ID Verification and Anti-Fraud Strategies Roundtable

FST assembled a panel of experts on identity to discuss the issues involved with identity authentication, trust, and how to deal with credit risk

The discussion started with the most basic questions of all – what are the drivers for better identity authentication? To what extent are they regulatory or internal? Marcus Watzlaff started the debate off by noting that however strong the internal driver, the FSA was always going to be an overriding driver. He pointed out that even given the global financial crisis "the FSA considers ID so important that it is pinpointing ID crime and financial crime as being potentially high up in the order of the list of its priorities".

Stan Matthews took the point forward, noting that whilst compliance must be a major consideration, the act of verifying identity beyond that level was always going to be a commercial decision weighed against the costs of getting it wrong. "Organisations are striving to get more genuine customers, but at the same time they are bound by the FSA regulations and have to go through the KYC [know your customer] process. This is a real challenge because the risk and compliance director will be saying 'I want to be as secure and robust with my identity checking as I possibly can', but the commercial director will be saying 'we also want to get more good customers through the door'."

However, can compliance be more than just a burden? Perhaps there are elements that are aligned to the bigger picture of the organisation's business. Edwin Aldridge picked up the point and placed a different perspective on matters: "Banks, like most companies, would aspire to know quite a bit about their customers. It helps in targeting their products and developing products and typically a bank's account database will have fields for many, many different attributes of a particular customer, so it's not entirely a one-way street. Banks are also rather keen to avoid being defrauded and one way of doing that is for the customers to pretend to be somebody else, so KYC is actually quite a valuable thing."

Is the issue, internally to the banks at any rate, more to do with how they view the 'churn rate' of their customers. If they are passing through, low level and low value, then some organisations might aspire to a basic level of information. However, other organisations might be willing to delve deeper and create far more interaction with their clients. Jonathan Wood endorsed that view, but with a caveat: "There's a follow-on implication for making sure that you acquire and retain clean customers. Particularly in a recession clean customers can go bad; it's not just a one-off task to make sure they're clean when they begin their relationship. We've got to continue to be alert to it because good customers go bad as well and, I suppose, conversely bad ones can become good."

As it stands, Aldridge notes that at least regulation provides a level playing field: "You can afford to do KYC because everyone else has got to do KYC." A view which chimes with Wood: "I think it helps if we're

managing our companies properly. The fact that you're actually doing checks correctly, appropriately and diligently should be the thing of beauty in a competitive market. It shouldn't be seen as a hindrance."

Generally the feeling around the table was that, although regulation could be a burden, it could be a positive driver – if handled properly. Nigel Dickens came up with perhaps the most graphic analogy of the evening: "When a company does KYC processes properly and well it is a business benefit because I can certainly remember doing two separate financial transactions with two separate companies where one was owned and made to feel good about this, and actually really worked well and I got what I wanted out of it – the other felt like they'd had a visit to a proctologist, so I haven't done business with that company since!"

Automatic for the People

The conversation moved on to discuss the role of automation in the process of identification. With significant gains to be made in both the speed and efficiency of identity authentication by greater automation, it was reasonable to ask why so much remains done by hand.

The consensus is that automation is fragmented, sometimes due to the lack of infrastructure, and at other times due to the limitations of the systems. Aldridge was typical in his explanation of this: "There's a real mixture between a manual system and the systematic methods, depending on what country as well. For instance, in India until quite recently I don't think there was an ID de-duplication service available at all. In fact, I think it's only recent legislation that's enabled that and credit-checking in the last two to three years. Some countries don't have systematic addresses – postal addresses – so it's very difficult to do this kind of work automatically everywhere. For more developed countries it can be automated through organisations like Experian using their data, but a lot of it is manual and I think will always be manual."

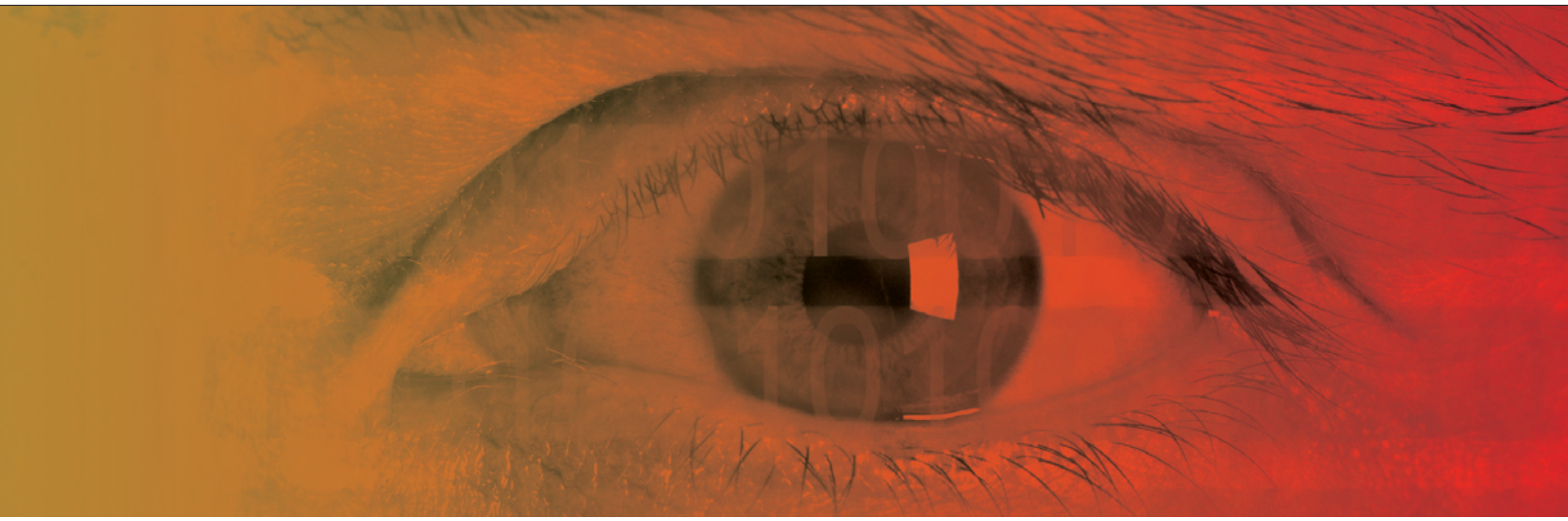
Wood made an incisive point on the matter, in that part of the problem is that there is not a single solution, and that in a many stranded system it is not always easy to define which parts should be automated – or how. "There are lots of people with lots of good ideas and lots of people with lots of good actions, but there isn't a consolidated worldwide approach to this. With so much automation, why are people doing it manually? I think the answer to that is that we are confused about the approach we should be taking with this because there are so many options, and can't work out the parts where automation would provide genuine benefit."

If technology is part of the solution, it can very well be a problem too, as Andrew Cunnington explained: "It's made things more difficult in terms of actually knowing the identity of the person at the other end and also the speed at which fraudulent activities can be committed. Paradoxically we are looking to technology solutions to overcome these same problems." This is a case perhaps of the disease and the cure being one in the same.

There is frustration with the existing methods, with no clear road ahead to create automation and hidden dangers in any solution that achieves this goal. Yet the frustration remains, as Phil

Attendees:

Ian Fish – Information Privacy Expert Panel, BCS (Chairman)
Edwin Aldridge – Information Security Risk Manager, Standard Chartered Bank
James Blake – Head of UK Data Authentication, Experian
Andrew Cunnington – Information Security Officer, Citi
Nigel Dickens – Information Security Officer, BNP Paribas
Stan Matthews – Key Account Manager, Finance Sector, Experian
Marcus Watzlaff – Interim Head of Risk, Old Mutual Asset Management
Phil Welch – Senior Information Security Assurance, Barclays
Jonathan Wood – System Development Manager, Bank of Cyprus UK



Welch pointed out – authentication still isn't perfect: "We are pretty much on a limit to authenticate our customers. We use all the checks that I think you've mentioned and all the relevant databases and there's a limit to what you can do with paper. As yet we haven't designed/focused on one system, but certainly I think that's the way we'll be going in the future."

How widespread is this situation? Watzlaff uses empirical evidence to form a conclusion: "Banks in the London Market are not really happy accepting any ID checks in a reasonably short of space of time and, to me, that indicates that the systems do not have automated solutions." Perhaps now is the time to reconsider the way in which each organisation sees the future, as we are arguably at the bottom of the economic cycle.

Certainly issues will not be getting any easier, and to echo Cunnington's point, technology is a double-edged sword. The problem is that paper is just not robust enough anymore to prove an individual's identity, and one member of the panel found 27 websites where you can buy anything from a driving licence to a foreign passport. These sort of 'Payslips 'R Us' sites offer paper-based identity for small amounts that can be very difficult to detect as a single source of identity. Apparently the going rate is three years' worth of P60s for £45.

Paper cannot alone provide the solution. Matthews notes with electronic identity the data and the resources that are available far outweigh the benefits of looking at paper for identity. "It gives us a better overview – Experian can access a huge database resource of over a billion records to be able to compare what somebody has. We can actually look and compare and have confidence on whether or not somebody is who they say they are. So we can run quite detailed analysis on what those people do and the profile that they have in seconds to give a decision as to whether that person is who they say they are."

Paper might be in decline, and less useful, but perhaps reports of the death of paper are exaggerated, for Matthews explains that with electronic ID authentication there will always be exceptions; instances where certain individuals have a thin footprint from a credit point of view – we could look at new immigrants or a first bank account as examples. Here, there is a need to fall back on paper and ask for a birth certificate, a driving licence or passport.

Organisations need to have a number of processes in place to make it easier for customers to do business with them; and to grant the ability to focus more on the ones that are higher risk.

There is another issue with paper, in that posted documents can take several days to be delivered, and such delays are obstacles in capturing new customers. This goes back again to the commercial aspects when financial organisations are offering services online – offering instant decisions after which prospects will not want to go through an online account opening process which ends with the need to supply by fax, post or e-mail paper proofs of ID. Providers often have a small window of opportunity to capture online applicants, and this is a business decision.

> "Particularly in a recession clean customers can go bad; and, I suppose, conversely bad ones can become good."

Regulation and the Future

We asked where the current trends were taking us, and how our panel saw the future of technology, identity and regulation. Regulation, of course, was to the forefront of the conversation, with predicted future tightening of the rules reigniting the debate over its benefits versus its hindrances.

If the easiest way to ensure that identity is connected to the rightful owner is by up-to-date and correct data, then one solution could be for an agency to take on the responsibilities that are currently undertaken by private companies. As Nigel Dickens called it, "an APACS for identity – or an identity clearing house".

A good solution? Well the panel was unsure, and unsure for several reasons. From Watzlaff, there was the privacy argument – both because of the distaste for large centralised databases, and the issue of privacy laws preventing the transmission of data. There was an equally thorny problem thrown up by Matthews, who has experience in trying to manage such data: "Maintaining the database of those identities is hard, when somebody moves the last thing that somebody will do is change the address on their driving licence because it doesn't have an impact upon their financial status – it's just irrelevant!"

An open question is how it can, or will, adapt. Cunnington sees regulatory compliance today in the finance industry as a one size fits all approach when it comes to identity assurance. He ideally sees a more flexible approach that would link the services and products offered to the level of identity assurance required. In short, to rate the regulation to the risk.

The future might see the rise of new banking competitors, and there are other sectors from which the banks could learn and apply their ideas going forward. The people who in some respects know their customers better than anybody else are the retailers, despite the 'casual' nature of their clients. As Wood notes: "Supermarkets are fantastic at knowing their customers. Perhaps they target them better, and the introduction of loyalty cards was a genius invention and they've proved very effective. They know their customers probably better than most high street banks do."

Dickens looks forward to the possibility of other new entrants: "Telecommunications companies are starting to act like financial services companies. They're heading in that direction. The line is starting to blur. They need to know their customer. They need to validate identities – they've quite a vested interest in that. So that may have an interesting influence on where we go." And Aldridge sees "Telcos will be co-venturing with banks, especially in developing regions."

But will the operational standards of new entrants be compatible – Watzlaff expressed some doubts about the way in which telecommunications companies chase perceived debt. Which brings us, rather neatly, to the concept of trust – so vital in identity. Cunnington notes that: "It still comes down to trust. Who would you trust to authorise and authenticate someone? Financial organisations have had some setbacks there, because at one time, maybe two or three years ago, banks had a degree of trust in each other and I think that post the sub-prime market collapse, a lot of that trust has been eroded and needs to be rebuilt."

The issue might not just be of inter-bank trust. Part of the issue might be technical, in that there is no standard way in which the information can be exchanged – as Dickens puts it: "There's no TCP IP for identity and we do need to come up with that so that if somebody wishes to federate or go through a third party at least we're talking the same language, so the systems will understand the same language and the same set of criteria. That's got to be done first."

Aldridge sees the future a little differently however, stating that: "I think when it comes to financial dealings individual trust is frequently superfluous, particularly between companies where the banks are traditionally a trust third party. I'm put in mind of the Identrus model which is operated by some large financial institutions. You do have an identity for the person or company you are doing business with, but the important thing is the trust relationship with your bank which in turn trusts their bank which in turn knows them. So the trust is not with the counterparty and it's not with their identity. It's that they are all part of the Identrus system and that you trust your bank."

Ian Fish, the evening's chairperson, called time at that point, summing up the conversation as having concluded that there is no one solution, because there is no one fixed problem. However, and to end on an optimistic note, he added that the more and better the data we have, the closer we can get to an effective system.