

NETEVENTS

GLOBAL PRESS & ANALYST SUMMIT

DRAFT

Security Innovation in the FinTech Sector

Chair: Eric Parizo

Senior Analyst, Enterprise Security, GlobalData

Panellists:

Bharghavan Vaduvur	CEO - OnDot
Robert Schiff	Partner - McKinsey & Company
Ratnendu Mukherjee	SVP of Information Security - Technology Credit Union

Eric Parizo

All right, I think we're ready to go again. Thank you so much for spending some time with us this morning. My name is Eric Parizo. I'm a cybersecurity industry analyst with Global Data and we're going to be talking about financial security in this session. Again, the description for the session is a little wide ranging, so we're going to try to narrow it down to a few specific topics here. Again, our objective here, we're going to be talking about some largely business-related issues, but for this audience, we're going to be trying to put things in perspective of the consumer because again ultimately, we're all consumers at the end of the day, so some of these financial issues will certainly impact all of us.

So just to briefly introduce the panellists, we have BV, who is the CEO of OnDot systems; we have Robert Schiff who is partner with McKinsey & Company; and we have RS Mukherjee, if I've got that pretty close, who is the senior vice president of

information security with Technology Credit Union. So again, thank you for joining us here today.

So first topic, we're going to talk little a bit about the Equifax breach which I'm sure just about everyone here has heard of in recent weeks, a pretty bad looking data breach there that, based on media reports so far, has involved a breach of up to 143 million consumer credit records here in the US and a few hundred thousand people internationally, which we believe is, again, probably the majority of Americans, adult Americans affected by the breach.

So to get things started here, I just wanted to throw it out to the panel, is there anything about this breach incident that is new or different versus other incidents that stands out for any of you and ultimately how bad do we think this will be when it's all said and done?

Ratnendu Mukherjee

So I'll start first. Well as we have seen with the Target breach a few years ago and Home Depot and we have seen how the retail sector has been targeted in the recent past and the healthcare has not been left alone either, so the Equifax breach is not out of the ordinary. It was pretty much known early on that it's not an if, it's a matter of when, when multiple organisations get targeted. So in terms of the uniqueness of the Equifax breach, it's not something new. Now the impact, of course, is far reaching and it has and it will probably stay a little bit longer for the consumers to recuperate from the impacts from the breach.

Robert Schiff

Yeah, maybe just to build on that, I think I realise this isn't a financial services focused audience, that the main activity financial services are doing, especially in the context of payments, is enabling trust. So when something like Equifax happens, it is pretty - it creates a huge amount of distrust and I think because most people won't understand in detail what happened or how it affects them, what it will really do is depress the kinds of financial activities that rely most on trust, where people feel asks the most trust of them. So in general, there is more confidence in making a transaction at a retail point of sale in a store, where you see someone and swipe your own card, than doing it online. There's more trust online in doing something with a large merchant versus a smaller merchant, so likely this impact of this, I would have to guess, would be to at least for a period of time, depress online activity relative to what it would have been and in particular, increase the burden on smaller merchants to create confidence among consumers.

Bharghavan Vaduvur

Yes, so agree with both the points, I just want to add one more dimension. You know, you talked about comparing this with some other retailer breaches. I think one of the key differences breaching a card or a payment instrument versus breaching identity. Breaching identity is a lot more widespread than breaching a card and the solution is a lot more complex because from a retailer's perspective, the job is to conduct commerce,

you have a payment instrument, you can tokenise it, you can obfuscate it. But the whole purpose of the bureau is to capture and consolidate all the information about the individual so that you can do things like KYC and identify individuals' identity. So in this case, if the identity itself is breached, solving the problem becomes much more challenging. So not only the problem more widespread, the solution is that much more complex.

Eric Parizo

Indeed, so what's interesting to me is that the breach itself, I think, as we've covered isn't necessarily that different so far from so many other data breach incidents that have happened out there. But what's interesting to me is that Equifax has been widely criticised so far for not responding effectively in the early days following the breach. It's difficult for effective consumers to find out if they actually were affected, their website didn't work well, their call centres couldn't handle the load, they had a lot of problems there. But on the other side of the coin, being in this industry for a while, no organisation is truly prepared to deal with an incident of that magnitude.

So I'm curious, to the extent that you can, panellists, can you talk a little bit about what's happening around on the inside from the perspective of an organisation like Equifax that is now handling a pretty complex breach investigation? What are some of the struggles there that they're going through?

Ratnendu Mukherjee

Well several, I think the, like I said, is that the impact of the breach is far reaching and it is impacting financial institutions and more importantly, the consumers, because when the consumers are impacted or affected with charges that they have not made, then it ultimately falls on the financial institutions to make them whole again and ultimately reissue cards and then there's an underlying cost with those. So in terms of the processes and stuff, it's a huge impact of financial institutions.

Now to your question, is that the general tendency is that people and all of us tend to think that nothing bad can happen to us and so we don't tend to prepare for the worst and this, I think, was one of the factors that led to the significant amount of the impact that Equifax had and the magnitude of the breach, but had companies or even Equifax taken a proactive approach, then this could have easily been deterred; I'm not saying avoided, but deterred.

Eric Parizo

So last question on Equifax and we'll try to give everyone to ask questions about all our topics as we get to the end and BV, perhaps you could take this one. Equifax is obviously, one of its missions is to help consumers monitor their credit, but in light of this issue, the big question is who's monitoring the monitors, if you will. Are there any good answers to that? Is technology going to help with that at the present and near future?

Bharghavan Vaduvur

Eventually the buck stops with the end user, right? So you monitor the monitor, right? So there is no other way out. So I think the point here is it's one thing, like I said, to breach a retailer or a merchant, it's a totally different thing to breach the bureau. So I think when it comes to that point, what's the last line of defence for the individual? So in fact as our perspective is that the only way out is to give consumers better visibility and it's really security through engagement, right? So if you look at it historically, there's always been a dichotomy between reaching out to the users and giving them too much power versus security, right? But now with new devices enabling always on communication, really higher engagement does driver higher security and I'll talk about that a little bit more in terms of the sort of solutions that we are looking at.

So just as a couple of examples, if you have the ability to block or control your payment cards or payment instruments, your cards, accounts, identity, if you have the ability to put a block on any time your identity is checked into or your credit scores are checked, if you have the visibility and you as an end user have the control, it might not solve the breach, but it can certainly mitigate it. Does that make sense?

Ratnendu Mukherjee

So to your point that is there and who's monitoring the credit bureaus or who's monitoring the monitors, I think what we are missing as a country is a standardisation and enforcement of a data security standard, which many countries in the European continent have been able to establish and been able to enforce. I think with the establishment of data security standard or a national data security standard and be able to enforce that across organisations that handle personally identifiable information, is going to help monitor the monitors.

Eric Parizo

Very good. All right, we'll shift gears a little bit and as an enterprise analyst, I don't get to talk about some of these topics much, so it's exciting for me to get to opine with a group of smart, intelligent folks up here. One of those topics I don't get to talk about much is retail payment security, because there's a lot happening there, worldwide and more recently here in the US there's a transition taking place to EMV or chip and PIN systems where the payment cards themselves have embedded microchips in them that encrypt the payment data with the idea of fostering end-to-end security from the point that a card is presented for payment all the way to the payment processor and ultimately the banks.

However, what's interesting is that not all of those experiences are the same or even working well at all. So maybe to start, Robert, I know this is one of your areas of expertise and banks ultimately are trying to compete on helping retailers provide good payment experiences, maybe you could talk about some of the motivations there and some of the ways those technologies are evolving.

Robert Schiff

Sure. So there are maybe two parts to consider, which are looking at it from a bank's perspective or an issuer's perspective with regard to retail payments. One is what is taking place at the point of sale and how do you differentiate in that context. The other is how you think about security, authentication and the related experiences more broadly and there's a kind of underlying question which is where does being great at those make a difference in terms of how much customers use your credit card versus somebody else's credit card.

I think one of the things, by the way, that's so interesting about payments in banking or credit card use in particular in the context more broadly in banking, is typically people only have one mortgage, you only have one chequing account, but we often have several credit cards and so it's a very different competitive dynamic than you see for other kinds of financial products and services.

At the point of sale, there's no question the transition to EMV has had its challenges. I think we've all waited 10 or 15 seconds in some cases for a transaction to process and I guess it's a - must sound a bit spoiled when we complain about waiting 10 seconds to process a transaction, but I think everyone recognises it's a source of frustrating in this transition. On the other hand, a lot of the most interesting experiences going forward are likely to be associated with Apple Pay or Android Pay or other kinds of NFC-based payments. There is no way retailers in the US make the massive shift towards terminals that enable NFC without EMV.

So I think one takeaway from everything that's happened around EMV is it's been a gift for those trying to push NFC and in some sense, one of the places in the retail payments experiences where banks have a chance to differentiate is how easy they make it to load your card into Apple Pay or Android Pay or Samsung Pay. Because at the end of the day, the EMV experience when you insert your card and you wait 10 or 15 seconds, that is not something that individual issuers control, that has more to do with the networks and the processors. So the point of differentiation, at the point of sales, going to have more to do with the NFC related experiences. I think that's something that BV can talk more about.

The one other piece just to say is I think the bigger source of differentiation is more broadly when it comes to authentication and security and the experiences around that. So we did some work looking at how consumers feel about authentication-related experiences for the top 20 banks across Canada and the US. What we found is there is tremendous differentiation. When we asked about the authentication experience, what it's like to sign in to your account, the experience range on an MPS scale from in the 70s for one issuer, down to the 30s or 40s for the worst issuers and we were surprised to see a pretty high correlation between the authentication experience and overall perception of what it's like to work with a specific banker issuer.

Because at the end of the day, logging into our accounts is one of the things that we do most frequently with any individual bank and it really resonates in terms of what that experience is like and therefore overall perception of the institution. That kind of differentiation is then in turn going to drive different usage levels for individual credit

cards. So if we're thinking about the role that security and authentication play, there's clearly a fraud management consideration, but the experience it's provided also is going to drive real differences in usage and that, at the end of the day, is where the value is for issuers.

Ratnendu Mukherjee

I will echo what Robert said, is it's all about the end user experience and whatever drives experience is going to be the key in leveraging and accelerating adoption, so yes, I echo what Robert said.

Eric Parizo

Just to press you on that point, I'm curious, why was the experience designed that way, if you have any comments, just because I was in a fast food restaurant just the other day at one of the most popular ones in this country and they have a system many other retailers have where they have both the swipe and the dip and you don't know what to do with your card. So you swipe and I don't know if there are any Star Trek fans here, but the machine makes an ah-ah-ah noise, like suddenly there's a warp core breach happening in the device right in front of you and you need to back away. So then you dip your card in and then if you don't take it out right away, it freaks out again on you. Why was this designed this way?

Ratnendu Mukherjee

I don't think I could answer that specific question.

Eric Parizo

You didn't design it, it's not your fault?

Ratnendu Mukherjee

I was not part of the design team.

Eric Parizo

Well I think it needs some improving, certainly we'll work on that. Before we move topics, I want to just touch on - you touched on digital wallets and Apple Pay and Walmart Pay and such, I want to talk about that adoption briefly because interestingly enough, it seemed like it was really going to take the world by storm when it debut here in the US a couple of years ago, but interestingly enough, it has kind of plateaued and in the case of Apple Pay, which is still the leading method of mobile wallets, its use actually declined a little bit as of late. So I'm wondering maybe you can talk about what's going on there and what the future holds in terms of the technology.

Robert Schiff

I think the sort of experience of Apple Pay in usage has been, I guess I would say it is underwhelming to what generalist expectations might have been. I personally consider

it pretty encouraging. There have been so many false starts relation to mobile payments in general, NFC based payments in particular in the US. There are real differences among markets, I'm not an expert on East Asia, but I think the general sense is that, for example, mobile payments usage and NFC based transactions are significantly more common in markets such as Japan or South Korea. So there is a bit of catch up that we're going through.

I think part of it is that what is the kind of value prop and usage, the experience wrapped around NFC based payment. As a rule of thumb, we tend to say that in order to get people to change the way they pay, the new payment mechanism has to be 10 times better than the prior one. My guess is Apple Pay is two or three times better, not 10 times better. But I think it will be possible to imagine experiences, in particular, for example, I think being able to load your payment credentials into a mobile app much more easily with Android Pay or Apple Pay is something that probably is approaching 10x better, typing in your credit card number. So I think we would see higher usage or adoption in those kinds of settings.

The other thing is that the banks themselves have some work to do to make the onboarding experience better. I don't know how many folks in the room have tried to load one of their credit cards into Apple Pay or Android Pay. There are two things that strike me. One is in almost every case it's a pain, it's pretty challenging, you've got to go through several steps, potentially call your institution. The second is there's a surprising amount of difference in what institutions require you to do to authenticate and identify yourself so that you can load your card into one of these wallets. As those things standardise and get easier, I think we will see many more customers trying out these services.

Ratnendu Mukherjee

I will add a comment to what Robert said here. I think you know, there was a little research that I did a couple of months ago for my employer and what I found was that the consumer adoption is purely dependent on an individual perception of what is convenient and what is secure. Let's go back into the past and consider when the payment cards or the plastic cards of course came into the market. The adoption rate was very, very low, but eventually when consumers found the benefit of using the plastic card, it immediately took ground and it just took off. The same thing happened with ACH. If you go back into the history, it took off a very slow start and then when consumers and the financial institutions found the benefit of ACH transactions, it just boomed.

I think the same thing will happen with the mobile wallet and the mobile payments, it's just the confidence of the user or consumer confidence, once the confidence level increases, the adoption will increase and once the adoption increases, obviously there will be more happening.

Eric Parizo

I want to jump ahead just to make sure we have time for audience questions, so my last question to the panel - oh yes, sure.

Bharghavan Vaduvur

So I started off with unless something is ubiquitous, it's very difficult to make it work and as of today, it's still not. That's the obviously point. But of course how do you drive ubiquity, that itself is a similar type of problem. The second one is friction. I think some markets are much more tolerant towards adding friction at the point of sale than others, so there's a reason why it's not chip and PIN, it's chip and signature, everybody knows about that at least was involved in the financial ministry in the US.

Third is I think the non-uniformity of the on-boarding experience, sometimes it just goes through the green part, sometimes when I on-board it goes through a yellow part, there are additional steps, there is no commonality, right? But I was in a conference last week on user experience, some really interesting things and the most interesting part of the conference was when they had a bunch of end users come in and talk to us between tech types as to what consumers really care about. We spent about a day-and-a-half talking about Apple Pay and Android Pay and wallets and whatnot and the key question was, why the hell should I pick up my phone when I already know how to use my card? What additional value do you offer? Really, to some extent, if all you're doing is changing the form factor, it's marginally useful.

So I think here are the key things and by the way, 42 per cent of respondents in the US have said they're not comfortable with using mobile as a payment, internationally it might be different. So I think there are two or three key things that need to happen. Number one, I think there needs to be visible value. As an example, if you're able to do digital issuance, as soon as I get a card or as soon as I get a replacement card, if that populates into my wallet and I don't have to wait to get a card and explicitly do activation, that's a key driver. So in my opinion, number one to drive wallets is digital issuance, instant digital issuance.

The second key thing is tying it to things like rewards. If it's simply a difference one factor, I don't think it works. Those that have worked best are those where either the payment itself has disappeared, like Amazon or Uber or where it's tied with rewards. I think that's the only sort of major long-term driver for changing the form factor.

Eric Parizo

Right and I would argue virtually every technology provider, service provider in that ecosystem has a way to go in terms of providing or proving that value. So briefly, I know we're short on time, so if we could one more time across the panel and BV, if you could kind of lead us off on this one, just to talk a little bit about technology and make sure we cover that ground. Maybe give - and this is a topic near and dear to your heart, I know, but one, maybe each of you, one kind of technology that is new or emerging that's starting to make a difference or has promised to make a difference in the realm of retail financial security.

Bharghavan Vaduvur

So I think the short answer is empower consumers to take control. So if I can control when, where and how my payment instruments are used, where my card is used and I

have instant visibility and if I have control, then I'm more engaged, I use that card more, the collateral benefit for the issuer is [lower].

Robert Schiff

I guess what I would call IoT for financial services and what that looks like is using all the different kinds of data and signals and feedback that customers give to figure out what is enabling good experiences and what is not in a nuanced and real-time way so you can act on it and I think that is real technology that large institutions are starting to implement and you see real return on investment from it.

Ratnendu Mukherjee

From a financial institution perspective, the ultimate is member experience and some of the things that we at Technology Credit Union have been doing and we have plans to do even further, is to analyse and bring in machine learning and leverage the data that we already have on consumers and then be able to predict and even prevent any fraud and even enhance the ultimate experience when it comes to the consumer, ultimately. So yes, in terms of the utilisation and the new buzzword, I think everybody must have heard of machine learning and artificial intelligence, that's the direction that everybody is going and I think this is the natural path for financial institutions to take to enhance member experience.

Eric Parizo

I think that's all the time we have, so BV, Robert and RS, thank you so much for your time. Let's give them a round of applause if you will. Thank you, thank you.

[end]