FINTECH ONE-ON-ONE PODCAST NO. 405-DON CARDINAL

Welcome to the Fintech One-on-One Podcast, Episode No. 405. This is your host, Peter Renton, Chairman and Co-Founder of Fintech Nexus.

I've been doing these shows since 2013 which makes this the longest-running one-on-one interview show in all of fintech, thank you for joining me on this journey. If you like this podcast, you should check out our sister shows, PitchIt, the Fintech Startups Podcast with Todd Anderson and Fintech Coffee Break with Isabelle Castro or you can listen to everything we produce by subscribing to the Fintech Nexus podcast channel.

(music)

Before we get started, I want to talk about our boutique all meetings event, Dealmakers East, happening at the Ritz Carlton South Beach on February 7th and 8th. Dealmakers East is all about meetings, there are no keynotes, no panels, it is 100% focused on hand-curated meetings, whether you are looking to meet fintech CEOs, bankers or investors, we have you covered. Now, Dealmakers events have consistently been our highest rated events so go to fintechnexus.com to find out more and register.

Peter Renton: Today on the show, we are talking Open Finance and Financial Data. I am delighted to welcome Don Cardinal, he is the Managing Director of the Financial Data Exchange also known as FDX. Don provides his perspective on the state of Open Finance today, we go through the five core principles of FDX, we talk about their API standard, he provides examples on how that actually works in practice. We talk about the different types of members of the consortium and how he manages the differences between them, we talk about the Open Financial Exchange, the OFX work group, we talk about FS-ISAC and explains exactly what that's all about and Don also provides his vision for the future of Open Finance and what barriers need to be overcome to realize that future. It was a fascinating discussion, hope you enjoy the show.

Welcome to the podcast, Don!

Don Cardinal: Good to be here, thanks for having me.

Peter: My pleasure. So, let's kick it off by giving the listeners a little bit of background. I know you spent a lot of time at one of the large banks but give us some of the highlights of your career to date.

Don: I'm a recovering CPA so I went to university for many, many years ago and I've had a distinct career at Bank of America before I retired from BofA to come do this, it's the real mission and talk about the FDX mission in just a bit. But I've done everything from Trust & Estate work to IT Support, to IT Audit, to Cyber Security was my last hop and, of course, digital banking and managed a lot of the consumer authentication pieces of the digital banking side. So, I was Head of Liaison at InfoSec and then I did InfoSec which led me into a lot of the risk-based stuff that we're doing with FDX so it was a natural progression.

Peter: Right. So, tell us a little bit about that move because you spent 23+ years at Bank of America and you go to sort of a start-up, what attracted you to this opportunity, I guess?

Don: So, within Bank of America, previous to doing the work in Open Finance I was doing their email authentication and getting them to DMARC it's a big thing, it's actually helping in reducing the amount of phishing and spam and brand impersonation and I got good enough finally at BofA that I was actually, through FS-ISAC, which is a consortium of FIs around the world that share signals and best practices, actually doing talks there and helping other FIs. Here's what I did that was not so good, here's what I did that was much smarter once I learned how to do it, and I started looking around okay, that's great, we're at a mature level, what's the next biggest risk vector?

And in having been in financial services for, you know, gosh, 20 something years and having run their military banking arm for a number of years where we literally did everything from ideation to invoice, bank-in-a-box, dealing with account aggregation and bots and harvesters and the notion of held away credentials was really the next biggest low hanging piece of fruit out there in the ecosystem. If you think about it, for any bank, credit union, brokerage, roughly a third of their digitally enabled customers have shared their ID or password with another entity in the last year.

You know, they'll say, no, I didn't, but did you get a mortgage in ten seconds? Yes, I did. Did you do your taxes with two thumb prints? Yes, I did. They don't consider the two the same, but they in fact are and I thought well, wait a minute. That's 100 Million financial pairs floating around. What if we could get rid of those, what if we could give everyone the same opportunity, the same access, the same tools and utility but not have to share credentials and what if we could do it in a way that had enterprise grade security and what if it was for free? So, I've gone from securing the financial services email ecosystem to now looking at the credentials, okay, let's just keep fixing problems, you give me a puzzle, I'm a happy boy. We did email off, that's great, now we want to fix, you know, screen scraping, held ware credentials and get everyone to this new world of API-based and so, I retired from BofA to come do this.

Ironically, FS-ISAC had an aggregation working group, it was doing okay and I always represented Bank of America on it, but we needed the fintechs, we needed the aggregators, we needed other parties as well. Strangely enough, in a data you have a sender and a receiver, right, Modems 101 so we realized we needed that, we couldn't do it within the FS-ISAC structure because they are structured primarily for financial services companies. So, we created this net new entity to move this forward and because I was so involved in the creation of this, the vision for where we wanted to go that tapped me, to be employee number one and lead this thing.

So, I just passed my fourth-year anniversary last week, been a fast four years from who's on it, you know, a few hundred thousand to 42 million consumers on it, gone from a founding 22-member institution to 230 organizations and growing, we have members on four continents now, it's just taken off, there's such a need for it.

Peter: Before we dig into FDX, I just want to make sure that, you know, you talked about this organization FS-ISAC and I believe it stands for Financial Services Information Sharing and Analysis Center, just describe what that is and the work you are doing there before we get into the heart of FDX.

Don: Sure. FS-ISAC is a consortium and there's ISACs in different industries. There's an Aviation ISAC, there's a health care, there's Utilities ISAC, their job is to share signals of cyber-attacks, information about zero day attacks and vulnerabilities and to do so in a way that liaisons with government and effectively provide a network of trusted partners of, you know, under correct issues roles and security and that stuff. Like hey, I'm seeing something, what are you seeing? Or hey, you're seeing this, oh that's a good idea, I'd better pay attention with this or hey, there's a World Cup coming up, is that going to be a good pretext for fraudulent emails, what do you see? Or any other news event and being able to share that information and do it in a way that's shared between trusted partners that complies with all the banks' secrecy laws is really valuable.

At the end of the day, cybersecurity is a team sport and bad guys will go after one FI or another, they will take the tools and keep hitting different houses on the block until they find a house they like. Well, if all the houses talk to each other, they can help make everyone stronger and simply of have hey, I used this and this worked, hey, I used this, this didn't work and have very frank and free flowing discussions amongst practitioners. I think that's the real merit of that and they have 7,000 members on, I want to say, on five continents, they are a global organization for doing this. The risk from how they handle credentials and screen scraping is just one tiny piece of the domains they protect.

Peter: Right, right. So then, describe what the original vision is for FDX and maybe how it's evolved to where it is today.

Don: When you start thinking about the millions of dollars that institutions spend putting up web servers, app servers, paying screens for all the computers they don't care what they look like, they're talking about wasting millions of dollars in hardware, you're talking about IDs and passwords floating around and you frequently have those issues and that's where every great idea starts out. Wouldn't it be great to dot, dot, dot, wouldn't it be great "if"? You could still have these apps come in, but do it with B2B level security, enterprise grade security, wouldn't it be great if consumers didn't have to do any different, didn't have to cough up their IDs and passwords, wouldn't it be great if. And so, okay, that's great, that's the whiff in for the banks, what about on the recipient side? Well, I don't have to hold credentials anymore.

Today's class action happens in the world, those are dangerous, I don't have to hold certain information about you. By the way, I now can get better and more hygienic data because I'm not having to guess about what his balance field is on this credit card screen is. I now know exactly what it means, FI to FI to FI which means the data is accurate. So, when I'm giving somebody advice on pre-filling an account application, if I pick the wrong data amount, I may overextend them credit, I may under extend them credit, one of them it does him a disservice, one may be a violation of law so if I can get their data, their raw material in a hygienic highly available secure way, I can prove their business. There are rare instances where both parties get wins out of doing this, but for different reasons.

Peter: Right. So, what we're really talking about here is the core of sort of this Open Banking/Open Finance movement, right? Before we go into more of the details, describe sort of the state of Open Banking in the US right now.

Don: Sure. The US and in Canada as well because a third of our membership is Canadian and they're doing a lot of good work, but in the US I think they've shown a lot of maturity on the regulatory front saying, okay, we kind of know what policy outcomes we want to have happen. But we're going to leave the technology, the "how", to industry, to people who own the customer risk, the people who own the reputational risk and the market risk in any sort of plans for losses and things like that. We leave that to them because at the end of the day, they are the ones whoever they build to have to live with, the old saying is, architects should be forced to live in the houses they design. Well, similarly, if you let industry design the tech solutions, they are the ones they can live with so I think that's really useful.

Now, currently, I'll give you an update on kind of where we are on regulation. It's not to say there is no regulation, there are some regs out there, it's less regulation in most jurisdictions, Open Banking/Open Finance isn't mandated. Now, the Consumer Financial Protection Bureau in 2017 put out principles about what data sharing should do, just thematic items. And they're in the process of revising Section 1033 of the Dodd-Frank Rule that came out because of the financial crisis that's going to codify certain elements of data sharing, it gives the specificity that the industry needs. What does that mean? That means probably you're going to be required to share data via an API, you're probably going to be required to have some security items in there, you're probably going to need customer permission, you're probably going to need a few things.

So, it's gone from 2017 high level guidance to some very specific things that are coming down the pipe and where we are on that rule re-write is under a small business review called as a SBREFA and regs are big enough, they said hey, this might impact small businesses and small banks, let's poll them and ask them specifically. So, that panel will convene in December/January and they'll say hey look, here's what we propose we're doing, how does it affect you? Typically, 90 to 120 days after that they will release their findings, and then 90 days after that they will release a rule. That proposed rule is very nearly the final reg, and it will actually say okay, here's what we're intending everyone to do, comment on it, see what you think.

And then probably we're guessing Q1 of 2024 the final rule will drop. The law of the land on Dodd-Frank 1033 that will start with what they call implementation period, whatever rule they come up with and, again, we won't comment on policy, but in the past, that's where these have gone and Director Chopra has said, as far as his timeline, that the implementation period will likely start in Q1 of 2024. At that point, whatever guidance things that they say to do, then people will have to start going to.

Peter: Right, right, interesting, interesting. So, you mentioned on your website there's five core principles that FDX operates under, can you just share what those are and how you came up with these five particular things?

Don: The idea being…….you know, we've gone past the idea of hey look, this is consumers data, it's not any one entity's data, this is consumer's data. And so, if you put a customer in the middle what does that mean for the customer to be in charge? Well, they have to exhibit five behaviors, we have a CATTS Principle, C A T T S.

Control, the customer is indeed in control, they decide what data from whom, through whom, for what purpose, what duration they're going to share access. They need the ability to be able to access it,

either they or their agent, and to be able to do it in a secure, you know, machine format, typically, an API is how we interpret that.

Transparency, you need to see what data you have permissioned, you need to see where it's going, so we see different entities, like different banks' standup dashboards now. Hey, do you know, Peter, that you're sharing data with this tax prep company, hey, do you know you're sharing data with this mortgage company, oh yes, I do or oh, I forgot about that one, turn it off.

Traceability, the idea is from a request to any intermediary to the data source and then back out again, every stop on that subway, you should know where it stopped and where it's going. Now, Traceability is important when you have….fraud claims, for example, being able to have attribution of well, where has the subway's been so we know where to go look is incredibly important. Without it, you'll really have a hard time establishing liability and liability frameworks have been the bane of Open Banking regimes for quite a while.

And, of course, Security, we base our security based on the MSTIC security framework, we have some of the leading cyber security engineers and architects for financial services from around the planet working with us, several of them have written things in IETF standards, several of them are part of the OpenID Foundation Identity FAPI Working Group. So, we have a who's who in security off-space and being a former practitioner, I'm proud of the work that they've done. So, I think those five principles, when it exhibits those five principles you really have a system, CATTS.

Peter: Right, right, really interesting. So, I'd like to get a little bit technical, if we can, and talk about the API standard that you guys have enabled, can you just describe exactly what that is?

Don: Sure. I mean, quite simply, it's JSON request responses against a RESTful API, it's both that simple and that complex. The authentication stack we use is the OpenID Foundation's FAPI 1.0 Advanced and CIBA. That 1.0 Advanced is an extension on to OOF2 which is a mechanism for tokenizing access, so you don't have to share credentials. In addition, it incorporates things like mutual TLS so that Man in the Middle is difficult, so you are authenticating both end points to each other. In addition, we also offer the ability to encrypt data or truncate or tokenize data at the field level. So from the actual, if you go up the OSI Model, we'll get really geeky, from TLS1.2 and higher and then going through all the parts of the session. We have security standards baked in all the way through that, and I think it's really important. End of the day, it is just payloads in this JSON objects. Again, we work on defining those.

Now, luckily, we didn't have to go first and our friends in Britain had the courage to do the first draft and, you know, we looked at our friends in Australia and other jurisdictions and we all look at each other's work and I think it's really useful. So, we were able to determine what we wanted to build there, we were able to leverage the same authentication center. By the way, Brazil, Australia, UK and eventually the Berlin group in Germany and other jurisdictions, Colombia is working on it, all RESTful APIs JSON request response all using FAPI 1.0 Advanced, we have the same building blocks under the hood for everybody, that's important. So, that's a big overview of the tech stack of what we have.

The other thing we did is we didn't want to reinvent the wheel so if there was a industry standard already for annuity payments we said hey, can we reference your stuff here so the field descriptions

are all the same because your backend system already has the same definitions and we don't want to write a translation later? Yeah, okay, go for it. So, we've talked to FIDO, we've talked to ACORD, we've talked to MISMO, we've talked to other groups as well so that, again, if someone were to get something defined and in use in the ecosystem for field definition, we replicated in our spec as well so no one reinvents the wheel.

Peter: So then, I'd like to get some sort of a more practical application here because I'm thinking about the work that Plaid is doing, for example, who I know are one of your members. You know, I go and open up any kind of account, like I did one the other day for a brokerage account and connect to your bank and I get the familiar Plaid screen where I log into my bank through Plaid, what is that compared to what you guys are doing, I mean?

Don: It's effectively the same thing. When Plaid facilitates a session, they will talk to Peter's bank and say okay, great, do you have FDX? No, do you have a proprietary guide? No, do you have OFX? No, then we're going to go ahead and scrape you. So, Plaid will acquire the data at customer's permission any mechanism it can, but they are more than happy to acquire data via a common end point. If you think about it, if you're Plaid and you have 15,000 FIs, that's banks, you know, big banks, regional banks, credit unions, neighborhood financial advisors connect to, has a lot of connections to maintain. If they're all bespoke, then I'm constantly having to update those every time there's a change.

Peter: Right.

Don: If they're all common and it works just like a USB where I just plug it in and it works, I just change whatever URL I'm pointing to and it just works, that's so much easier.

Peter: Right. I have some of these aggregation platforms where they're losing connections from time to time and you've got to go and redo the whole process. I imagine that's because it's not just all one thing, right, everyone's got their own flavor of it.

Don: Not yet, we're getting there, we've gone from, you know, a few hundred thousand connections to 42 million consumers. We have this long tail of financial services of, you know, small FIs, regional FIs, they're going to take a while to adopt, just like they took a while to adopt online banking. Not everyone had the online banking we know of today on day one, remember back, well, everyone forgets that, but, you know, Online Banking 1.0, banks had it, but it was simply balance, maybe a few transactions and that was it, eventually, it worked its way through the rest of the ecosystem.

The MV Card, same sort of thing, mobile banking, same sort of thing and we're in that same deal. Now we are a faster adoption curve, certainly, than those three examples. So, you've got this legacy world out there of thousands of end points, some of them have legacy OFX, some of them have FDX, some of them have proprietary, some of them have none of the above and so they're scraped. Over time or organically, they're moving very rapidly to FDX because it's more secure, it's more consistent, it's free.

Peter: I think you mentioned earlier not having to enter your credentials so when you connect with Plaid you have to enter your credentials into your bank and I always think it would be nice to not have to do that, but are you talking about a system where when you're connecting say a brokerage to a bank, are you going to be able to do that without having to enter your bank credentials?

Don: Wonderful point. So, let's talk about the journey and it's called a Redirect Flow around the world. And so, I pull up an app and I think oh, this is a really great app, I want to use it for advice, for investing or buy a car, or whatever, one thing under FDX is a session gets handed over to the financial institution so that any authentication takes place on the FI's real estate.

Peter: Right.

Don: So, I'm not part of the authentication session, I don't see it, I don't know it, anything happens - it wasn't my fault. So to the extent that even though it's Plaid, it's probably handing the session over to the FDX end point at Wells, Citi, Chase, Navy Fed, whomever. So that fixed end is really working well. On the legacy connections that haven't migrated yet, and they're working very hard to do so, they will have an ID or password to do that because they're still having to log in as if they were the consumer. There's still that long tail of legacy connections we're dealing with and we're moving as fast as they can, but typically, the way it's going to work globally and the way it does at the end state, is that app hands it over to whatever bank or broker or real estate company or payroll company even and then the authentication is done locally.

Peter: Right. So, does that mean then if you've got, like you're on your phone and you've got face ID you can just use the native authentication on the device you're using, you won't actually have to enter in your information?

Don: That's correct and we're a big fan of Better ID Coalition, the FIDO Alliance and so the extent that you have WebAuthn or a FIDO2 biometric enabled on your device, technically that redirect is over to Chase's mobile app or BofA's mobile app and then you can just touch the device and say hey, are you sure you want to share those data? Touch your device, yes, it is great, boom you're over and that's it. And I've never keyed in an ID or password, you don't technically have to. End of the day, we want to a world without passwords, everyone does, and so the extent that you have a FIDO or WebAuthn enabled endpoint, all the better.

Peter: Right, right, okay. So then, you've obviously spent some time in cyber security, but, you know, the hackers love passwords, right, because they work and they're relatively easy to access, it seems. But if we move to a world without passwords, your face is your face, your fingerprint is your fingerprint, you can't change it. You know, how do we kind of get to a world where that is secure and the hacker can't get your face and start using it opening up bank accounts?

Don: Good question. Now, two big differences. Remember the Office of Personnel Management that was breached several years back and you had personnel records with biometric fingerprints and things in it that were lost. And to your point, you can't reset a biometric, you can reset a password and other tokens, you can't reset a biometric which is why one of the core tenets of the Better ID Coalition and the FIDO Alliance is the customer holds their biometric in a secure enclave on their device.

When you touch your device or do your face recognition to your device, what's actually passed isn't the actual biometric, it's a hey, they've authenticated it's them, the token goes across and says yep, we've checked them out, he's to whatever degree of a certificate you need and it's really Peter. It's

absolutely Peter, it's a known device and that token goes across and that's what goes across, not the actual biometric.

Let's say you're a bank, I came from BofA, I don't want to hold your biometric, I don't even hold your password technically, all I know is whatever you keyed in matches whatever I've got encrypted. So, you never want to hold a biometric, ever. And so that's why we've written FIDO and call it out in our guidelines for our security and authentication and I think that's the important thing, the customer in the center, right? So, if I stay in control, my credentials stay with me, my biometrics stay with me, I'm in control so it hits two of our CATTS, Control and Security.

Peter: Right, right, got you. Who are the members of FDX, can you just roll through some of the names, some of the more recognizable names that the listeners would know.

Don: Sure. I mean, if you look at…and we have FIs, non-FIs and then fintechs so let's start with the fintechs, we have all the major aggregators, so you look at Plaid, Yodlee Envestnet, Amex, Finicity Mastercard, Pfizer even has a large aggregation business and of course, in Canada, it's Flinks and there's some other aggregators as well. We also have the large fintechs so you look at PayPal, Venmo, Stripe, Block, you've got Intuit and all their brands, Xero and so you have a lot of those folks that have a need for data.

Then the FI side, of course, the usual suspects, Wells, Citi, Chase, BofA, Navy Fed, Regions, Citizens, PNC Bank, we're just going down the list, Akoya, owned by member banks, a clearing house run by member banks, and trade associations. We also have consumer groups as well and that's an important get, we've academics, that was one of the other things that we learned from our friends around the world. You can't just get a regulator, a couple of big fintechs, a couple of consultants, and a couple of big banks and say okay, everyone, you're the group, you're the committee, you have to have a huge community or you have the two young ladies in the garage, you have to have academics, you have to have consumer groups and trade associations. Everyone has to have some sort of a voice and I think that's one thing we did right with FDX and not trying to do all hearts and puppy dogs thing. But for this to be durable and to reflect a diverse group representing millions of Americans, you have to have a consortium that big.

Peter: But, I imagine, it's got to hard managing that, right, because you've got the fintechs who like to move fast, who have a pretty clear idea of where they're going, you've got the banks who are very concerned about staying on the right side of the regulators and they'd like to move slowly then you've got the consumer groups who have might have a completely different perspective. How do you kind of manage the tensions between those three groups?

Don: Believe it or don't, one, lending like to solve problems together and we know if we don't solve it together…governments, unfortunately, they get involved in technologies, they're not known for picking really great technologies, you know, that's just one of those things. But two, that balance, and we have our leadership, whether chairing the committees, work forces, task forces, always have an FI and a non-FI, it's co-chaired, co-lead and the natural friction gives us a certain amount of energy, believe it or don't, it's actually a good thing, we have that balance.

We require two thirds majority on anything which means we have to have consensus, but it helps weed out extreme positions because we can only have central positions, we can only have common elements and that's been really useful to establish trust amongst all the players. Hey, you know, we follow this process at FDX to make sure that we only move where the entire herd wants to move and then no one group gets excluded, and then there's equal opportunity for an effective voice, not just a voice, but actually being able to be persuasive enough, punch way above your weight and we actually do have members who do so. So, I think that's one of the things we've gotten right.

Peter: Okay, that's great to hear. So, I want to ask about OFX, the Open Financial Exchange, it predates you guys considerably, but what it is it and how do you work with it?

Don: Well, it's the OG, Original Gangster, in the space (Peter laughs), OFX merged with us in 2019, although we have a lot of same members that can co-chair that, and there are 7,000 instances of OFX around the world. So, there are a lot of instances, and versions 1.0, 1.1, 1.2 up to 2.2 so there's whole continuum up there. FDX is a success respect, but if you've got a fully depreciated and paid for OFX instance and you're happy with it, you know, no one's going to come make you get rid of it.

Now, the older versions are being started to be deprecated, the 1.01, 1.02 because they are SGML or XML which is an older technology, or they only support ID and password and don't support OOF2 tokenized access, and for security reasons people are migrating off of those simply because they're not as capable. I mean, some of older versions of OFX are 20+ years old and on older tech so you're starting to see those deprecated and just you normally would in due course. But, certainly OFX is certainly viable OFX 2.2 with, you know, a good, strong tokenized access, it's just fine and you can keep that as long as you like. We have a lot more capability in FDX, just like I'm not going to make you let go of your high school mix tape, you can still keep it as long as you like. I hope to make MP4s and Spotify so much better that you want to organically move to it.

Peter: Right, right, got you. And so, how are you keep yours updated, right, because technology is changing all the time and I imagine you want to keep making your API better, tell us how you're kind of handling that.

Don: One, we copy everybody else's homework (Peter laughs) so we talk to our friends in the UK, Australia and Europe and other jurisdictions as well, see what's going on and we have consultant firms who are members of FDX who do business in Brazil, friends who just did the savvy Open Banking Standard and so we're talking to each other constantly about what's going on.

Of course, we're also watching standards by ETF, W3C, the OpenID Foundation keeping an eye on what's coming in on the security off-space, are there any draft specs we need to know about, get ahead of and it's simply just getting together and talking to people, you can stay pretty well abreast of things on behalf of our members. Luckily, our members don't have to be an expert in all those areas, they can come to us and say okay, what's the news, okay, here are the headlines, okay, cool, let us know.

Peter: So, do you guys have engineers on staff or are you taking engineers from your member companies to create this?

Don: It's total volunteer effort. We have nine employees, so this is the ultimate Tom Sawyer gig, our members do all the heavy lifting, it's their spec. We facilitate the calls, we do certainly the media outreach and go speak at conferences and help them where we can, but this is their spec. They wrote it, they designed it, they vote on it, and we're here to facilitate. But I'll tell you the advantages we have over other markets. No taxpayer dollars were harmed in the making of this spec.

Peter: (laughs) Right.

Don: We're not dependent on a change in election cycle, changing the regulator. So, think about it, if you're about to commit and lend $20, 50, 100 Million to Open Finance, you want a spec that's going to consistent and not worried about the vagaries of election and government changeovers, not dependent on tax dollars and budgeting fights. We're something that's going to be consistent and self-funded year over year over year. I know where I would spend my money, remember, I'm a CPA.

Peter: (laughs) Right, right, got you, okay. Let's close with, I'd love to get your vision really for the future of Open Finance, what's it going to look like and what barriers need to be overcome to sort of realize that future?

Don: And I'm thrilled that you've mentioned Open Finance almost more so than Open Banking because Open Banking tends to focus just on current accounts, checking/savings, credit cards, M&A and that's it. Open Finance is anything being scraped today in financial services, but you're starting to see other areas, like, adjacent to it. For example I mentioned payroll because if you think about it, a lending decision. If I can get your balance, can get your statements, your assets, the only piece I don't have is verification of income and employment. If I can put that on a common format, now you really could get a loan, buy a house with two thumb prints.

You look at Corporate Treasury, we can do this for consumers and small businesses, why can't we do this for the vulcanized role of Corporate Treasury? We're seeing fraud APIs, we see fintechs who see pre-fraud before it happens, but didn't have anyone at big bank to talk to and say hey, I'm seeing weird stuff on Emily's account, now they can with FDX. We built that because our members wanted it so we're going to start seeing ancillary capabilities as we move from Open Finance into Open Data, you're going to see utilities, I think, over time.

Our friends in Australia and in Brazil have called us out, Australia talked about five and fives, they're working on telco and utilities, you know, payroll certainly and other areas as well because they want to get the benefits of security and ubiquity for them as well. Brazil has insurance to property and casualty and life built in, I think we'll start seeing expansion to that as well, that's part of your overall wealth package over time so I think you'll see it grow and touch these ancillary areas. I know that's a long answer, I'm really sorry.

Peter: (laughs) That's alright, that's great. That was a really interesting and we'll have to leave it there. Don, thank you so much for coming on the show, just such a fascinating project you have.

Don: Thank you.

Peter: If you like the show, please go ahead and give it a review on the podcast platform of your choice and be sure to tell your friends and colleagues about it.

Anyway on that note, I will sign off. I very much appreciate you listening and I'll catch you next time. Bye.

(music)