"Banks have the potential of creating ecosystems, because the technology is there to do it. Whether the culture or the will is there to do it is another matter. But the technology is certainly there to do just that."

MARCH 16, 2020

Creating a Banking Ecosystem

Presenter: Neira Jones

Summary

Nowadays, fraud prevention and cybersecurity go hand-in-hand. In order for financial services to succeed and thoroughly protect themselves, they must adapt and strategize according to open banking regulations. Brian talks with independent cybersecurity advisor Neira Jones about what this means for institutions of all sizes and their competitors.

Transcript

Brian Contos:

Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Neira Jones. Welcome to the podcast, Neira.

Neira Jones:

Oh, thank you very much. I'm delighted to be here.

Brian Contos:

Neira, I'm so excited to have you on the show and I have so many questions to ask you, especially as it relates to cyber for financial services. But I was hoping you could give our listeners a little bit of background about yourself and your journey and what you're doing today and how you got interested in cyber and that sort of thing.

Neira Jones:

Oh, sure. Well, first and foremost have been financial services for the whole of my career, spanning both financial services institution and also technology companies. So, I guess I have been in FinTech for a very long time, even before it was called FinTech. So, I started my career as many of us have done as a programmer. These days are long gone now. So, I do the more interesting stuff not that technology and programming are not interesting, they certainly made me who I am.

Brian Contos:

Well, awesome. Well, again, it's a pleasure to have you here and one of the reasons I wanted to have you on our show is we haven't talked to a lot of people that specialize in FinTech, and I know some new regulations or some regulations that have been existing have recently been updated, and I was wondering if you could give our listeners a little bit of background about what's going on right now.

Neira Jones:

Whoa. Well, for first and foremost, suffice to say that it's so very interesting. And I know some people might find the regulations rather boring. I actually...

Brian Contos:

What? Who thinks that?

Neira Jones:

...I happen to find them extremely interesting and certainly they give a very good picture of what's happening in the world right now. So, more particularly applying to financial services and FinTech. What's been happening in Europe is since last year the advent of the Second Payment Services Directive or PSD2. And that was really a major paradigm shift because what the directive primarily wanted to do, is to promote innovation and competition. Traditionally, the financial services ecosystem is very difficult to penetrate for new entrance and small FinTech companies, what the PSD2 has actually done is actually promote more competition and enable those new entrance to basically be part of that ecosystem, also become regulated because many entities that weren't previously regulated are now regulated, especially in the third party service provider area in terms of payments and payments services.

Neira Jones:

That was really interesting to see develop. Why the regulation is also particularly interesting is because it goes hand in hand with the worldwide phenomenon that is open banking. So, PSD2 came into force last year, in January of last year. In European states, it got enacted into law back then and since then, we've had a lot of controversy. And the controversial elements, so to speak, as far as the regulation is concerned, is the way it's a specified requirement for

what the regulation calls Strong Customer Authentication and also Secure Communications. Now, Secure Communication is probably not the accepted term in the industry although it is determined in the industry, but this essentially relates to the ban on screen scraping, which has affected many young organizations that actually relied on that model.

Brian Contos:

Of course.

Neira Jones:

This is not just... Let me just add that it's not just the PSD2 which applies to Europe, but you well know yourself, Brian, but worldwide and including in the United States and Canada and Asia and so on and so forth, you will have seen lots of regulation either being discussed, being passed in terms of open banking, which goes hand in hand with what we're talking about here.

Brian Contos:

Neira, what exactly is open banking? Just for some of our listeners that might not be familiar with that term.

Neira Jones:

Well, put simply, open banking is allowing third parties to access payments or banking accounts. And this may raise a few eyebrows in terms of accessing data, which is inherently sensitive because it's your financial information. But the rationale behind that is that essentially... let's take a very simple example. I'm sure you're familiar with QuickBooks.

Brian Contos:

Sure.

Neira Jones:

By Intuit. QuickBooks is essentially used by smaller organizations to automate, well, their accounting processes essentially or their tax returns or whatever they need to do. And with open banking, what you can do with a product such as QuickBooks, is have access directly to your banking information so that your tax return or accounting reports can be produced automatically on the back of the actual information without you having to do anything such as downloading it, uploading it, putting it into the appropriate format, and then share with the third party provider to do that.

Neira Jones:

That's one side of things. The regulation calls that specific scenario, an Account Information Service Provider. Now, there are other types of providers that can benefit from open banking and these are called Payment Initiation Service Providers. And they're essentially those providers that would allow you to initiate a payment from a completely different interface. So just for example, the mobile payment platforms where you actually initiate the payment which will directly, eventually connect to your bank accounts. So, that's really interesting. What that has enabled, for example, is such services that have been cropping up everywhere worldwide to consolidate all of your financial accounts onto the one platform. So, therefore, money management platforms, for example, benefit greatly from open banking because now they have access to APIs that enable them to connect to different providers, different banks, different financial institutions so that the consumer themselves can actually see everything in one place.

Brian Contos:

That makes a lot of sense. So, I'm wondering that in having all this interconnection where we're seeing this in healthcare, we're seeing this in retail, we're seeing this in all sorts of other venues and it makes complete sense that the financial services would be embracing this even more. What does this mean now with open banking, with some of these new changes to help foster competition? If I'm a large financial institution or maybe a small up-and-comer, what do these new regulations mean to me from a tactical perspective? What do I need to be doing?

Neira Jones:

To you, the large bank? To you, the FinTech small institution? Or to you as a consumer?

Brian Contos:

The large bank and the smaller institution.

Neira Jones:

Okay. So, to the large banks, it's very interesting because the traditional financial services ecosystem, as I mentioned earlier on, was a closed one. The regulation is now forcing it to open up to third parties and essentially competitors because it's not just opening up to the smaller institution, it's also opening up to other banks. So to banks, it's a bit tricky, it depends on their strategy. So, they can decide to comply to the minimum extent possible, which is essentially providing access to third parties for payment services and just do that. And that's essentially pure compliance and just do the minimum and that is in my opinion, not a viable strategy because it's purely defensive and they're doing district minimum, but they've had to develop some sort of infrastructure.

Neira Jones:

For example, in the UK, the nine largest banks were forced by the regulators to actually develop the Read-Only API and the Read/Write API to enable a third-party providers to access their infrastructure. And that means opening up to the competition, if you look at it in the cold light of day. So, if they just do that, in my opinion, that is actually not sustainable. Now they can choose to do something a bit cleverer, but realizing that they had to make the investment to develop the infrastructure to allow access to payment services, and they've made that infrastructure investment so therefore they could potentially capitalize on the investment they've made and offer other services that are not related to payments. So, that's capitalizing on the infrastructure and I move beyond payments and they offer other financial services that others can have access to and essentially, potentially brings me more revenue by offering new services such as insurance or the bits and pieces that they may want to give wider access to a totally new audience.

Neira Jones:

That's the second strategy but that's also still very much inward-looking because it is providing access to your own infrastructure. There is another strategy which was over and beyond that is for the banks or traditional financial services institution to realize that they have developed access to potential competitors, but because it is regulation, they must realize that their own competitors that basically have financial services accounts also had to provide access. Instead of just looking inwards, they could start looking outwards and say, "Well, I've provided access, so have all the others, so I can now develop my own services on the back of me now being able to provide access to services from my competitors." And you will have seen most of the largest bank set in the UK and elsewhere in Europe, providing those kinds of money management accounts where you can consolidate and see your accounting in one platform provided by the back.

Neira Jones:

And that's a more defensive strategy, I would call it perhaps keeping up with the competition. And that's one step beyond than just looking inwards. Of course the next strategy, and I don't see many banks at all in fact doing that, which is suddenly realize that you have an infrastructure, you have the technology and the resources of being capable of providing much more than just access to other banks, but you could potentially, if you're clever enough to have an aggressive enough digital transformation strategy, become an ecosystem. And what I mean by that is that, imagine for example, if you have a traditional bank and they've realized and they've got the suitable infrastructure to do this, you go on your online banking app. And what is very well known about banks is that they more or less know everything about you. I mean what you do everyday, what you pay for...

Brian Contos:

Oh, sure.

Neira Jones:

...the kind of transaction can actually derive the fact that you go on a holiday or you just bought a car or you do a direct debit to this particular company. They know absolutely everything. So, imagine the scenario for example, where I go on my banking app, and it just so happens that this time of year I go for a mini break at the weekend. And they do know this because obviously I've paid for it and they've known I've done that for many years, I go on the book banking portal and they suddenly say, "Oh, we now have offers with our partner such and such airline for example, our train company offering a deal on this weekend, and by the way, I also have a deal on travel insurance and car hire with my partner and so on and so forth. You can imagine it, you can just go just about anywhere.

Neira Jones:

And what I'm trying to say here is that banks have the potential of creating ecosystems, because the technology is there to do it. Whether the culture or the will is there to do it is another matter. But the technology is certainly there to do just that. I mean we must... We don't have to look far enough to see how this happens. I mean let's look East and let's look to China. If you look at what WeChat is doing, they're doing just that. Everybody lives in the app. They don't ever leave the app. And do everything from there.

Neira Jones:

That's... Unfortunately, I don't see any bank have having reached that digital maturity state, the path perhaps BBVA in Spain who are not completely there, but certainly making good headways in terms of digital transformation. Now, one has to be fair to banks. Banks have been there a very long time and therefore banks are really burdened by legacy infrastructure. And yourself trying to change any kind of legacy environment is extremely complex and long-winded to... By contrast, if you look at FinTechs, they start with a very clean technology stack and therefore they're able to move very fast.

Brian Contos:

Yeah. Well, it seems to me based on the different categories that you laid out or adoption rates that you've got one group that is moving, kicking and screaming. They just don't want to adapt. And then on the polar opposite, you have groups that are aggressively going after this, but then you have this underlying story of, there's so much information, and the more APIs you integrate, the more interconnections, the more information and the richer the Tapestry they can form of your life. Right? And as much information's out there. So, I guess it's a balancing act, right? How quickly do I embrace this? And if I do so from a consumer perspective, what does this mean to me from a privacy perspective? Now that I've got so much interconnection throughout these APIs and now everything's tied into a single platform or app, essentially meaning if that's compromised, a lot of my information's at risk, right?

Neira Jones:

Oh, absolutely. Which is why the Second Payment Services Directive actually is the first, in my opinion, financial services piece of regulation that makes a very big play on security. I mean the PSD2 has whole articles about security and how security should be managed equally in fundamental security principles that the CISOs are very familiar with and to how incident response should be performed and anything in between. It is extremely comprehensive. So, they've seen that coming. Security is a big problem. Going back to what we were saying about the PSD2 and Strong Customer Authentication and the ban on screen scraping is because imagine suddenly you want banks to open up their infrastructure and many of those companies were using screen scraping as a model. And essentially what is screen scraping apart from the fact that it is in breach of banking terms and condition because essentially, in order to allow a third party to do what they need to do via screen scraping, you need to give them your credentials.

Neira Jones:

From a bank's point of view, and I sympathize with that from the bank's point of view, they don't know whether it's you you or whether it's you through a third party because all they see is your credentials. So essentially the PSD2 said, "Either we will develop APIs or we will actually modify the online banking interface so that the third party is able to authenticate themselves as well as the individual who wants to use the service of the third party and essentially authorizing them to do this on their behalf." So, there was a very good reason for the ban on screen scraping and a very good reason for a Strong Customer Authentication because you want to be able to recognize genuine customers through these increasingly digital platforms.

Brian Contos:

Of course. It just... Looking at it from our perspective now with everything else being the same, of course you want to know if it's company A as opposed to user A or user A accessing it through company A. I mean there's just so many different variables and combinations there. But from bank's perspective, we got⋯

Neira Jones:

Absolutely.

Brian Contos:

...to know who you are. So, I would think that this would... this is kind of like table stakes. Well, you've been so close to this for a very long time. You've seen the changes happen. On your wishlist, is there something that you're like, "I really wish FinTech was doing this from security or compliance or privacy perspective. There's some just basic things

that haven't happened yet but need to happen." Are there one or two or three things that are top of mind that you just think they just should have been implemented by them?

Neira Jones:

Well, it's very difficult to generalize because you will see that there are some FinTechs that do this very well at the outset. So, some of them it is not just about developing an MVP quick out to market. And we look at security and privacy afterwards once we've rolled out something and we've got some customer engagement. Some of them do it very well. But on the main, what I would say for the majority of smaller organization that are looking into this, is first of all, look at the basics. And as you know yourself, Brian, it's always... We'll always fail at the basics. So, look at the basics of information security and also look at it in the context of the information you actually collect and try to decide whether it is absolutely necessary for you to collect it.

Neira Jones:

It hits two birds with one stone. One, you will comply with the data minimization principles of many data protection regulation worldwide, but also the less data you have, basically the less risk you have because you're not having it and you're not collecting it. Now, as soon as I have it, you have a responsibility. You have a responsibility in terms of many aspects of protecting it, securing it, retaining it, deleting it, making sure it's accurate and so on and so forth. So, with data comes great responsibility, especially in the era of data privacy regulations. So, let's not forget about the fundamental information security principles of protecting your systems and your networks and your infrastructure and looking at all three aspects of information security, which are essentially people, process and technology. And I would say you're looking at people and processes, is equally important than looking at the technology, because you and I know the technology can always be fixed, the people, that's much more difficult.

Neira Jones:

I'm sure you've seen the various recent reports which more or less are being released every day, it seems, relating to most data breaches will actually originate from a phishing attack. Now if you are able to curb that at the outset, which of course involves technology as well as people and processes, imagine the impact that would make.

Brian Contos:

Well, I think you've made such a great statement about some of the basics. It still surprises me today when I hear about a breach. And the data at rest is not encrypted, the data in transit might be encrypted, the data in use usually is not encrypted, so they're missing, you say, a couple pieces of the puzzle there. So, you just think of the basics. "I've got a bunch of data, boy, better encrypted, I better control access to that data." Even that's not being done sometimes and I think that's hopeful, that's happening less and less. But the other piece of that is stepping back to another point that you mentioned is, what's your strategy around that? Right? Do I need to collect 100 pieces of information to be effective? Or do I only need three? Because if I only need three, then it becomes a lot cheaper to store, when I dispose of it, when I... everything that's wrapped around it becomes less just by sheer factor of volume. Right?

Brian Contos:

Well, now, I think that's very interesting. And what's the future of cybersecurity for FinTech? What's does it look like?

Neira Jones:

I think I would perhaps expand the question, what's the future of cybersecurity in financial services in general not just FinTech.

Brian Contos:

Sure.

Neira Jones:

And I think people have now come to the realization that fraud prevention and cybersecurity are two sides of the same coin. I'll explain what I mean by that. I've been an advocate of this for at least the last 10 years. Because you will find that you have things that are particularly related to fraud prevention. So, for example, any kind of anti-money laundering regulation, any kind of mandates from the curb networks and so on and so forth. So, fraud is part of daily life when you talk about payments and financial services. And you will have found in the early days, let's say decades ago, you will find that the fraud prevention teams in any organization would probably be part of the risk organization and they would be looking at AML then they would be looking at KYC and all those good things.

Brian Contos:

There're former three... In the US we have a lot of former FBI investigators that are on the fraud side and then the security side where all the network security system administration, they were very different and their background was so fast.

Neira Jones:

And that's right. So on the one side you will need that particular organization wanting to understand who their customers or indeed businesses that they do business with are, and they will need to verify them and then they would implement systems to be able to do that and they will deploy identity verification systems to be able to do KYC and so on and so forth. That was on one side of the organization. Now on the other side of the organization you will have the security teams more often than not perhaps reporting to the IT organization, I think that's been traditional to do that, and they would develop or deploy solutions that are related to identity and access management and so on and so forth. At the end of the day, it's all about digital identity. As we become increasingly more digital, digital identity and authentication and verification in the fraud context and in the cybersecurity context are essentially the same thing.

Neira Jones:

And because we are becoming more and more digital, you see those two areas absolutely converging. And recently, certainly over the past couple of months, I've seen very reputable organization expressing that very same idea. And I am very glad because organization will be able to realize economies of scale very rapidly if they look at regulations in a wholistic fashion as opposed to in silos. So, avoiding regulatory silos I would say is extremely important. I mean, I've mentioned identity such as KYC, Strong Customer Authentication, IAM, the use of behavioral analytics and biometrics for such things are common to the Second Payment Services Directive, the Anti Money Laundering Directives coming to the GDPR as well, the General Data Protection Regulation.

Neira Jones:

If you look at other aspects of security, for example, you've got incident response and disclosure. And I know you've heard disclosure laws in the US for a very long time. This is something that is new to us in Europe, so only since the GDPR was implemented last year. But if you look at the Incident Response and what you need to do as far as the principles are concerned, it is the same. The requirements are perhaps different because depending on the regulation is 72 hours or 24 hours or as soon as possible disclosing to the regulatory authorities or to the individuals under certain circumstances. But nevertheless, all of those are coming to PSD2 and GDPR and AML and so on and so forth.

Neira Jones:

And then you've got all the aspects of data security, data privacy, data protection, which are common to all of the regulations I've just mentioned. So, avoiding regulatory silos I guess is probably what I'm trying to express here.

Brian Contos:

Yeah. And I think you've expressed it very well and just going back to the simple idea, and maybe it's a simple idea, it's a little bit harder operationally, but the fraud team and the traditional IT security team working more closely together. And we've seen the same thing with physical security and digital security keeps being put together whereas those biometrics readers and the video cameras and the CCTVs and all the disparate physical security controls have now been digitized in there, now you can integrate them with some of the things you're doing from a traditional cybersecurity perspective. It made sense to integrate the teams. And well, academically it made sense and it's definitely the way it's going.

Brian Contos:

It took a little while to get there. I'm seeing it more and more often now and I think it's just as clear of a value add to your point with the economies of scale to do it with the fraud side as well. Despite their different backgrounds, they're dealing with risk and they just have a different approach, but they can also leverage some of the same tools and training and techniques. So, that's very well stated. Thank you for that.

Neira Jones:

You're welcome.

Brian Contos:

I have one more question I'd like to ask you. And this is something we like to ask everybody on our show. And that's, Neira, who's your favorite superhero or supervillain and why?

Neira Jones:

Oh, my God, Brian. So, you've probably read my bio. So, perhaps this is not going to come as a surprise. My favorite superhero is actually Batman for one reason and one reason only is that, I absolutely want the Batmobile.

Brian Contos:

Well, I do know you are a big fan of automobiles and especially fast cars, and I don't think any are more unique from the Batmobile. So, I think that would have been a good yes. Very cool. Well, thanks so much Neira for being on the show. And again, thanks to all our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts sponsored by Verodin.