voice over IP, right?

[00:08:39] So when you start pulling all these different informational points together, you can get a really clear picture of who is You know, who you're actually transacting with and what's great about leveraging tech in this manner from our perspective is that when you do this, you don't need to take some of the antiquated paths we've got here in the U.

[00:08:58] The Importance of a Smooth Onboarding Process

[00:08:58] **Heidi:** S. to start onboarding. Right? You can offer that great, easy check in experience because from the consumer's perspective, they've entered six pieces of data, right? And potentially onboarded with that. So that's the approach that we take when we're building software and we're just always exploring, Trying to get ahead of whatever fraudulent activity is accompanying these various data points that we're attempting to verify for our customers.

[00:09:23] **Satwant:** You made me smile when you said all the various pieces of data to make onboarding better, because. We've all been there where you feel like a criminal, [00:09:32] **Heidi:** It's 15 minutes, right? Submit, send, submit, send, right?

[00:09:37] **Satwant:** I can't tell you how many thousands of dollars I've not spent because I just thought, I just can't be bothered with this, especially on a mobile device.

[00:09:44] **Heidi:** Yeah, absolutely. You're looking for something that's quick and expedient, right? And if you think about, you know, traditional banking, it was such a stepped process and it didn't matter if you were You know, if you, if you provided valid data and there was no risk, you were still going to run through that full onboarding process, but if compliance doesn't dictate, you need to do those things, right?

[00:10:06] You should be looking for opportunities to offer that sleeker experience, because again, in this crowded market where there's a lot of fraud, the tried and true methods we've been using to onboard Consumers over the last 15 to 20 years, they're not secure enough for one because they don't go into the right kind of detail to prevent the fraud that's happening.

[00:10:25] But in a crowded market where you've got, you know, there's things like neo banking and the non traditional banking that offers all these different kinds of incentives. If you're gonna, you know, stay relevant in the market, you want to leverage tech to your advantage, right? Because then what you can do Sat, you're not only bolstering your ability to prevent fraud, you're also Competing in a crowded space where again that digitized experience has got to be for lack of a better word sexy right in order to Attract that consumer but then keep them as a customer

[00:10:58] **Satwant:** Yeah, agreed. And the other thing is in different age brackets as well. So older people really struggle with a lot of tech verification that I've seen. YoU know, younger people obviously are much more adept at it and faster. So there's a big variable there because I did see in the research from your company

[00:11:18] Synthetic Identity Fraud

[00:11:18] **Satwant:** Often the people who suffer the most from things like synthetic identity fraud, for example, and if anyone listening doesn't know what that is, is where you make up a person from different pieces of, different pieces of information from different people. And so, your research showed that vulnerable people are more, susceptible to this, including the young, the elderly and deceased people as well. So there's just so many variables I could talk about in this episode. We could probably talk for three hours,

[00:11:48] **Heidi:** Yeah,

[00:11:48] **Satwant:** big one.

[00:11:49] **Heidi:** it is and it's, it's a big challenge. I think the thing that I have found very striking about it is there's, You know, as an organization, and I, I've, I'm a customer of some large banks and also a credit union that's local, right, for different reasons. I see them attempting to educate consumers about what to do and not to do, right?

[00:12:10] You've got people like Brian Krebs. Locally for me, there's a really great guy Clark Howard. Who I subscribe to and I've subscribed my grandmother to because she's 95 or Facebook gets hacked every other week. Bless her heart, right? And they are we are we I think everybody is trying to help educate but that you're not gonna solve that problem As a business, right? The best thing that you can do is build the appropriate levers to Protect yourself from being taken in by those types of scams.

[00:12:40] Data Depth vs Richness

[00:12:40] **Heidi:** But the synthetic problem is very pervasive because while it is a longer strategy, Sat, you, in order to do that, you have to be willing to take the time to build that profile to a level of richness, which oddly enough, what we will see is people do things like actually open different kinds of accounts, credit accounts on them, low limit, instant access, and then they'll sit there and actually use them and pay the bills for a while to grow. And as the credit gets better and better, then it's ripe to be used for taking advantage of businesses, right? And there's just, it's going to be challenging, I think, for any organization to thwart consumers from allowing that to happen, right? Because they're doing that data collection by spamming kids, by spamming grown adults through SMS.

[00:13:26] They're doing it by sending, you know, emails that are invalid. I mean, and I, myself in particular, I find myself to be, front edge of tech. I'm very transparent with my kids about what's appropriate and what is not. I felt like we were very secure, but even in my own home, my, my kids mistakenly went to a website and we're putting in information about our property. Now, thankfully I saw it before, but I was, what are you doing? We talk about this all the time, right? So it can happen. It just, it's gonna keep happening, right?

[00:13:57] So what you want to do is have tech capabilities in place that can filter that type of activity out, right? Because to your point, there's, while there will be some richness to these type of identities, there's not going to be depth, right? There won't be depth to them. There's going to be things about them that make them inaccurate and correct. You know, problems with the mobile number, potentially problems with the email. Things are not going to match up when they're used.

[00:14:23] And the other way that, you know, we know you can thwart them is through adoption. You can escalate them to things like a digital ID verification, because then if they have to scan a physical ID, that's going to be challenging for them to, you know, accomplish that quickly. So that's another great barrier to kind of weeding that type of activity out. But you have to do it carefully, right?

[00:14:42] Because you don't want to be screening out good consumers who. are, are underage, right? Or I would say underage, under my age that are like in their, you know, their 20s and maybe you're just moving out for the first time or new to country. So it's a very scalpeled approach to evaluating data to find those problems that needs to be done. But there is great tech on the market, ours and other, other things that can help you get there.

[00:15:04] Differentiating Factors of Ideology's Solutions

[00:15:04] **Satwant:** Yeah. Actually, that's what I wanted to drill down on next, because if we look at the solutions, the main solutions from ideology, identity verification, anti money laundering, know your customer, and fraud management, now on the face of it. Other people that compete with you guys will say, well, we offer that as well.

[00:15:24] **Heidi:** I picked

[00:15:25] **Satwant:** And

[00:15:25] **Heidi:** me, but

[00:15:26] **Satwant:** your solutions that you offer are very comprehensive. And I just wanted to talk about some of those in detail to differentiate you guys. And I picked a few that attracted me, but feel free to, to, to mention some of your favorite sort of differentiation points as well. So for me, with the transaction monitoring, for example,

[00:15:45] **Heidi:** monitoring, for

[00:15:46] **Satwant:** Giving.

[00:15:46] Intuitive visualizations and alerts to people who are sitting at those retailers or payment companies, for example. And in the fraud management, you've got your eDNA, digital identity engine and real time velocity alerts. So all this stuff sounds really cool, but I'd love for you to maybe talk about some of those key differentiation points where you could address a customer, future customer, perhaps on, well, I've seen all this from somebody else.

[00:16:14] **Heidi:** Yeah, absolutely. I think something that I fall back on, and it's funny, a lot of times I think our, our competitors like to use this against us saying that we're, well, we've, they've been around for years.

[00:16:27] They're not, you know, they're dinosaur, they don't use, but. What comes from that, though, the knowledge that's built into this product, these products, all of them, because all of them have tenure. Everything that I work with here in the U. S. region, there's, it's over 20 years of technology and experience, right?

[00:16:46] And the maturation of those products have evolved as the data has evolved, right? I actually joined the organization at a time where, if you can believe it, Sat, we used to analyze customer rates to figure out how to approve as many people as possible. So if people were not being approved, my job as a customer agent was to figure out how, make settings changes, and drive as many people through the funnel as possible.

[00:17:08] So I went from that time to where fraud became, digital fraud suddenly came into the mix and customers are trying to figure out how to wrap their hands around it to this time now where it's table stakes. If you're, if you're working in this, in this space and you don't have layers for fraud prevention, you're not going to.

[00:17:27] It's going to be difficult for any customer to find value in what you're offering, right? And our solutions have, all of them have lived through that experience, right?

[00:17:35] eDNA: Data Collection Across Industries & Markets

[00:17:35] **Heidi:** And specifically our eDNA and our consortiums that we have, what's great about those is these, these solutions are not geared towards data collection to any particular market. They traverse into every vertical that we work in, right? So, and I think that's a really important differentiation is the depth of our customer base is what adds the value. Because a lot of times if you're, if you're specifically working, if your solutions are tailored for a specific market, gaming, financial services, retail e com neo banking, if you're gearing towards just that style of base, right? The data that you're collecting is going to live just in that environment.

[00:18:20] But with GBG, our solutions transcend, right? Like my sister company, Locate, for example, their reach is incredible. When you're factoring in insights from all these different sources, Verticals, it's easier to find fraud because what we see often, right, it would be foolish for these fraudsters to spend all this time stealing, collecting, creating this data, using it one time and walking away.

[00:18:46] It's an investment, right? They're going to use it until they cannot.

[00:18:49] Money Moves: Find It Faster

[00:18:49] **Heidi:** And a lot of times, and, and I'm sure your, your listeners know this, money moves. And a lot of times their fraud is one part of the process. They may have been, you know, it may have been a credit card that was opened and all the money was was extracted off in some method, but then it's got to get moved and maybe it gets moved through a payment service and then that's going to go into a different bank account or it gets moved to a prepaid card where it's got some level of of transients, right?

[00:19:15] Because of our reach across our solution sets, we can watch this move, right? Our ability to find it faster and flag it sooner is expanded because we're watching it move. And we actually will see this in our data. We will see a fraudster go from one customer to the next, to the next, to the next, to the next.

[00:19:35] And the way that we've engineered these solutions, we can provide those insights to all of them. Right? This was iffy when it came to you, then it went to this person and this person and it's moved and it's traveled and that greatly enriches, right, the probability that this is a fraudulent activity.

[00:19:51] Because again, going back to, you know, what you were talking about, I mean, what, why would a, why would a consumer go open 10 bank accounts in one day? They wouldn't, right? There's just no reason. Unless they're gonna start running money for the mob, right? They're not doing that. So, it's

[00:20:07] **Satwant:** the only, I was thinking the only reason you do that is if you win the lottery. And that's about it.

[00:20:12] **Heidi:** too, right?

[00:20:13] And you want that FDIC insurance at every account, right? A thousand, yeah. So I think For us, right, the facts, those, those would be the two key differentiators I'd stress. And for anybody who's looking for better identity tech, right, these are the questions I would ask is, what is your base made of? What value am I going to get out of your solutions if they're offering a consortium model, right?

[00:20:33] What's your reach? What's your coverage like, right? And also, too, have those models been built through a privacy driven lens, which ours all have, you know, so are they compliant with things like CCPA, CPRA, the New Virginia data laws, right? What are your obligations under that? Ask those questions. That's a key differentiator.

[00:20:51] Because you don't want to be in a position where you're getting the value of this, but you find out it was built through a non compliant lens or it's not privacy conscience. So having that, having that extension and that reach, but also to, you know, technology that has that tenure because data has changed how it's aggregated, how it's sold, how it's made what's valuable, what's not has changed tremendously over the last 15 years.

[00:21:14] And so a solutions provider that has lived through that and adapted their, their tech accordingly is one that. is going to be able to give you a lot of trust and value because the tech's well built.

[00:21:27] Layering Data: Data Breaches & The Dark Web

[00:21:27] **Satwant:** One question that just came to me, just purely out of interest, all these dark web marketplaces where you can buy IDs from as little as a few dollars. I'm guessing that's one of your data points that you feed into your system. You grab those Data dumps as well, and just feed it into your system.

[00:21:43] **Heidi:** It's not one that Americas is currently offering today, if I'm being honest. I think they add a lot of value. I always recommend to my clients that you look at the lift that insights like that can provide and possibly use it adjacent, but above what we're doing. Cause it's one, it's similar again to my sister company, Locate.

[00:22:03] You always, you know, layering tech in a manner to get to the best outcome is going to give you the most value. That's a great way to kind of at the top of a funnel screen out things that just do not, that you should not be transacting with. But the tricky bit I think about the dark web searches and is that at some point everybody's data gets breached, right?

[00:22:23] So if you're going to leverage that type of tech, you want to make sure that you're not screening out people that are that have been tied up in that, but are not the person that committed that fraud. They just maybe mistakenly clicked an SMS phishing link that or smishing link that collected their data.

[00:22:39] Right. So,

[00:22:42] **Satwant:** I think I might've had that in the past as well

[00:22:44] **Heidi:** you know what? I had one catch me one time. It's like I was saying, I work in the space that happens to the best of us. Right. So, yeah.

[00:22:53] Industry Consortium Fraud Network & Cross Border Verification

[00:22:53] **Satwant:** Another point that interested me was you offer a multi industry consortium fraud network, you also do as well as domestic, cross border identity verification. So it might be good to talk about that and how that is implemented into your solution.

[00:23:14] **Heidi:** Yeah, absolutely. So within GBG, we have built we, we call it the network alert here in the U. S. You would hear about this outside of the business also through our trust framework, but essentially it's a contri it's a contributive model. It's a value addition to being a customer of GBG ideology here in the U.

[00:23:34] S. So we don't. We do not charge for this, it's just shared insights, but that model, our clients that work with us, when they find that activity is fraudulent in their base, they can share, not a person, so it wouldn't be Heidi, it would be a piece of data, so maybe it's the address that was problematic, the email that was problematic, domains, they share that information into the model, flagged as being associated with fraud with a reason.

[00:24:02] And they put that into the system on their behalf. We have many clients that contribute to this and then we will actually send them analytic pieces. So if I am customer A and I find out that an email address that I got at registration, like I've collected it, I've sent it into ideology as part of my identity verification, customer B may have flagged that a year ago, or 6 months ago, or a month ago as being associated with a specific type of payment fraud. Do I'm not told who customer B is when they made the contribution, but I will get signals back that say, Hey, by the way, somebody else has said this was fraud for this reason. And you can take that and include it in your model, right?

[00:24:46] So, and again, going back to the, you know, our consortium, because it's the same level of reach, right? Finding that out, it's a really valuable data point. At any given point, it has around 30 to 40 million attributes in it. You know, obviously data needs to age. So we do recommend that thing, our clients age things out of it.

[00:25:05] And It allows customers to anonymously share feedback with each other, which is great. It's kind of like a community, right, that they can do that with. And where we also differentiate with this as far as I know, we were one of the first U. S. tech companies to offer something like this that was an identity services provider, but we also back these insights with a fraud team.

[00:25:26] So we have a dedicated fraud team inside of the company. If you want to ever talk to the leader of that team, her name's Crystal Blythe. She's on our page, VP of Fraud. She helped build this entire model. She's been with the company for over 10 years, but Crystal and her team actually pour manually over data sat every day.

[00:25:43] So they look at our client data, they look for things that need to be reported to my team as potential trends that we need to add some analytics or some modeling against. They also report that feedback to clients. So they will say, you know, your decision rules or your model didn't catch this, but we found it because of subsequent activity and we would recommend that you take a second look.

[00:26:07] And... Then we have a,

[00:26:10] **Satwant:** so hold on, when you say a customer's model didn't find something, that would be. But that would be your solution that they're using.

[00:26:19] **Heidi:** yes.

[00:26:21] **Satwant:** So I'm just trying to understand what you mean by that. How does that work?

[00:26:25] **Heidi:** Yeah. So different, there's different reasons why that could happen. So maybe when they onboarded with us, right, they wanted to take a lower level of risk profiling, right? They don't want to be astringent on a certain piece of information. So we might recommend that you put some friction or decline, you know, this, this, and this, and they may look at the outcome and go, We don't know that we want to do that right now.

[00:26:50] So this, and also too, well, hold on, let me take a step back. So that can be part of it. The other part of it is that, you know, with all these different solutions, sometimes a client may choose to not take verification of a phone, right? They may say, we're getting mobile insights from somebody else. We don't, we don't need your, your tech, right?

[00:27:08] It could also be that, you know, like we talked about before, data will traverse. It could be that they were the first customer. In a line of fraud, right? And they are only, they only know what happened with them because maybe they were the first one impacted. There's lots of different reasons why this can happen.

[00:27:24] ouR system has like, millions of settings combinations it can do and lots of little dials to turn and tune things so that we can support those different verticals. Her, her team, why they're so valuable is as the nature of data changes. And I can give you a cool example of this during COVID, but like as the nature of data changes, as the risk to the customer changes, that information's not static.

[00:27:47] It's dynamic. It's always shifting and changing. By her team finding these patterns and reporting back things that didn't get through the way that they're decisioning through us today, it allows us to come back in and start turning those knobs and those dials and really refine the settings to address a particular layer of fraud, right?

[00:28:07] So that's, that's how those things can happen. And then her team helps them basically always stay on the edge of what they need to be doing to either loosen things up or tighten things back down to dynamically adapt to a new situational instance of things that's going on. So.

[00:28:24] **Satwant:** I've got this vision of all of you working in this bunker every day, with lots of, lots of screens in front of you, like in

[00:28:32] **Heidi:** Well, I will say that is appropriate. I mean, during COVID, people were taking the monitors. I have one of the folks that works for me, bless him, he has six monitors and he's just constantly, he's my product data analyst, but yeah, that's about appropriate. Most of our fraud team has multiple screens that they operate against looking at things, but you, you just have to Sat.

[00:28:51] I mean, We use machine learning as part of this, but it runs post cycle. We don't run it up front. We run it after. So every day, because I mean, AI is fabulous. You need to use it to speed this up, because if you can imagine the quantity of traffic we're processing every day, we actually utilize machine learning as part of this cycle, right?

[00:29:10] So client runs a transaction, it gets It really says that's the consumer side of things. So they will determine, yeah, all of those issues are bad. Then they will go back and report the bad and they will determine what's on the consumer Those are just dead end primitives just beyond like communication and thinking.

[00:29:30] Runs and runs and runs, right? So AI is fabulous to speed up this process, but we don't feel that you can be solely reliant on a silver bullet. It doesn't exist, right? If anybody creates it, they're going to own the entire market for onboarding individuals in any capacity, right? It, it absolutely, the scams are so different.

[00:29:50] They materialize so different. Consumer data is so variant, you have to have sophistication, and it has to be, you need a relationship with an identity solutions provider that's going to keep you abreast of these things as they're constantly moving, because they always are. That's the best way to handle it.

[00:30:08] Fraud Trends: Surge in Fraudulent Domains

[00:30:08] **Satwant:** And that's what I wanted to move on to next. What trends are you seeing currently with fraud? I mean the extent to my knowledge comes from some YouTubers who actually fight back against scammers. And I read Krebs and things as well. So, but it'd be good to know what's, what's happening right now, which maybe somebody's not aware of or, or even myself.

[00:30:27] **Heidi:** Yeah, oh gracious. I think one of the things that I have found pretty shocking over the last six to nine months, it continues to propagate. There are a number, again, digitization. There are a number of businesses online where you can buy registered domains You can get banks of phone numbers. Now, they're used primarily for small business. You can get websites.

[00:30:55] And there has been an absolute surge in the usage of those domains and those banks of numbers to file fraudulent accounts. For whatever reason, I guess it's easier access. I do know that some of the TLDs are seemingly aware. I know they're very aware of, you know, the bot attempts because when, when you're going to do a digital account creation, right, what are the, in order, so you need identity data, but what are the other things you need, Sat?

[00:31:20] You need to be able to have contact pieces. That's going to be a mobile number and an email address. You can't just falsify those because what are they going to do, Sat? They're going to send you a registration email and they're going to send you an OTP to finish it, right? So you actually need to be able to hold those and use them.

[00:31:35] And I don't know if this is something like, Some of the TLDs, because I know Gmail's gotten a lot more stringent about creation, I think it's challenging for some to create banks of emails in the manner that they used to. Maybe they're in a smaller quantity because there's so much over usage of some of them.

[00:31:52] But I think leveraging these third party programs like this, suddenly you've got a brand new domain that has no user creation against it. You can create Thousands through that at a very expedient rate and it's not going to be governed the same way that Gmail is, right? And likely because it's a new domain, if there is a client that is using a negative list, they're likely not going to have it because again, it's a completely new domain.

[00:32:16] So from a risk perspective, it's going to look clean unless you are diving deep into the detail of the domain, right? Likewise, the mobile numbers, unless you're diving deep into the mobile numbers, To try to assert ownership to identity, to look at tenure, to look at the type of account it is, is it prepaid, postpaid, is it a VoIP?

[00:32:34] If you're not taking the time to look at that detail, it's going to look okay because it's not going to be on your flag list. And we continue to see that propagate again and again. That's pretty wild to me.

[00:32:44] The Investment Fraudsters Make in Synthetic Identity Profiles

[00:32:44] **Heidi:** Again, that just shows these guys, the gain must be so good that they're actually willing to spend and transact, right?

[00:32:51] They take the time and the money to build the synthetic. Identity profiles or steal the data. And then in tandem, they're actually paying for business services to create banks of information that they can use. So I think the surge of that has been pretty shocking. And we find it, we, you, we can find it through our solution when we do, it's always, let's get it.

[00:33:10] To the client as quick as possible, find the accounts. It's been, if there's stuff that got through, have them get them shut off. But that's been, if I look at our contributed consortium, that's been 1 of the biggest contributions we've had this year is email domains and mobile numbers.

[00:33:23] The Surge in Voice Over IPs

[00:33:23] **Heidi:** I think as a consequence of that and also the increase in Voice Over IPs again.

[00:33:28] They're very simple to obtain. You can, you know, host them in any format that you like. So if you think about, you know, if you're, if you're filing fraudulent applications on your PC, you've got multiple screens going. I've got a screen where I'm taking in all these mobile numbers. I've got a screen and that's all hosted, right?

[00:33:45] My different voiceover accounts. I've got my emails loaded up. It makes, it makes this a very clean, organized process, right?

[00:33:52] Efficiency of Fraudulent Submissions

[00:33:52] **Heidi:** And when we look at the timing of these submissions, it's wild. I mean, they're like. Almost timed perfectly a minute, two minutes apart. So it's either running on some kind of computer program or these guys are just that efficient.

[00:34:04] The business model is so efficient that they're just rapidly doing that for creation.

[00:34:10] Regulation and Legislation Around Money Transfers

[00:34:10] **Heidi:** From a payment perspective, I think it's interesting that, you know, there's been lots of legislation around you know, sending of money to different individuals, what the limits are for that, how they're going to start reporting it.

[00:34:22] It's been wild to see that threshold of, of activity. Get reduced to appear be under the radar. That's been pretty wild to see. And I think likely as the government continues to turn the dial on the regulation around P2P transfer, right? I think we're going to continue to see those guys potentially trying to find some alternate method to get their funds moved around.

[00:34:45] But again, that's, that's a challenging problem to solve.

[00:34:48] The Challenge of Differentiating Fraudulent P2P Transfers

[00:34:48] **Heidi:** What's the difference between the fraudster that's using P2P to funnel money they've stolen against me and my boyfriend kicking back the same 40 cause we keep taking each other out for dinner. Right?

[00:34:57] **Satwant:** Yeah. When you say PDP, you mean like something like PayPal or Venmo,

[00:35:00] **Heidi:** Yeah. PayPal, Venmo. Yeah. Cash App, Zelle. They, they all, I mean, there's, you're seeing now it's in the US, right? They passed laws in the last, I don't know the exact timing. I'm sorry. It's been about 18 months, but to regulate how much, if, if, if a consumer is, is sending over certain limits, it has to be reported to the IRS's income.

[00:35:21] That's their way to look for people that are trying to gain income under the, under the radar, right? So I babysit and I pay cash, right? They're trying to track that activity so they can get it for financial, but there's also a regulatory side to that because they know that fraudsters, mob cartel, they use those mechanisms as well where they can to transfer the, wash their money and get it moved around.

[00:35:42] So they're trying to get a handle on that. That legislation I think was a Big step. It's going to continue to tighten. And it'll be curious to see what avenues those guys go to next to try and get their money moved around

[00:35:54] **Satwant:** Yeah. the one I read about recently was it, it was in the, in the, one of the online newspapers here, a lady lent her friend some money about 50 pounds or so, and then that person paid her back, but, but paid I think three or 400 pounds and then said, oh. I'm really sorry, I was supposed to pay you 50, but can you just withdraw the cash

[00:36:19] **Heidi:** and give it to

[00:36:19] **Satwant:** and give it to me?

[00:36:20] And she thought, yeah, sure. You've made a mistake. And then the next thing she knew, her bank account had been shut down because they were doing the travel, travel rule stuff and said, well, that, that account that the money came from.

[00:36:31] **Heidi:** Was

[00:36:32] not

[00:36:32] **Satwant:** of crime or whatever,

[00:36:34] **Heidi:** gracious.

[00:36:35] **Satwant:** So, so even in your own friend network, you could potentially get screwed over like that.

[00:36:42] **Heidi:** Absolutely.

[00:36:44] Predictions & The Future

[00:36:44] **Satwant:** What's your predictions for the future in terms of next year, in terms of what's happening with fraud and, and cracking down on it, it's a constant cat and mouse game.

[00:36:53] **Heidi:** coming

[00:36:54] **Satwant:** you know, we're

[00:36:54] coming up, we're coming up to Christmas now. There's going to be lots of shopping and

[00:36:58] **Heidi:** to shopping. Retail

[00:36:59] **Satwant:** lots of fraud as well.

[00:37:00] **Heidi:** holiday fraud. Oh, a thousand.

[00:37:02] **Satwant:** all that stuff. So

[00:37:04] **Heidi:** a

[00:37:05] **Satwant:** it's a good time to talk about what, what's coming next year. If you're allowed to share anything cool that you've got coming up, perhaps depends on how you want to address that question.

[00:37:13] **Heidi:** share anything.

[00:37:19] Business Verification Is Increasingly Important

[00:37:19] **Heidi:** I think as the digital consumer market has grown so quickly and has so many people attempting to get into it, it's become very crowded. I believe that business verification in the U. S. and specifically the small to mid, the small to medium business, there are very, very many independent contractors and small business owners in the U. S. that still have a very heavily friction process.

[00:37:44] It's It's very challenging for them to get access to the lines of credit financial services. It's even more challenging if you think about retailers that offer business lines to make sure they can make collections against that. I believe as the consumer market continues to get crowded, that business is the next step.

[00:38:01] So what I would recommend is that anybody in financial services look at that as a potential opportunity to open up and find new ways to offer your products. Because I... Believe in the next two to three years, that's going to be the next gen market that everybody wants to go after. They are almost completely untapped from what I can see as far as offering digital onboarding products.

[00:38:22] And I think be thinking about that. That's just a recommendation for me.

[00:38:26] The Impact of OpenAI on Fraud

[00:38:26] **Heidi:** Relative to fraud, I mean, I think the elephant in the room is ChatGBT, OpenAI. If you are not, If you haven't gone to that site and tried to use it and seen what it's capable of and the information it's capable of providing, I would recommend that you do it today.

[00:38:46] Or get someone on your team, get someone that's educated in AI and machine learning. If you're not using it in your company today, think about the application of it and can it help improve your systems and what you're doing. But also, be on guard, because I fully believe that now that that is readily available, the fraud, the way that it's being committed, is going to be supercharged through OpenAI.

[00:39:15] If it's, it's terrible conundrum, because it's such a... valuable and interesting tool, I think, for humans, right? We're all entranced by it. Learn about it. And if you have someone in your company that's scrappy and good at figuring things out and is a critical thinker, let them play with it. Think about your product.

[00:39:35] Look up your company. Look up information about your account opening process. Look and see if it can give anybody any insights into potential vulnerabilities and how to cheat your company. Look and see how it talks about security, privacy, technology, and be advised that likely Or not likely, I mean, I would guarantee it that it's opening avenues for fraudsters.

[00:39:59] So try to get a good understanding as an organization of what it's capable of and apply that knowledge to any potential weak points you may have in your own processes because likely that's going to be the next gen. Evolution of, of how we see fraud traverses, these guys were already super charged with, you know, being able to spin up servers and, and run rapid quantities of activity and share information with each other.

[00:40:23] And, you know, transacting and sharing and selling information on the dark web. Now, they've got artificial intelligence to back all of that, and they're very smart. So don't let them get ahead of you on it. Try to get an understanding of it and look for vulnerabilities in your, in your, and your digital workflows to make sure that you're not going to be taken advantage of.

[00:40:42] Right.

[00:40:43] **Satwant:** a lot of fraud is committed overseas where person's second language might be English, not first, and it can perfect if you're using chat GPT to even just say, write this. As someone in the UK or US would,

[00:41:02] that alone is just a huge

[00:41:04] **Heidi:** It's huge because how are you going to differentiate between a phishing email? Now, today, it's easier to spot it with the grammatical errors, but if that gets weeded out, Right. And, you know, again, if, if they have access to cleanse domains, how can you prevent that? Right. It's very challenging.

[00:41:20] So I would just caution everybody. I mean, just take the time to learn what, what its limits are and what it's capable of doing and make sure that you have proper filters against that. I mean, yeah, that was

[00:41:32] **Satwant:** I mean, yeah, that's, that was always my filter. I'm a, I'm a grammar and punctuation Nazi. So, um, I can't use that anymore necessarily. So, it's crazy. Okay. Well, thank you.

[00:41:45] Know Your Business (KYB) Verification

[00:41:45] **Satwant:** One interesting thing I read was that

[00:41:47] **Heidi:** that your

[00:41:48] **Satwant:** your Know Your Business (KYB) compliance requires business to, to verify the Ultimate Beneficial Owner Maybe you could talk about that for a minute

[00:41:58] **Heidi:** Yeah.

[00:41:59] **Satwant:** what that's all about.

[00:42:01] **Heidi:** Well, so that this is probably the most challenging layer of being able to perform KYB digitally or even physically. Right? And in the US, it's, it's not uncommon for the. Folks that you'd want to target in this area, right? My father's a great example. I'll give you one. He has been so readily challenged getting lines of credit at so he does roofing.

[00:42:25] He's a, he owns a roofing organization, a roofing company. It has been so challenging for him to get lines of credit or bank accounts because he has multiple LLCs, right? One's in Florida, one's in South Carolina, one's in Georgia. I think he actually has two in South Carolina. But he also funds some general contracting house framing, right?

[00:42:43] And he always gets screened for being risk because he has these different LLCs. And I've tried to explain to him, you look like you're cleaning money for the mob. That's why, like Florida's a hotbed for fraud. So is Georgia. You have these LLCs, you're not doing a ton of money through these things, right?

[00:43:00] These individual business groups. And, you know, for him in particular, every, his, his personal digital Experiences are so seamless, but his small business interactions are endlessly painful, right? And add a lot of lag time to his projects when he needs to lean on, again, getting, getting a line of credit at a house to, at a warehouse to complete a roof job.

[00:43:21] And what's challenging about verifying the ultimate to. The ultimate beneficial ownership in the U. S. is that consumer data is very cleanly organized. It's in many different places. You've got public record aggregators. You've got credit companies. The IRS has access to information. There's lots of different data points you can pull to assert identity that are all compliant.

[00:43:47] Business information and things like small businesses, LLCs these smaller incorporated organizations, their information is not as readily available. There's only some states that release that information digitally or if at all. It's very challenging the way that these sometimes get brokered and created sub organizations having, you know, sometimes more than one beneficial owner.

[00:44:12] So when you get into the point, you have to do that verification. It's very challenging because that data can be hidden. Right. How do you know who actually has ownership of this business? The way these things are brokered, bringing in the complication of the 50 states where that can change. It just is a really challenging shifting target to do.

[00:44:30] What we've provided is data insights that can do that verification for about 50 to 60 percent of the, of the U. S. consumer base, right? And for us, we pull that information from multiple data sets we pull it from public record, government licensing, secretary of state filings, business credit header data, and we are able to assert that through a few levels and verify Ultimate beneficial ownership against again, like my father's scenario where they potentially have multiple businesses that they're joined to or where a business is, you know, these sub corporations that have been created.

[00:45:05] We can do that on about that much of the base. Again, I think in a future state. As we continue as here in the states to digitize data and, and the states get more on the same page about releasing information. I think you can go fully digital. What that allows you to do is automatically approve or disapprove information immediately.

[00:45:27] Right? And then you can step the rest into. A more traditional process where you're asking for the Articles of Incorporation, the business license, Secretary of State filings, whatever paperwork you need to get that assertion completed. What I also like about what we've done is we've brought in kind of our tricks and our plays we've learned with KYC.

[00:45:47] So, from a digital perspective, the challenge is still there. You know, and the interesting thing about business data is because, you know, you can go to a local office and pull business license information if you aren't the owner of it and, and business, business record data. It makes it challenging to want to be able to, I think, sift out fraud from non fraud, right?

[00:46:08] But we find that there's the same type of challenges. So being able to look at a property and see if, if the address that they've given, is a commercial or a non commercial, that's one of the ways we've integrated our solution set with Locate. Right. Because our sister company, Locate, knows if something's a CMRA or a residential address.

[00:46:25] So, can we bring that into the play here and see, did they actually give you a commercial address for the filing? And is that the same one that's on the paperwork, right? Looking to see if that property is vacant. Have there been any bankruptcy filings against the judgment, right? Going and looking at some of the historical...

[00:46:41] If you're looking at the data that's around what they've given. Is it a, is it a mobile number? Is it issued? Is it a corporate mobile number? Is it a personal? Right? Does it have any assertion to the owner? There's great ways that data can enhance the UBO verification beyond just confirming it. It's also looking for Potentially fraudulent scenarios in that as well.

[00:46:59] So from our perspective, that's, that's what we've brought together as we went and found some really great data. We had some great data and we've built a solution set that tries to give you as much information about the business data that you've collected as you can as part of your S& B onboarding or.

[00:47:15] You know, we have people that like interesting use case I had for it with a client I worked with. He has a series of check cashing locations, and in his case, about 10 percent of the traffic he got that came in the door was people cashing on behalf of a business. And he said, I. I'm only making five dollars on these or so.

[00:47:35] Like, I don't want to, like, I don't, I don't need an enhanced check here. I just want some kind of insight if this business is legitimate or not because I'm gonna cash this and then I'm gonna find out two weeks later about two percent of the time that it's not. Right. This is a fake check. And given how challenging check fraud is, which we could probably have a whole conversation about that at some point, right, Sat?

[00:47:57] But

[00:47:57] **Satwant:** Me if you can.

[00:47:58] **Heidi:** right, exactly. But through data we're able to help him screen a fair amount of that, a fair amount of that stuff out. Right. And so that's, there's other applications for this other than just onboarding. Right. But again, that's data coming in at, at a, at a great rate with a great solution to help prevent him From dealing with this where again, it's a smaller amount of his business.

[00:48:21] It's still making money, but in every region he was challenged by that and had a pretty decent fraud rate he was having to deal with. And this was a great application of technology to help close that gap up.

[00:48:33] **Satwant:** I'm glad I asked that question now because in the UK, you probably heard of Companies House in the UK where businesses are registered and articles started coming out from what I've seen last year, where random people overseas are registering companies.

[00:48:49] In the UK for addresses they don't know, they've never been to, they don't know these people, they're just picking addresses out of the address book because they would have seen a vulnerability there or lack of checks. So, yeah. So you're, you're putting all that together, to counter it. So, okay, great.

[00:49:06] Glad I asked that question. Thank you.

[00:49:08] **Heidi:** Thank

[00:49:09] Get In Touch with IDology

[00:49:09] **Satwant:** Getting towards the end, I'd like to ask you in terms of how customers can engage with you. Because you guys work with all sorts of industries that we're just going to read out a few here.

[00:49:19] You 4, 000 plus customers, you know, finance, banking, fintech, which you mentioned already. You work with government and border control, retail, travel, automotive, a whole. Bunch of things. So what's the best way for a business to engage with you and by the looks of things, no matter what industry they're in?

[00:49:40] **Heidi:** Absolutely. So you can always go to our website and we have some really great content around. We publish annual studies around fraud. We do that locally in us. Again, we mentioned our global state of identity, which our parent company publishes. There's just some really great insights on there if you want to get some fraud playbooks and some insights into our company.

[00:50:00] But on that, there's also a contact us form, which will connect you with our organization, our sales team, and their, Always happy to show you what we're working on, give you a demo of our solution, see if we might be a good fit for you. I am also available on LinkedIn, and if you just want to have a chat about fraud or things that are going on, please always feel free to send me a message on LinkedIn.

[00:50:21] You can find me Heidi Hunter, I work for Ideology or GBG, I'll come up under either. Please feel free to give me a chat. I love when people say hi. Even if you want to challenge my thought line for this, I greatly welcome it. So please feel free to give me a, give me a message and I'm always happy to make a warm introduction to anybody in the company who might be valuable to you or just talk to you about fraud and product.

[00:50:44] **Satwant:** Great stuff.

[00:50:45] Your website is idology.com and on Twitter you're @IDology and do you provide demos and do you have any events coming up where people can meet you folks?

[00:51:01] **Heidi:** we're actually getting to the end of what we would call trade show season here in the US. But we are always at places like G2E, the gaming conference. We're at Money 2020. So you can always find us there. We go to a lot of lending events FinTech events FinTech Nexus.

[00:51:18] We're at FinTech Nexus. All the shows like this across the states. So, likely you will find us at one of the key financial services or FinTech shows always or other, other conventions. I think given we're at the end of that season, we don't have anything that I'd say is upcoming. Likely in the spring we'll start kicking back off going to things again.

[00:51:36] We, oh goodness, what was the other question you asked me? What do we have available? Oh, demos!

[00:51:42] **Satwant:** Yeah.

[00:51:43] **Heidi:** Yeah, absolutely,

[00:51:44] yes.

[00:51:44] **Satwant:** you mentioned, you've got lots of great information on your website, but a lot of people watch videos and audio and podcasts now. So what, what do you have, available there?

[00:51:52] **Heidi:** we do have some links on there that walk you through how we like to approach digital onboarding through things like orchestration and fraud prevention and the value of, you know, leveraging technology to give great consumer experiences. So you can find some great video links on there to kind of get a sense of that ideology experience and some of the products that we offer as well.

[00:52:13] Chit Chat

[00:52:13] **Satwant:** Thank you so much. And going to finish off with a fun question. I always like to know what people are reading or watching or learning about at the moment. I just bought Arnold Schwarzenegger's new book. I think it's called Be Useful. So I'm looking forward to getting stuck into that. Oh, what's that?

[00:52:30] **Heidi:** I've got it right here. So

[00:52:31] **Satwant:** Devil in the White City.

[00:52:33] **Heidi:** I love historical. Novels of any kind. So I am always reading like my, one of my favorite books is Benjamin Franklin's autobiography. I read it at least once a year. I think it's fabulous. So this, this is Eric Larson. I'm a big fan of his. He has another one that's about the Tesla and Einstein Edison.

[00:52:53] Situation, but he basically, it's, it's not historical fiction, it's very factual, but it's just things that you've never heard about. So there was actually a serial killer at the 1880, uh, Chicago World's Fair. So this is a very interesting story about the dichotomy between the guys that put this event together and how challenging it was, and how there was a serial killer making his way through.

[00:53:16] Which I had never heard about that aspect, right? We've heard about, I've heard about the World's Fair a lot. One of my favorite movies is Meet Me in St. Louis, which is all about, you know, the World's Fair. But this has been, this has been pretty tremendous. And likely since Christmas is coming up, I will be rereading Charles Dickens A Christmas Carol because I just think it's one of the best books ever written.

[00:53:35] So,

[00:53:36] **Satwant:** Nice. Thank you so much. Well, give me some work to do. I haven't seen that movie that you mentioned either.

[00:53:41] **Heidi:** oh, it's so good. I'll send you a link. You can

[00:53:43] **Satwant:** What's it

[00:53:43] called? St. Louis?

[00:53:44] **Heidi:** Meet me in St. Louis.

[00:53:46] **Satwant:** Okay. All right. Well, I'll definitely watch that over Christmas.

[00:53:49] **Heidi:** It's very, very good. It has the lady who was in Oz oh my gosh, The Wizard of Oz. And I'm missing her name now, but... It'll come to me after we hang up, but yes, yep. It was made in the, in the forties. That's a great movie.

[00:54:04] **Satwant:** Fantastic. Great. Well, thank you so much, Heidi. I really appreciate that.

[00:54:07] **Heidi:** that.

[00:54:08] Thanks

[00:54:08] **Satwant:** almost at the hour on the dot. I know we could have talked for ages, this is a huge topic, so you're welcome back whenever you want to in future, if you can handle

[00:54:16] **Heidi:** rest of your week. Thank you, Sat. You too.

[00:54:18] **Satwant:** so thanks a lot and have a enjoy the rest of your week.