



## PODCAST Transcript

### The Fintech Files: Keeping Open Banking Safe and Secure

With George Aliferis, CEO The Fintech Files and John Broxis, SVP Konsentus Group

**George:** We're continuing our investigation into the world of open banking. There's a natural tension between being open and being secure. And I'm delighted to discuss with John Broxis, SVP at Konsentus group, about keeping it secure both for the user and for those that provide data and services through open banking. John, welcome to the FinTech files.

**John:** Thanks very much George pleasure to be here.

**George:** So, we've talked about this tension between a security and openness. Can you tell us a little bit, can you guide us through the first steps of, how does it work with open banking and what are the risks or fraud or other types of risks that are involved in the system?

**John:** Yeah, sure. Open banking is a bit of a paradox in some ways for centuries, the whole point of banks has been about keeping things secure, keeping them secret keeping them locked out, the place you put your treasure and your jewels, or you get the bank to help you transport your money across the mountains.

This is how the beginning of banking started. Now we get into a different world, the digital world of open data, open finance, open banking, and suddenly the banks are expected to open the bank account compelled by the law to open their bank accounts so that citizens, consumers can unlock the power of the data that's held within the banks, the transactional data, the financial data, the balances, the amount, and this is both incredibly exciting and incredibly dangerous, because we all are irritated by the fact that we have to scan and fax or send three copies of our bank statements through to somebody when we make a loan ask for a loan or what we want to prove a credit worthiness, and wouldn't it be nice if we could just click a couple of buttons and get the bank to confirm the fact that there's money in their account or our salary or something, on our request, this is a very nice thing that we want to see open it's usable, it saves a lot of time. It saves a lot of energy.

But when you think about it as well, I don't want everybody knowing, my salary or my transaction history, or how many accounts have gone or where, for a variety of different reasons. So, there's always something a bit of attention here, and a few



years ago, different to what we now call TPPs, these third party providers started coming on the market promising people that - listen you don't have to go through the difficulty of logging onto your banks yourself. We can do this for you. Just give us your password, your username and your password, and we'll log on and we'll collect all that information. We'll aggregate it together and we'll give you a better, faster, cheaper, nicer experience than your boring old bank can give you. Which is great. As long as we're all in a sort of trusted weld but it's very dangerous when the bad eggs come in and the rotten apples get in between you and the bank and that, that username and password that you've given out, probably in breach of your contract with the bank, starts being abused.

And so, the regulators have had this very difficult, very paradoxical game to play, a balancing act of saying how can we open this up to let more people get simpler access so that they can do more things with their data, but at the same time, keep it really, really, really secure, so that no bad elements can get in and that's part of the problem really, one we're still struggling with I think and will be for evermore.

George: Yeah, and you highlight a lot of elements here, which are very interesting from the user point of view, that's called the UX, the ease of accessing the service, which you could see it from the bank point of view as a marketing issue and both the stringent regulation in terms of security and also you have to open. It's not a choice anymore, so I can see there's a lot of tension there. So how did you get into this?

**John:** Well, if we go right back, I was hitchhiking and got picked up by some people who, he worked for a company Logica, which is the computer consulting, and I'd done an Arabic degree and they sent me off to the middle East and I got into payments the payments business for them over there. But that was a while ago that was payments, and I got into clearing systems and I got into The infrastructure that banks need to communicate with each other securely. I ran step two, which is Europe's largest clearing system. We were overseen by the European central bank and had very strong security pressures put on us both to keep systems going, business continuity and to keep fraud out.

And then as PSD2 came along, PSD2 being the regulation that creates open banking in Europe and UK at the time, we understood that the banks would need a certain amount of common infrastructure to make this work, because in the end payments and banking is a collaborative endeavour. It's no point having one bank account on its own, every bank account has to be linked to every other account through payments, otherwise there's no point in having the account. You want the account to pay people as long as it just stores your money, and because we were experts in collaborative systems, we knew the banks would need some level of infrastructure to keep them secure, to keep the frauds fraudsters out, we and a few other people from Konsentus then started getting together to just an understanding that this what was needed was a special sort of building block that would keep this ecosystem safe. And so, we understood this was a directory verification service so



April 2021

that the banks could understand who the bad actors were and who were the good actors, so that the banks could give access to the good actors and give access in a very fast, immediate way so they weren't blocked in any way and ease of openness but could definitively shut out and tell the bad actors in a very quick way as well. And we created the product which now sits to protect the banks who are doing open banking.

**George:** All right and can you just give us a bit of a timeline for that? Because from my understanding open banking really came into effect in September 2019, if I'm correct, although it started quite a bit earlier. So how, when did Konsentus start building the solution that you're offering now?

**John:** Sure. it's true that the live date was in September 2019, but that was 18 months after a piece of legislation came into effect, say January 2018. And that legislation was passed something like three years before that. So, we're back, I don't remember the date exactly, but back in 2015 or so. It was around the times that people realised that these were the rules that were coming, and it wasn't completely clear how they would be applied or what technology would be needed, but it was around these times that the seeds came into the minds of Konsentus and Open Banking Europe and said, yeah, we need to do this.

There's definitely a need, this need for collaborative endeavour. Get everyone together. Build this piece of technology for this very specific purpose, but for other purposes also to help make the environment more secure for open banking, I mean it's been a good few years really. It's only 5 years we've been talking around Konsentus as the company is three years old, but even before that, we've been speaking with the banks and with the TPPs the fintechs, so everyone can understand what's needed and put it out there.

**George:** Sure. That's also why the, it came into effect after such a long period of let's say discussion and building an ecosystem because otherwise it's just a, it sounds a bit from an external point of view as a bit of wishful thinking, make it open, make it make it faster and make it cheaper.

**John:** There's an old of slogans in this world, but when you make it operational reality as I said at the beginning it's both exciting but dangerous as well, it's very powerful.

**George:** Yes. So how does the Konsentus product and solution fit in the open banking landscape? And maybe we can talk about layers that you need between the access and the final application?

**John:** So, the Konsentus Verify software is quite near the front quite near the the outside of the bank. So, typically it's banks, it's not only banks, but I'll just use the banks for the second.



So as the TPP, these third parties are on knocking on the door to get access it's at that point that the verification software kicks in and does a couple of different checks. Firstly using, firstly checking, the eIDAS certificates that these TPPs are presenting to prove who they are.

So, it's being authenticated. I know who you are and then it's a checking. Various regulatory registers to ensure that these TPPs are allowed to do what they say they're allowed to do, because there are a number of different services within open banking. One service allows you to make payments another service allows you to get account information.

Some TPPs have one, some of the other, some of both, so you need to be very sure - who is the person asking for that information and what is that person allowed to do? And Konsentus Verify does that right up front, right at the outside of that journey as the TPP tries to come in and blocks them or allows them there.

So that really is, yeah, it's like the bodyguard or the bouncer on the front door, letting the right people in and stopping the wrong people. And after they're in, then there's more data handling and stuff going on in the background. But that's where Konsentus Verify sits.

**George:** Understood. Yeah. And just to state it clearly, there's a lot of FinTech startups app developers who are now knocking at the bank's door and say, we want to have access. And I guess the more, the whole point is to have a large and recheck of systems. But the more players there are, the trickier it is from the bank's point of view. And the more connections there are, the more monitoring and safeguarding you need to do.

**John:** Absolutely. There's already something like 5,000 banks in Europe, any of which are allowed to play this role themselves. Plus, you've got in Europe and the UK 450 TPPs and that number has pretty much doubled in the last year. Every month we get another handful being added, and this is very much in the scope of open banking. If we widen this out to open finance you can start getting non-regulated players coming in, who have some bilateral arrangement with the bank or part of some other scheme that the bank recognises, but it's not mandated by law. So, we're only at the beginning. Banks have done the minimum that the PSD2 compliance and Konsentus Verify on protecting against that. But as we go forward that ecosystem will get more diverse, more complicated, and the banks will have a more and more, well harder and harder job of checking that access, which is why they need real state of the art technology.

**George:** And what's also distinct, I think it's important to emphasise there's a lot of entrepreneurship, a lot of the innovation coming, happening, in the current era, but



it's quite different in finance or anything really to find this then. Other industries, because other industries, you can be perhaps lean and try to move fast and break things. Whereas in, in the financial sector, you really never want this to happen. So, there's a different layer of safety compared to any other industry.

**John:** Yeah, correct. If we talk about electricity companies, energy utilities, that the type of data there is much less sensitive. There are a couple of industries or perhaps air traffic control of some sort where you really don't want things to go wrong, but you know, banking financial system is right at the heart of our economy and our society, and if there's doubt about who's got access to data or false payments being made, then, trust crumbles very quickly and at the national level, you become vulnerable very quickly. It's a matter of national security. Yes.

**George:** And for this burgeoning open banking system that people are embracing more and more if, it would be, I think devastating if we heard that There were major issues, or something had happened. So, I guess, that's also where you play an important part. Can you tell us how does it, how do people get started using Konsentus and, can you tell a little bit about how your clients use you specifically?

**John:** Yeah, absolutely. We have. If you want to get started now, you just go to the website [www.konsentus.com](http://www.konsentus.com), you can click through to the developer area. You can sign up to the sandbox, you can try it. It's a software as a service system. You don't have to install anything. You don't have to do a complicated integration process. But you set up your systems such that when somebody comes knocking on your door to use your API, you make a very simple call to us handing over the credentials that they're using to prove who they are. And we come back with an answer about, are they who they say they are? And what are they allowed to do? And based on that you can let them in or not. So the integration is super simple. It's a very light footprint within the bank. And by the way, it's not just banks who are using us. It's electronic money institutions, payment institutions, so regulated but smaller players who also need to give access to accounts that they hold virtual wallets or things like that. Yeah, for very light, very light impact integration and very simple to enrol.

**George:** And the sandbox that you offer is for banks to be able to test it out, but without actually facing the third party providers that would build applications on top of it. Is this how it works?

**John:** Yes exactly. So, the banks can test it out, we provide a set of dummy customer profiles that they can test it with some dummy certificates. They could test it with a real third party provider if they wanted, and that would work as well. But yeah, we give them a very quick, because we're coming from a development place because typically this is a digital software kind of revolution. It's very important that we get straight into showing by showing, by doing giving people access, let them have a go and then they can sign up and become a proper customer if they want.



So that integration is very easy that's not an issue at all. It's just probably the harder job is making sure that everybody's aware that they have these, especially the compliance requirements to do something. And secondly the risk requirements, because people are not always clear that there's bad actors out there. They can visit the happy path, and there's a lot of very well-respected TPPs out there who are ready and willing to access the accounts and do what they should. But not everybody has the enthusiasm of all this new open banking open finance, open data and they'll always think about the consequences of, how do we really know that they are regulated?

**George:** Yeah, sure. And that's the key issue, they have to be regulated, and that's the one thing that you check for them across registers?

**John:** Yeah. We checked a few things actually but one of the key ones is that they're regulated and again, there's a lot of half information or false information around this that people are saying you don't really have to check the regulatory status. You can just check the certificate that's enough, which is not, checking the certificate is fine to know who they are, but it doesn't show you that they're actually regulated right now.

There're other registers that exist given by the European authorities who say, 'Oh can't we just use one of them?', no, you can't for various reasons around accuracy, liability, performance, they're not designed for that, they're not complete and you won't find the information you're looking for you need to source that information yourself.

In theory, a bank could do this themselves, but Europe being Europe, the information that has to be checked is so scattered and fragmented in different places, in different countries, there's 31 national locations. Each one may have two or three different registers itself, they're all in different languages a credit institution in Ireland may be different to a credit institution in Lithuania, the words in English are the same, but actually one's regulated in a certain way and one's not. And unless you have this very specific information and you know how to build that directory that you're going to check against, you don't know who you should be letting in and who you shouldn't.

There's quite a lot of edge cases, some quite strange, weird and wonderful ones. I didn't know, before I started this, for example, that banks in the Faroe Islands, which is part of Denmark, part of Denmark but not part of Europe. So, they do have access into Denmark, but not an access into France or Germany for example.

The regulation to them, and you have funny other edge cases around sovereignty, a lot of discussions about Gibraltar at the moment, but quite whether that was in or out and what the legal status of that is. As well as other institutions like post offices, some countries have post offices, which are regulated under a very specific regime.



April 2021

They are allowed to do certain things, they should be allowed in, but are not necessarily in the normal lists and it takes not only a lot of technical capability to deliver this, but we actually speak pretty much every week, we're speaking to a national regulator to check things and to build up that volume of information and understand that everything we're doing is state of the art.

So, it's a real job.

**George:** Yes, that allows us to have a quick look into what's going on behind the scenes. So, if I do understand it's very much a data business where you have to aggregate and also sort out, make it structured data with all this information from many different registers in many different countries and make it easily accessible into one entry point, which is your API.

**John:** Yep, exactly, that's 60% of the job, but bringing all that data together, making it accessible, building all the rules and providing, that's half of that. The other half, I think is less around aggregation, but being extremely performant on the certificate checking that we're doing. Because in Europe we have a regime of certificate issuance that's again, regulated, different to call them QTSPs, Qualified Trusted Service Providers, who are creating these special certificates. So, they used to check these certificates and go back to the revocation list to verify that the certificates are still active and to deliver all of this to a bank in a less than 200 milliseconds.

So that none of this is interrupting that real-time user experience that the customer is getting.

That's the magic.

**George:** So, is Konsentus really, could we say that it's a data company?

**John:** It's data, it's regulatory and it's technology. Yeah.

**George:** So, we understand what's happening in the background and there's a lot happening. Can you tell us a bit more about the types of risks that financial institutions would be exposed to without this security in place?

**John:** Sure. Well, the financial institutions who are using our software have got different risks. If they do, and if they do it. And I say, do it right. And if they do it wrong later, there are different risks going on. The biggest risk that obviously they don't want, is unauthorised payments going out of their customer's accounts.

They don't want the reputational damage of giving their customers transactional sites payroll information, account information to unauthorised people. They don't want that



from a reputational view, and they don't want that from the supervisory point of view, and also from a GDPR point of view, if they're found to be leaking data, to have effectively a data breach, that allows unauthorised access to my data or to your data, to some third party where it should not have gone, then they're liable under these data laws.

But they also have to - any checking they have to do has to be done in a way that does not create obstacles for the TPP that's accessing the account. They can also be, there's also a risk that they actually create obstacles by doing bad checking by wrongly blocking somebody who should get access or by spending too long doing the check and blocking access in just too long, a time. This is why it's not just important to have software. We'll have to have a check-in place to have a good check in place that is really benchmarked and performant enough to be able to do the checks that's needed within those couple of hundred milliseconds such that it doesn't interfere with the normal traffic.

**George:** Understood. So that gives us a very good overview of the challenges and what the Konsentus is providing. Now looking a little bit ahead. What would be your advice for financial institutions that are approaching this open banking world? Are there some key elements that they need to know in order to make the most of it?

**John:** Yeah, I think there's a couple of rules that the banks are finding out as they go. One is, buy it, don't build it. There're often the temptations for banks to start creating a whole monster of bespoke code to try and do something that's actually being done by a lot of other people.

This is where we come in, but other companies as well, you're much better buying the components and assembling them. Don't, don't build your own TPP checking software. Just come and take ours, or fine, one like that. So buy it, don't build it, and second, stay open to new things. Don't see this as a short-term fix. I think a number of banks have taken the view that this is a compliancy project that they had to comply with by a certain date, end of last year. But in fact, this whole phenomenon that's open banking, open finance is moving. It keeps extending and it will keep extending.

And if you don't put future proof solutions in now, you're just going to be throwing it away and starting again, because what you've not put in place is not adequate. Think ahead and try and get some best of breed architecture into the bank.

**George:** I like what you said about buy or rent, not build. Previous guests have said that if financial institutions were airlines, they would probably make their own jets.

**John:** They'd have a go at it yeah, probably.





**George:** Yeah, it's a cultural challenge as well, but I think now people are really understand how to better this approach this. So, thanks very much for this advice. And tell us a bit about what is one of the most exciting things in this space? Are there things in open banking, or FinTech in general?

**John:** I think some of the services that are starting to come out of this now. At the beginning, it was, at the very beginning, people didn't really understand it. And what was the point and why do we need this stuff? And then you start seeing some fairly basic services coming out, account aggregations. So, I can see the balance not just in my own bank, but in two or three banks that I bank with simultaneously, but now you're getting some really innovative solutions coming out: Artificial intelligence, linked cashflow forecasting for small businesses, on the fly sign up with KYC checking to help the user journey when you're applying for loans or financing of something that you're buying.

So, you don't have to stop that and send off paper via some, scanned, PDF mechanism and wait for an answer, three weeks later, it's all starting to get real time. So that's very exciting.

You're also seeing the data that's used in the accounts, starting to be used for insights to help the consumer to try and show them how to, how they perhaps could save money on insurance based on the profile of spending and their account movements.

So, it really is a question of, the thousand letting the thousand flowers, bloom in an environment that's safe, secure, and open. So, we spent a long time getting that safe, secure, and open, and we got there.

Now we're starting to see the benefits coming through of that. And I think the next two years are going to be really exciting. From Konsentus' point of view, actual real usage.

**George:** Yeah, no, that's indeed really exciting to see, just to envision all the possibilities and coming back to your point about the advice for banks, because we're very focused on developers, etc.

That also shows how important it is to not treat it as a piece of regulation that you have to tick the box, but perhaps you have to be really prepared strategically for this to evolve and offer more opportunities as a bank, as the years go by with opportunities and challenges.

**John:** The banks are starting to look at now value-added APIs that go beyond the regulation that maybe they can charge for, they're trying to see how they can play



April 2021

the role of the TPP and actually get information to help their customers. So, it's two-way street.

**George:** Very exciting. And just to finish off a couple of personal and light-hearted questions, please, John. The first one is what would you do if you were to choose a different career path and maybe your story about hitchhiking? Give us a clue, but I'll let you.

**John:** I think if I If I wasn't doing all of this, I'm sure it'd be up a mountain somewhere. I'm a scout leader, so maybe I'd be running some kind of youth education program, outward bounds, getting the kids out of the houses, off their screens and out into the wild enjoying some fresh air.

I think that would be, that'd be a lovely thing to spend my time doing, but yeah, I'd like to do more of that.

**George:** And how very appropriate as I understand there's a sort of lock down or not full lock down in Paris. So, let me ask as well, where, when we can, what would be your ideal holiday destination?

**John:** I've talked about mountains. And you mentioned skiing before we were talking just before the podcast. So yeah, I think places where I can have good, active adventurous, fun, so it could be mountains, it could be seas. I didn't really mind, I don't feel I have to keep getting on an airplane to go to different countries necessarily, as long as I can go to some beautiful landscape place, outdoors and have fun there then that's all good.

**George:** Wonderful, John, thank you very much for your time and your insight. It's been a pleasure talking to you.

**John:** No, thank you very much, George. It's really been fun.

