Adeptra
The art and science of customer contact

fst
FINANCIAL SECTOR TECHNOLOGY

FST Payment Fraud Roundtable

Thursday 29 April 2010

CH Do customers want to do banking by phone? I believe so - not just from my experience in O2 and Vodafone but also the banks. Within the banking community people do their banking via their mobile, even if it's just to receive balances and statements. And updates or movements on an account can help reduce fraud if they are managed correctly. An example is a suspected transaction, so rather than block that transaction, such as a credit card transaction, you could communicate there and then with a customer to verify it is genuine.

JC But you've also got to cater for different audiences with different levels of sophistication. The most basic level is when the phone rings and you have to confirm that you did actually carry out the transaction. That gets to everybody. With something more sophisticated, you're only going to appeal to a proportion of the people who carry mobiles phones.

WC I'd agree. Younger people are comfortable with technology, some older people not.Some banks have got, I think, a card for teenagers where you can get up to ten pounds, but no PIN is required. So great product - too limited or wrong audience. If they'd given my pensioner dad that card he would have loved it.

PB Do you think those audiences can change over time? Because it strikes me that banks are doing a tremendous amount in terms of looking to educate the customers. It seems that banks are focused on interacting with their customers through mobile channels to provide a more robust customer relationship outside of a common call centre.

KP The key is to ensure that the correct contact channel is deployed to effectively engage as many consumers as possible across any portfolio.

MS It does very much depend on the market - compare what's happening in, say, Africa with M-Pesa. There you are moving to a situation where people are using the mobile truly as a payment mechanism in terms of getting their salary paid on their mobile; paying their electricity bills on their mobile, which is not something that I have seen happening here or anywhere else really in Western Europe. I think that reflects the fact that in that particular market there aren't as many banks and there aren't as many easy ways to make payments.

RLB We appear to be seeing a fragmentation of the banking market, with different providers for different things. So with PayPal you can do a small transaction either online or via iPhone. High street banks like Lloyds or Barclays provide lending, deposit accounts and national payments and then international payment companies like Caxton offer overseas transfers. We may find ourselves with just a lot of niche companies all providing one bit, or two bits or three bits of the puzzle, but it's all linked somehow in a payments cloud, so to speak.

MS Do you think that doing that, having that fragmentation, is going to lead to a much greater risk of fraud? Everyone's doing their little bit, whereas before if it was all being done through a bank, the bank would see the patterns.

JC There's a bigger spread of attack because you've got so many different channels - you can go through someone's Oystercard, you can attack from the way they pay through the 'phone, or attack through their debit card or their credit card. You could still, check for fraudulent activity going through the background systems. As you get more methods of payment you get more methods of attack (and more places to monitor).

AD Add the question of mobile payment for example take Vodafone and its Empresa offering: how do we protect our borders from the invasion of these less regulated payment technologies without constricting the deployment of innovation.

Attendees:
Mark Evans - Publishing Director, FST Magazine (Chairman) (ME)
Wil Cunningham - IT Commander Control & Execution Lead, Lloyds Banking Group (WC)
Alex Dhew - Interim Director Payments & Technology, Travelex (AD)
Mark Silverstein - Head of Legal Services, Citibank (MS)
Tim Decker - Head of e-Channels Payments and Cash Management, Europe, HSBC (TD)
Brian Kinch - Head of Customer Account Fraud, Lloyds TSB (BK)
Keir Pritchard - Client Development Manager, Adeptra (KP)
Phil Bader - UK Sales Manager, Adeptra (PB)
Rupert Lee-Browne - Chief Executive, Caxton FX (RLB)
John Cronin - Senior Information Risk Manager, Independent (JC)
Craig Hutchinson - Senior Product Manager, O2 Financial Services (CH)

fst
FINANCIAL SECTOR TECHNOLOGY

Adeptra
The art and science of customer contact

TD Another of the issues is the different password methods various companies are using. On a personal note, I recently registered a credit card online, and I've got a normal password that I use, a good strong password. However, I couldn't use it because they didn't allow you to use punctuation marks, so therefore the next time I come to use this account online I may not be able to remember that password and I'll have to request a new one. Some standardisation could help here.

WC I think flexible technology needs flexible controls. You need the right level of controls for the right product. You don't want to have one-size-fits-all because it just annoys people when a transaction for a tenner stops your account because they don't know where it's coming from, and I'd like a baseline of the rules, rather than one company stopping my card one month when I use the same pattern spend and another company not doing that.

TD My wife has a pay-as-you-go mobile, so she tops it up online with £10. Unfortunately that's one of the most likely attacks by someone who's got your card details. The next time she goes with two trolley loads of shopping the card is stopped because she topped up her phone. That's happened more than once, so why couldn't they learn the first time that this is part of her normal behaviour? Possibly we're securing the wrong thing. We're securing the technology, we're securing the transaction and the payment, when actually what we should be securing is the person.

KP I think that's absolutely right. Many financial institutions are moving to a personal level of fraud monitoring or trying to move in that direction, but the difficulty that all institutions face is getting personal profiles updated at a speed that there is real value and especially as we're talking about more and more people fragmenting their spending patterns across multiple channels and products.. So, an organisation will typically have multiple monitoring tools, each looking at a separate channel. The provision of profiling to cover all spending patterns and channels is not there yet.

PB Some banks are establishing a profile of preferences based on customer input about preferred services, method of contact, and information such as travel plans. If you've got a better customer profile, and you apply this in the right way, it can improve the overall customer experience, for example, by reducing the chance of you having a transaction stopped for suspected fraud.

RLB Is there not an authentification issue here? Rather than having one method of authentication for all your customers, if you had a variety of different styles of authentication, for example, voice biometrics etc. There's a variety of different things that you could introduce, but would the systems allow you to do that and does it increase the risk of fraud because you've got to choose from different systems?

MS That's one of the dangers. If you give people too many choices will they make the wrong choice and then if they do, what do you do about it?

BK I think surely the customer education piece is key; letting people know what the relative risks are. Then you can take a particular risk-based approach to the whole verification protocol. I guess the difficulty is we've seen circumstances where something that is relatively low risk has then been exploited by the fraudsters in order to gain access to something else.

Taking it easy

ME One of the problems seems to be ease. If the customer wants ease we want to give it to them, but surely the customer is concerned with security too?

WC So, why don't we offer the customer to set their own risk profile? I'd set my own at any transactions under £50 I don't care about.

BK I'd say that part of the problem that we've got today is that organisationally we don't really best understand the consumers and also the consumers don't necessarily understand how they can best interface with us in the event that they think they've got a problem. We have the intelligence, but it's difficult to use.

AD Is there an opportunity to create governing body that collects the data? Adopting the credit checking agencies model.

RLB When you're dealing on a global basis, it would be great to have some sort of global regulator.

WC I think that governing bodies don't just mean governance; they actually bring out best practice. I fell into the trap where I did forget my password and I felt like I was being tortured. The difference was that if I'd forgotten my password online I'd get three attempts, but because I was talking to an individual, I got one attempt and then they went on to the next password, to the next password. So I'd like a governing body to say the best industry practice for rules in terms of combating stupid / unworkable process.

TD I think that would be great. I think the trouble is if you came up with a standard approach for those types of security questions then you're playing right into the hands of the fraudsters who can manipulate that.

CH My experience of governing bodies is that it takes two or three years to agree on how they are going to scope the work and take these things forward - I don't know if there are members here, but the Payment Council were trying to come up with a national

Adeptra
The art and science of customer contact

fst
FINANCIAL SECTOR TECHNOLOGY

mobile payment system several years ago, and that drifted in to nothing at the back end of 2008/ early 2009 when banks' attention was....elsewhere!

RLB And there's still the mountainous issue of the customers. Customers don't want any liability and they don't want any hassle - so all they want is that phone call at three in the afternoon to say that somebody's cloned your card, but don't worry, it's all been sorted. More and more we're seeing customers saying "We don't want your security levels - we want it to be as straightforward as possible", which is great for the technologists as it leads to things like voice biometrics.

PB And to demonstrate the impact of giving customers what they want, a Javelin Survey on customer fraud revealed that 17 percent of victims of credit card fraud will change credit card companies; 15 percent of fraud victims on their bank accounts will change their bank. So, given that customer propensity to change as a reaction to a bad fraud experience, you need to factor into your blocking strategy some consideration for the lifetime value of that customer, the impact on your brand and the opportunity cost of lost revenues.

BK I saw an annual survey that refers to where the customers feel the liability sits; so in the event that you've had a fraud problem, whose fault is that? A vast majority of consumers say "Well, actually we think that's the bank's problem. They've got a duty to look after my money. If they haven't done that then naturally we see that as being their problem". The financial industry adds to that viewpoint in terms of advertising that customers will not have any exposure in the event of a fraud. So I think we're raising consumer expectation and then, of course, when something goes awry as often it takes a number of days to produce new financial instruments or to re-set passwords the delivery is lower than expected.

ME One of the truisms is that assistance rapidly becomes a sense of entitlement. If you had a service saying you're liable for anything that goes wrong with your card unless you're registered with XYZ service, I think you'd find people being a lot more careful.

JC Consider the insurance model. If you look at an excess mechanism then you could say to a client, we have this range of authentication methods and various methods of controls. Depending on which option you select (and the resulting level of risk), this will determine your excess in the event of a loss. Then let people chose what suits them (just like an insurance policy excess affects the size of the premium).

AD As always this area is evolving and at the moment this space is in its infancy. As it grows up it will begin to impact at a social level and this will drive users to realise that it is inconvenient to have multiple payment platforms. Seen as an opportunity, this could play into the institutions hands in that you start to say "if you do everything with us they'll be a consistent security model; we'll take care of the risk etc", rather than having it spread out all over a number of providers.

CH Allowing the customer to choose their own method of authentication and then grading them in terms of risk will be challenging. With banks, I have seen the challenge of those that are trying to promote a simple experience with the consumer which is a single sign-on system where you have one set of credentials regardless of what channel you're trying to come in to the bank whether it's mobile, online, face-to-face, IVR or whatever. Security people say they hate that because all the hackers do is target the weakest channel and then they've got your credentials to go on to other channels.

GETTING SECURE

ME If we were trying to build a gold standard, the best practical security, what would you guys think to actually provide? Would you go fairly heavy on biometrics?

BK It would need to be based on the socio-demographics of the community. We talk about the aging population and the fact that biometrics is generally seen as invasive by the ageing population. That's not to say in the fullness of time we won't go down that route, I think we probably will. Many of those sitting around the table have experimented with trials of things on biometrics, but it's about the acceptability to the consumer base and you need to get broad scale acceptance. It's matching the technological development with the consumer acceptance.

CH What is the consistent biometric that you actually want to use, or do you use lots of different ones? Online you cannot use iris but you can potentially use a fingerprint reader if you've got a physical reader attached to your PC or even your mobile phone. Voice biometrics - again you can't do that clearly in areas with any background noise such as an ATM as that interferes with the speech and voice recognition algorithms.

JC People are very wary of biometrics. There is still a perception of the unreliability of biometrics [and privacy concerns]. Clients don't want to get locked out of their own bank account, but they equally don't want somebody who is perhaps a very close member of their family to be allowed access because they share family characteristics. You also get problems with people in certain professions. For example, where they are handling bricks in a kiln, they don't have fingerprints - they're burnt off - so this

fst
FINANCIAL SECTOR TECHNOLOGY

Adeptra
The art and science of customer contact

rules out some forms of biometrics for those individuals.

ME What is the strongest possible security there is?

RLB The aim must be to make accounts as secure as possible, combined with the best possible customer experience at the best possible cost to the institution. With this in mind, it is background data gathered from a variety of different sources, mostly financial, allied with some physical evidence - and the two have got to match up. Ultimately the customer has got to be inconvenienced as little as possible - otherwise they will simply not use the service and move to a provider that makes it easier for them.

CH To me the level of authentication should be against whatever it is you're trying to do. So a balance sent to a verified mobile phone may require no authentication, but to pay a bill, which has been paid before, does require authentication; and to set up a new bill or payee requires even more, just in case a fraudster is attempting to empty an account by transferring to an account they control.

TD I think all the information and data is there to enable this to work, it's just that the technology is trying to catch up with it. For instance, if you look at people's spending patterns; most people don't move very often, they tend to use the same ATMs. Equally, organisations know where a fraud has occurred. They tend to know a particular online site has been compromised and details have been stolen from there so therefore that will be a trigger to suggest that that card is potentially compromised. So whilst all the data is there, we're maybe a little bit away from getting the technology to have the sophistication to be able to catch only the really suspicious transactions.

MS Because banks and other organisations know that if there is a fraud there is a risk that they are going to have to pay out - there is a tendency to be cautious in their approach to fraud monitoring. Yes, banks could be more intuitive in their approach to fraud monitoring; but there has to be an incentive for banks to do this. Banks may avoid being too intuitive because actually if they get it wrong they are going to be liable for it.

PB Can you ever see a point where there is some sort of liability shift, more to the consumer?

MS The difficulty is how does a bank prove fault on the part of the customer? Over time, as the technology improves and the public becomes more and more used to doing business online, there may be a greater willingness for banks, and perhaps legislators, to insist that consumer have more responsibility and liability for fraud .

KP The challenge that organisations are faced with is the balance between the investment required to segment contact methods and strategies as much as possible, and bringing about the best customer experience possible. Does the additional investment make sense?

TD We always need to balance regulatory compliance and risk reduction with the need to do profitable business. We need then to also balance this against the cost of any customer churn as a result of a poor customer experience. Understanding these costs and business drivers is really key.

ME That's a very good point. You have internal barriers to this as well as external, plus the question, if you are a bank, your own priorities. Where does this sit in the priority list? What are you trying to achieve: a huge market share and worry about security later, or are you trying to get a huge share of secure accounts? It's an internal debate.

TD In any discussion like that in a large organisation everyone will probably agree it can be very very complex. Often, there's no one person or department that makes the decision on that, so a consensus view is needed.

HIGH NETS

MS It's striking the balance and saying "Ok - you do need something sophisticated, that's safe and that may make the client happy, but you're actually spending a lot of money doing it." Is it worth doing all that or do you cut it back a bit and say, well, ok, this is a bit of a cheaper option, but it's not quite as happy an experience for the customer, but it will do?

CH Major Banks in the UK still have a large number of customers that are not making them any money. To be honest I think some of them would not be too unhappy to lose these customers due to them having a bad experience, as long as it's the right customers having that bad experience.

WC You're quite happy to lose 20 per cent or 15 per cent of customers, but if you lose the wrong customer that surely hurts in terms of business as opposed to a family account. Lose Fred Gates - who cares - lose Bill Gates - you must care. There must be people who'd say if you are going to be bad for me, you're going to bad for my company and therefore I'll take my company out as well.

KP And most account holders would probably accept this type of experience as normal, whereas the higher net worth consumers will reason "actually, I'm worth more than that and I'll take my business elsewhere". And these are the consumers that will take action to move.

Adeptra
The art and science of customer contact

fst
FINANCIAL SECTOR TECHNOLOGY

ME I'm not sure either the banks or the consumers are always fully understanding of the consequences of this. We're talking about very sophisticated organised crime and, funnily enough, most organised criminals don't file their accounts at Companies House. We don't know exactly what proportion goes where, but there's pretty good evidence that it does filter down in drugs trafficking, people trafficking and terrorism and various things that aren't particularly nice and I do wonder if there's a civic duty on the banks to perhaps tighten their security and convey that message to their consumers.

CH I can remember someone from the Metropolitan Police saying that you had a moral obligation to reduce card fraud because of the things that you've just been saying. I have not seen any moral arguments in any business case that I've seen in a financial organisation. So, whilst everyone else around this table may nod and say "Yes, we all agree with the moral position" and everyone back in the office will all agree, none of us have seen that in a business case? It might unfortunately, be a cynical view, but I think it's valid.

MS But a lot of these issues have been dealt with by all the laws that have come in over the past 20 years, for example the EU Anti Money Laundering Directive. Organisations can say "Well, the law has come in and we're now compliant with the law and doing all that is required of us. That is ticking the box in terms of our social responsibility". I'm not saying that's necessarily right, but that is what someone could say. The law has stepped in and brought in these standards and that's how we're dealing with it, so what else do we need to do?

ME There's a business opportunity there. This is the account; it's very secure and we will ensure your money doesn't go to supporting bad things.

BK It's the regulatory landscape we're having to play in. In some ways that means that what we do from a fraud perspective we need to do faster; and also we need to better share data across organisations, and it's difficult for us to do that sharing of data because we're constrained from a privacy perspective and the limited times we can say "I've got some information here that may be fraudulent"; it's always got to be proven to be absolutely and categorically and legally defensible. Defensible to say this is fraudulent in order to provide it to another organisation, and that's frustrating. It's a challenge for us.

MS At times there is a real tension between data protection and crime/ fraud investigation.

BK We've almost got a proven case if you like, to say, “well if you share data you can get a greater value. If you don't share data, you're going to get a worsening customer experience; a poorer false positive range on your detection, therefore you're likely to allow more fraud; poorer customer experience; loss of lifetime value and all this sort of thing, simply because we haven't shared,” but it's getting that message across and, as big as fraud is, it's actually miniscule in relation to other losses from an organisation. So you credit their losses or other sort of regulatory related exposure that might be out there. It's difficult to get it up the agenda to say, “ok, allow us to share this information; get sort of a central governance to recognise that, we should share this data for these good reasons.”

WC And why do you think the FBI and Interpol share information? To prevent crime.

SUMMARY

PB It has been very useful to understand and share different perspectives from different organisations. Clearly, there are a lot of questions that have got no easy answers. We've heard about the banks' different perspectives on prevention, detection and resolution and also discussed the responsibility of the customer. There is clearly a growing and increasingly complex fraud challenge, but also a sense that sharing information between banks could really make a difference. Combating that fraud threat effectively also needs a response that combines improved customer intelligence with the increasingly sophisticated contact technology available, so the customer feels you are really looking out for them. But should the banks try to make it as easy as possible for the customer and do everything possible to proactively make their experience straightforward and problem free, thereby promoting confidence and perhaps increasing the loyalty of that customer? The technology is there to make that happen. Or should the banks prioritise on actually looking after their own money? You've got to try and find that balance.

JC I think that customers expect their experience to be painless. At the moment it seems to be arbitrary and random whether transactions are permitted or not permitted. There's a lot of pain in getting valid transactions through, but people are very grateful when an invalid transaction is stopped, or if they are called back, even if it is just to check that a valid transaction is OK. It still feels like the brakes of a car that are coming on by themselves at random intervals. What people want to get to is the point where it's like anti-lock braking, it only kicks in when something dangerous is happening, and the rest of the time it's just in the background working quietly and unobtrusively to keep them safe.