# Inside FCA Podcast: Using technology to fight financial crime

**NC:** Hello and welcome to the Inside FCA Podcast. I'm Nick Cook, Director of Innovation at the FCA and I'm delighted to be joined today by Jennifer Calvery, Global Head of Financial Crime Threat Mitigation at HSBC, and David Brear, Co-Founder and CEO at 11:FS. Hello.

**JC:** Hello.

**DB:** Hello.

**NC:** We are recording in the midst of our Global AML and Financial Crime TechSprint at the FCA where we are looking at how new technology might be used to shift the dial in terms of AML and financial crime prevention and detection rates. Jennifer, if I can start with you? We all know that firms and other institutions are dedicating significant resource to tackling AML and financial crime yet clearly there's still a lot of room for improvement. What do you think are some of the barriers that need to be overcome in order for us to really make a step forward?

**JC:** Well first of all, thanks for the question, Nick, and thanks for the opportunity to be here today. I think that the first thing we have to do is have a shared understanding of the problem that it is that we're trying to solve and in that respect, I think of it as we need to find more financial crime faster. And then we need to think about, you know, how do we go about doing that and it's probably having a shared understanding and a very detailed understanding of how does crime occur, what do the typologies of crime look like, what kind of techniques would be good at detecting that type of crime and what type of data will help us to perpetrate and use those techniques.

**NC:** That's really helpful. I mean, your experiences, you've been on both sides of the fence, if I can use that phrase, having been a regulator yourself at the US Department of the Treasury before taking on your current role at HSBS. Do you see substantially different challenges for regulators and firms to overcome and, if so, in what way?

**DB:** I'm quite relieved there when you said 'both sides of the fence'. I was, like, 'What crimes did you do before this?' That's good...

**JC** I haven't done that!

**NC:** That's a very helpful clarification!

**DB:** Yeah, I'm glad on the clarification there but...

**JC:** You know, the jobs actually are not that different, they're more alike than they are different. We are both trying to protect the communities in which we live and operate and protect the financial system from financial crime. So we're more alike than different. To the extent that there is a difference, some of it is in the scale of the data that we each have, regulators are certainly still in a big data world but they have less of it, banks are truly, truly inundated with data which is both a challenge but also a great strength because we have the ability to dig deep and know more about what is happening out there.

**NC:** Do you see different challenges in terms of resources and methods to approach the task in hand or is it really just the data that's the big differentiator?

**JC:** No-one ever has enough resources so there's very little difference, quite honestly, between being in government and being in the private sector in that regard. Everybody always feels they need more and the problem is always bigger, you know, you could throw an army of resources at it and you'll still, still have problems out there to solve. Maybe the key difference is that regulators also have the obligation of regulating the very financial institutions with which they're meant to be partnering and so most of the job is about partnering and for a regulator it's about partnering, encouraging regulated industry to go after this shared outcome, protecting communities, protecting the financial system. But a portion of that job is also about ensuring that those same firms are in compliance with the regulations and when they're not, sometimes even having to enforce. So that always makes a partnership a little bit more tricky and certainly undercuts a bit of trust at times and so, yeah, I think the challenges for the system to work and to work together is really folks realising that we are about a shared outcome and building that trust.

**NC:** And David, you're nodding, you seem to be recognising some of this, does this resonate with your experience?

**DB:** Yeah, I think it's – I mean, financial crime is such a broad category of stuff and I think it comes back a lot to – I mean, there's business decisions between the level of experience that you give to consumers and the things that you put in place to protect the business and that is a balancing act, you know. I remember when I was at Lloyd's Banking Group, fraud is a business decision really in terms of what you're doing because the easier you make it to get into things, the easier it's going to be for other people to get into things as well and actually with that in mind, really it's how you manage that process, how do you manage new technologies coming in which reduce the friction of access of services but also to your point actually, the data that you can start to gain access to, to start predicting and preventing issues rather than just resolving them essentially.

**NC:** And we hear a lot about the promise of better use of these big datasets and the application of new technologies to those datasets to improve compliance procedures and effectiveness. What do you think are some of the key enablers that we'll need to focus on as a group in order to be able to leverage and exploit these technologies to the full?

**DB:** Yeah, I think most of it is again it comes back to early warnings. I think the datasets that big organisations have, if we can figure out the best ways of connecting those datasets together, that it doesn't just become an isolated incident but that trends and understanding can be taken from those things, both current in terms of what's happening right now but historically as well in terms of different types of either attacks or impacts that are happening, then, I mean, preventative measures again are always the best way of actually sort of dealing with these things and data should be there for making decisions, you know. Again, to your point, it's being in a situation where you can do something about it rather than just sifting through the wreckage for the black box, as it were.

**JC:** And I couldn't agree more, I think oftentimes we want to jump straight into a technology solution and first we need to start with 'What is the problem we're trying to solve, what exactly does that problem look like?' and we can talk about that in terms of typologies or however we want to describe it, and then, 'What techniques would be effective at finding that typology?' Then you can get into data, then you can talk about technology solutions but we have to be careful not to put the cart before the horse.

**DB:** Yeah, and it's micro and macro, right? You know, in one instance you're talking about preventative measures for, you know, breach attacks for logging into internet banking, the next you're talking about money corridors for, you know, money laundering globally. The things that you need to do with them both are data but it's being able to zoom in and zoom out of that data.

**NC:** And one of the things we've been focused on throughout this event, and indeed we've had conversations with regulators today, is whether the call to action, whether the need to respond has been made clear enough, whether we as a collective group of both industry participants and regulators have grappled with the problem statement enough and have identified that there is a need to move forward and progress things. Do you see that there's a strong enough call to action and a strong enough impetus to change and innovate or is there work to be done in that space?

**JC:** Well, it's interesting as someone who's at a global bank and so we're in more than sixty countries, we kind of get a global view and experience through, you know, working with regulators and partners and law enforcement peers in each country and so there's no one simple answer to that. But there are now enough countries that have come to the recognition across the landscape that what we're doing today is not good enough and that there is a call to action to iterate and be able to find more financial crime faster. And so we have jurisdictions, not least of which this one and not least of which the FCA by hosting this TechSprint which are doing the types of things that will enable us to make that leap forward.

**NC:** I mean, it's one of the things we've been focusing on is this sense that in order to move forward, though, there needs to be more coordinated and I think you used the word, 'partnership'-type efforts. We've latched on to the phrase a bit, 'Taking a network to defeat a criminal network'. We see highly organised crime, laundering through financial markets and yet our responses tend to be somewhat individual, somewhat siloed. How do either of you feel we should collectively go about encouraging collaboration because it's difficult, it's a difficult area to collaborate, it's a difficult area to coordinate – what would you propose are some of the steps that we could take in order to move that forward?

**DB:** I mean, to the point we were saying about before is like actually data, you know, you guys from HSBC are in a situation where being such a big organisation, you are going to be more prone to people seeing a bigger opportunity, so, I mean, the impacts that you will feel and the information that you can share, the data that can be given to other people for that and vice versa from, you know, Barclays or Lloyd's or whoever. You know, actually, the sharing of that data to be an early warning sign to other people who might have yet to feel some of those impacts, we're definitely not at that global level. I think it's one of those things, it's not a single organisational problem, this is an industry problem and a global industry problem that we're not even – we're not even close to fixing, you know? I think, again, there's definitely going to be a fact check on this one but what is it, 1 or 2% of global money laundering that is actually caught? Is that about right? You guys are going to know...

**JC:** I think the numbers I've heard it is 1% of criminal proceeds are confiscated.

**DB:** Okay.

**NC:** I think that's a UN estimate.

**DB:** There you go, I was close enough. But, yeah, like 1% - like, really? So, you know, 99% of criminal proceedings is not being picked up – that's insane. So, you know, this is surely something that is happening, that is impacting countries, not just industries and, yeah, the more we can do about it, the better it will be.

**JC:** In terms of encouraging collaboration and I think it's different what we might think about doing to encourage collaboration versus encourage innovation, so focusing on collaboration – one of the things that I think we've been keen to promote and be a part of is really public private partnerships, so trying to bring together regulators, law enforcement, industry participants, other participants around the table to work on specific problems, whether that's by focusing and just talking typologies or whether that's focusing on a specific crime group and what we can do together to go after this particular problem. It's in the joint problem solving that you get not only the collaboration, you start to build the trust and you start even to sow the seeds for some of the innovation that might come about through that collaboration.

**NC:** It's hard because it's – is this a part of doing business now in a digital age, you know, like, because essentially this isn't something we are going to fix because wherever you move to, the criminals are going to move too, being more advanced and there's this weird sort of arms race of like staying ahead of the criminals and moving... So, actually...

**JC:** The War of the Machines.

**NC:** Exactly, yes, so is this just sort of part of doing business in a digital age, do you think?

**JC:** I guess I am not so optimistic as to think that we'll solve crime...

**DB:** That would be wonderful, wouldn't it?

**JC:** It would be great if we did.

**DB:** Fixed it, done!

**JC:** But I think we can make a real difference in communities and solve crimes and I think if we don't go at it as hard as we can, criminality could grow. So, we have to think of it like that.

**NC:** Do you think there's a strong enough connection, I guess, almost culturally within institutions to recognise that AML and various other financial crime compliance is fundamentally about preventing some pretty heinous activity in society – these are the proceeds of human trafficking, proceeds for terrorist financing, modern slavery and it's these profits that are ultimately being laundered through the system. Do you think in institutions we've got a strong enough link between the societal harm and the activity of kind of AML compliance, if you like?

**JC:** It's hard to answer for every institution...

**NC:** Sure.

**JC:** ...across the board and all the people who work in it. What I would say is I certainly feel like I've seen over the last ten, fifteen years even, within banks, a real maturation and appreciation for that and then you've seen other parts of the regulated financial industry who have been behind and then you see their maturation and there's still other parts that still are probably at the very beginning of that journey. And then within any institution, people are at different levels of their appreciation and I think the work needs to continue to build that very appreciation, that understanding and a shared sense of responsibility around it.

**NC:** Do you see that, David? Do you see from, I guess, a wider societal perspective that people connect AML and, if you like, the underlying predicate crimes that are generating those proceeds?

**DC:** I mean, definitely not from a general public perspective, you know, I don't think there is that – it's like, 'There are bad guys' and it's like 'Ooh', but they don't – people just don't see that on a day-to-day basis. I mean, if they did, they would be bad, bad guys because that would be very obvious. It's like, 'Those guys in the corner are doing money laundering – we should stop that'. So I think to the point of headlines in the newspapers and things that kind of come through, it's sort of a bit of a boogey man that doesn't impact day-to-day people. I think from a business perspective, for sure, because it's such a leak to the bucket, as it were, in terms of the system. So, I think this, again, it comes back to, from my perspective, it's an in to this digital age, banks are technology companies and actually part and parcel of having any network is the sort of intrusive nature of other people straying into it for whatever reason, whether they're bringing in, you know, bruiting access into that or whether they're bringing in money that is unaccountable.

So, you know, part and parcel of becoming a technology company in its truest sense, which I think it's something that financial services is sort of still coming to terms with really, is really being in that situation where, you know, being that technology firm, this is what you need to be doing – like, house security is done in a way that actually protects your interests and your customers' interests – again, it's an evolving line which is really just sort of difficult to keep up with. You only really have to look at the amount of investment big organisations have to make in maintaining their operating structures and their operating cost for technology capability to show that this is a, you know, multi billion pound investment that's being made year in, year out.

**JC:** But it's funny, I talk to folks who have been in banking for a while and they'll say, you know, the culture has always been around protecting customers, protecting their data and having the keys, the keys to the safe was the most sacrosanct responsibility that you had as a banker and it's just now that the keys to the safe are a different thing and those keys are based in technology and aren't anymore the physical keys. So I think the mindset is there, it's just a little bit of a shift of what does that mean in today's world.

**DB:** Yes, it's an interesting one, isn't it, because when, I mean in the good old days of, I mean, maybe not the good old days, that's definitely sort of pointing...

**NC:** The old days at least...

**DB:** But if like let's go Wild West, somebody rocked up with a gun at a branch and took money, the bank was not at blame for that and would have not been, you know, that was like Billy the Kid taking the monies vibe. But in the situation where actually a bank through a gap from a technological perspective is open to some sort of intrusive capability or security failure, then actually now the bank is to blame for those things and it's different, isn't it, you know, you can't in one instance be accusing banks of not having 55 people marching round every branch to protect them, but like I say, it's like an arms race.

So, I think technology has fundamentally shifted responsibility for these things, whether it's from a legality or a regulatory perspective, but it's definitely one from a perception perspective.

**NC:** So, one of the challenges we face at the end of TechSprint is the 'Now what?', the 'How do we move forward?' set of questions, moving from idea to implementation. David, what are your thoughts about how we go about doing that?

**DB:** That's the, you know, trillion pound question. Like, how do start-ups scale effectively in terms of getting out there? I mean, it's really, really difficult because you can have, I think you can have the perfect technological solution but if you cannot convince somebody else to care about the thing you care about, then your business is not a business. For me, bizarrely in many instances, the technology that we're talking about actually doesn't have to be many people or really that sophisticated to bring a different lens on solving these problems but actually being able to work with big organisations to gain access to the datasets to prove your hypothesis about the impact that you can actually have is really, really difficult. But I guess, I mean, that's why you've started this event, right, to sort of bring that to life and bring people together to try and solve these problems.

**JC:** And we're in a really interesting place and I could only imagine from the kind of tech start-up standpoint there are those who are out there trying to take what we do today and make it cheaper and more efficient. And then we've talked about the problem statement, we need to find more financial crime faster, we only confiscate 1% of proceeds globally – that's not about taking what we do and making it cheaper, it's about finding a better way to do what we're trying to do today so we get better.

So first, you need to get start-ups and encourage start-ups to focus on that problem and not the one that's easy to monetise and easy to get investment in, which is make what we do today cheaper and you need everyone across the system, whether it's the start-up, whether it's the bank that's going to invest in the start-up or whether it's the regulator to buy into what is it we're actually trying to do?

Then when we work with start-ups, we're huge, right, we're a huge bank and we can kill a start-up with our scale and their ability to deliver - even if they have a great concept - into a big organisation like ours is quite a challenge so we invest in start-ups as do other peers, so we'll actually take a position, we'll partner them with bigger consultancies and companies that can help them scale, to help them get to that next level but then there's the piece – that's us, a bank encouraging the start-up, how does the regulator encourage the bank or the industry more broadly?

**DB:** I like that, you flipped it on him!

**NC:** It was a rhetorical question, I thought Jennifer's just about to go about answering it.

**JC:** I would love actually to hear your answer! I hope it's about the TechSprint because I do quite frankly brag about what the FCA does to other jurisdictions and say, "I think this is one really good way to encourage it". I like the idea of supportive healthy competition, which is what you get here and the idea of the ongoing support, so winners from last year you're still supporting this year as they continue to try to incubate the ideas and I think that's a great model.

I look at MAS in Singapore as a regulator and, you know, they're doing a couple of things. First of all, they have an incredible culture around innovation just as an agency themselves, they're not afraid to fail and see other players fail when they try things out there and they just get right back up and go at it again and they also put some investment out there, so they put some investment dollars to help drive some of that innovation.

And then the last one that I would mention, I think they do a pretty good job is Mexico, and the Mexican – both the Central Bank and the regulators there, they've had a tough position, they themselves have had to worry about access to the dollar because of concerns about the status of the regulation in that country and banks' ability to manage financial crime and so with that kind of incentive to get things right, they themselves have become very innovative and they've instituted some of the tech solutions first and then forced industry to come along with them. So, a few different approaches to get us there.

**DB:** I think it's, your point that you were making about working with big organisations is, it is this end of technological innovation for a big bank almost the benefits case create themselves, so almost the, you know, justifying a new cool banking system is difficult, justifying, reinforcing your defences from a security or a crime perspective sort of – it's self-fulfilling really, isn't it, which I think is great. I think the problem for a start-up, I think I'm still going through procurement since like 2016 with some company, so like you say, it's like being in that situation where you've got the ways to sort of move from, you know, slow and methodical in the way that you need to be from a bank's perspective but actually being responsive and innovative in the way that you need to, to respond to crime. I mean, if you dialled 999 and somebody came three years later, I mean, that crime ain't going to be a crime anymore.

So being in that situation is difficult and for a big organisation that means actually, from a technological perspective, just working in such a different mode. But it's good to see people are kind of stepping into that because it's the way that we'll actually really address it.

**NC:** In terms of things that we can do to support this, I mean, this event is part of it, we view it as a catalytic, kind of, convening effort bringing people together, sharing the problem, trying to create new connections, new networks between entities across different sectors that may not know each other and trying to encourage further collaboration and development is part of it. Being prepared to highlight areas where we would wish to see progress and where we will support and encourage progress I think is part of it as well – I don't think regulators are always fully honest about where there are issues in the current system and where the outcomes are not at the level that they would like them to be, so I think that's part of it as well, creating the conversation.

I think equally regulators need to do a lot more to deepen their own understanding of modern technologies, advanced analytic methodologies and become active experimenters with those technologies themselves. How else are we going to have meaningful conversations with HSBC and others if we don't have familiarity with the underlying technology? So, that's a really big part of our journey, I think, is deepening our capability and our understanding there.

And then I think we have tried to provide environments for testing and for developing beyond prototypes so our Sandbox and that kind of thing, but we really haven't seen much in the AML and financial crime space in the Sandbox and I think there's a number of reasons for that, one of which is the nervousness of how a firm's going to be treated whilst it's innovating. So it's one thing to say, 'We encourage you to innovate', it's another to say, "We're starting to learn about the innovation" but I'm not sure as a group of regulators we've yet created the environment where you at HSBC or elsewhere feel we can take some risk because the regulator's going to be with us through this process. It's not just a UK issue, that's the other thing, I guess.

**JC:** It's interesting because when the FCA first came with the Sandbox, some of the others first came out with the Sandbox, we thought, 'We want to be the first ones in there because we're already thinking along these lines and innovating – let's get in the Sandbox'. The response, initial response we got is, 'You don't need to be in the Sandbox to do the things you're trying to do because if you're doing it in parallel to your existing systems, if you're not turning anything off, you don't need to be in a Sandbox, you can innovate all you want and it may cause more friction than not doing it.' And likewise, even if you're in a Sandbox, if we were to find some technique that all of a sudden we felt like we were finding crime that we weren't finding through our other controls, we'd still want to act on it, we wouldn't just say, 'Well, we're in a Sandbox, we don't have to do anything'. That's not the right answer either.

So, I think in this area, some of the attributes that companies get from being in a Sandbox just aren't present here and so in some ways are unneeded. Probably the conversation we are all dancing around and need to kind of advance is when are we comfortable saying that we're going to stop a technique that we do today and move to a new technique? And so I think we've very much gotten our heads around well, we're going to be comfortable when we feel that we can find more financial crime faster using this technique versus the old one, even if they don't find exactly the same things.

And that's kind of where our heads are at at the moment and honestly, we don't even feel like the new technique has to be perfect and all of the risk has to be out of that new technique if it's finding more financial crime faster. What we do think it needs to do is pass the 'should we?' test, so certainly it needs to be legal, certainly it needs to be in compliance with the regulations, always pass the test, but then there's an 'even if we can do it, should we do it?' question and so there's some questions around can we explain it, is there bias in here – you know, the kind of ethical questions. We want to satisfy ourselves on those, we want to make sure that it's doing what we want it to do, find more financial crime faster, then we're pretty ready, we think, to say it's time to go to the new thing.

**NC:** And I think one of the things you touched on as well was of course we don't have great effectiveness measures for the current system so what are we comparing these new approaches to I think is a perpetual challenge for all of us and the temptation – and we see it at things like TechSprint is people are pursuing the 100%, people are pursuing the perfection and we have to remind them 'You're starting from a 1% base' and I think we need to have far more in depth conversations about what is the effectiveness measure that we're both going to be judging these new solutions, these new innovations against and how are we making sure that the baseline we're using is fair and is an appropriate baseline to drive forward some of this progress.

**DB:** Measuring improvement and direction in a 3-dimensional model is really, really difficult and that's the thing – this isn't a linear process of like 'We're 2% towards solving the problem'-type thing, it just doesn't work like that and actually every time a big organisation puts something in or slows down from where they're at now, then actually that 1% or that 2% becomes a lot lower in terms of the completion which is just the fundamentals of actually how quickly the world outside of financial services is moving as opposed to the world inside financial services. And this isn't I guess – to make us feel slightly better, this isn't just a financial services problem – I mean, like financial crime affects every industry to some degree and security affects every industry to some degree, so big tech companies are dealing with this in ways that actually within financial services we can really learn from as well.

**NC:** Absolutely, and I think in an era where the advancement in the criminality is driven by the use of fundamentally exponential technologies, the idea that you're going to address that by moving forward in a very cautious linear fashion doesn't seem to stack up, you know? We're in a world where actually standing still is moving backwards...

**DB:** 100%. I think [what's] really difficult as well is that this isn't a fair fight to a certain degree. You know, we're talking like David beating Goliath every day because that's what we're looking at here – some of the most impactful crimes in this space have been like two people in a bedroom really sort of knowing what they're doing from a technological perspective in getting ahead of the curve where security measures might be in web technology or things that have been put in place from an internet banking perspective.

So, I mean, it's just an amazing, impactful thing but I think to your point there, it's like actually whether it's big organisations like yourself or whether it's people like the FCA and then you guys have to do so much to stay ahead of this curve which is, I think, an exciting thing because, I mean, it's probably the best time to be doing your two jobs which is wonderful, so well done, but also being in that space where actually you're continually having to move this stuff forward, continually having to learn, then I think that's quite exciting as well.

**JC:** Yeah, it is fascinating but coming to – I think you started with this point around collaboration and networks fighting against networks. It does come back to that so really getting law enforcement, regulators, industries, getting all the players to share information and go after the problems, we do that quite well when we put our minds to it on a particular bespoke issue of the day and it's really, I think, the challenge and the opportunity here and the thing that's probably the most fascinating is how do you scale that? How do you scale that really great work that, you know, professionals who are at the top of their game are able to do when they come together, how do we now scale that to go across the size of not only the problem but the amount of funds that flow through the financial system on a daily basis because you can't just do it through bespoke efforts – it's got to scale.

**NC:** So clearly there's a lot to be done, you talked about the need to scale the network, David, you talked about levelling up the David and Goliath playing field – this is a long-term endeavour for all of us, no doubt, and a battle that's never finished, one would assume. With that in mind, though, what would you hope to be able to say in, say, let's say a year or two's time if you were looking back on where we are today and to project from here forward – what would you like to be able to say has happened in terms of us nudging this forward, making some meaningful progress over the next couple of years?

**DB:** I'm not sure it's going to happen over the next year but I think to the point of real-time systems should allow alerting and mechanisms for connecting these networks – not just the networks as in big organisation to big organisation but, I mean, the regulators should be more engaged in real time to the systems that are actually being affected, always on fully digital systems, these are the benefits of them. So, the more we can do to connect the dots, the better I think if we've got even a remote chance of fixing this problem.

**JC:** I think I'd be in some ways less ambitious but only because I think it gets to the ambition that you're laying out which, as you mentioned, is probably more than a year ago anyway and so I would step back and say let's make sure we have a shared commitment to what the problem is we're trying to solve and that is that we're trying to find more financial crime faster, and then let's get ourselves comfortable with the idea that means changing from what we do today and we're going to be comfortable changing to a new technique problem and a third technique the next day and another one the day after that. So we're comfortable in a constant state of change, we're comfortable with cloud computing, we're comfortable that we understand how to think about the ethical issues here, we're comfortable that we can govern models and do so in an agile way.

Like, we just have to get ourselves, and I think some of it does come through the learning of these types of events, we just need to get ourselves comfortable with the kind of opportunities we have in front of us and be open to constant change.

**NC:** I absolutely agree, there's a lot for us to get comfortable with, there's a lot for us to work on together but I think really specifying the problem statement and getting some shared clarity around how we're going to break that down and tackle it over the years ahead I think is the key here.

That's all we've got time for in this podcast. Jennifer, David, thank you very much for joining me, appreciate your insights and your thoughts and your commitment and support for the TechSprint event. I'm Nick Cook, thanks for listening.