BAE SYSTEMS

PSD2 reaches beyond EU borders; Open Banking reaches beyond PSD2

Executive summary

Gareth Evans
Senior Fraud and Financial Crime Prevention Consultant at BAE Systems

For the last 18 years, regulation has held the cudgel of prosecution, censure and imprisonment over banks for failing to report or halt illicit transactions and suspect entities. There are sound reasons for doing this, but the general message has been 'don't do' rather than 'do'.

In contrast, global Open Banking initiatives, including the EU's Second Payment Services Directive (PSD2), represent more of a carrot than a stick.

Instead of adding to the list of 'Things Banks Need to Stop Helping Bad People Do', the spirit of Open Banking promises a far more rosy future. Under Open Banking, institutions have a role to play in encouraging innovation – for others and themselves. There's a strong argument for lowering the barriers to entry for third parties, since healthy competition tends to produce more creative solutions to problems, lower the cost of participation for all and end up creating better, more affordable services for wider society. Open Banking is also a fresh, unexplored landscape for fraudsters.

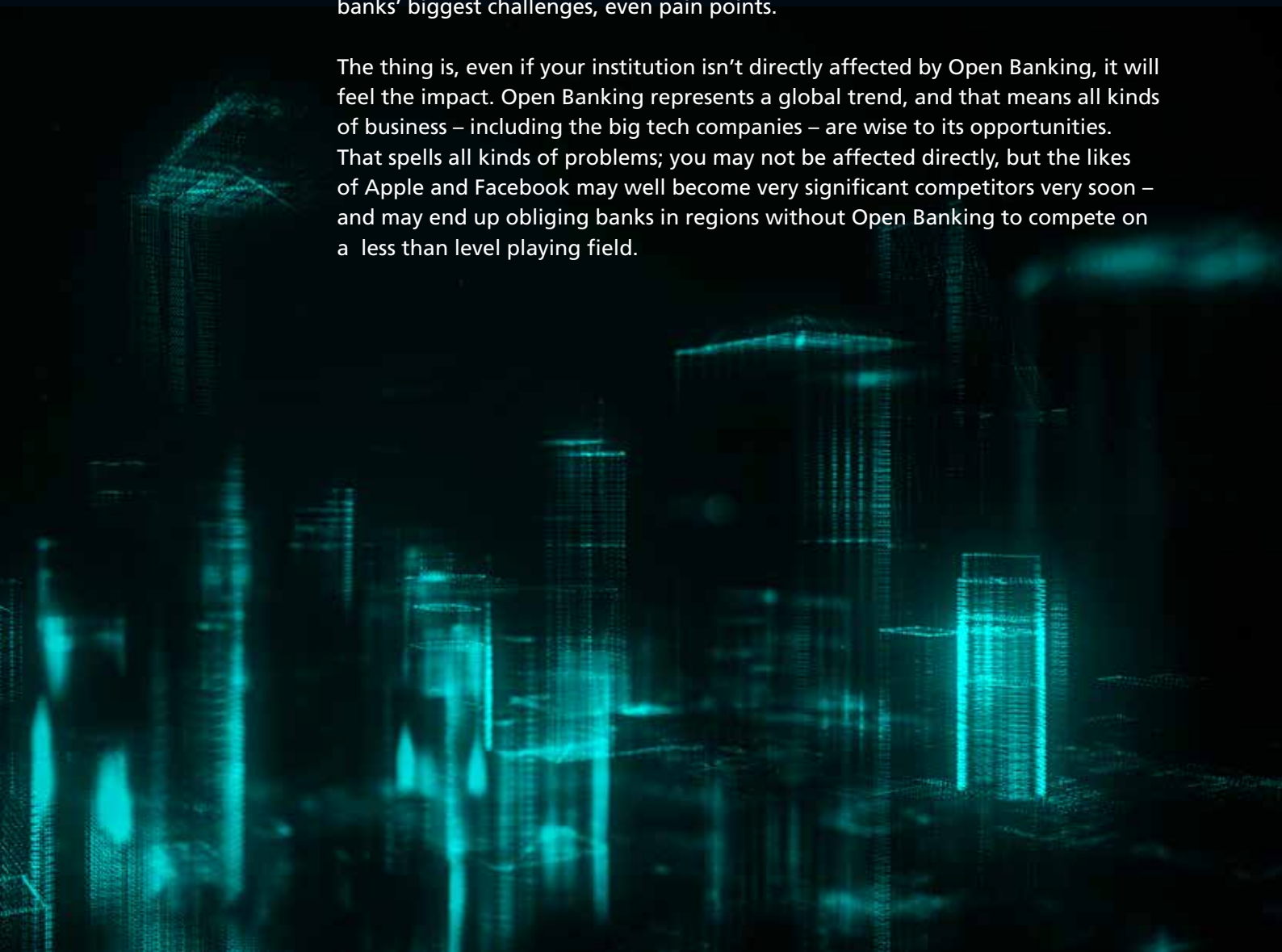
But before we all start weeping into our smartphones, I'll make one point: banks are going to play a very high profile role over the next few years in creating innovation, and helping it happen for other businesses too. Fraud has always been a cost of doing business, and it's important to, rather than getting hung up on the potential risk, work out how to safely avoid the most serious risk and how to position your organisation for some significant success.

Under Open Banking, institutions have a role to play in **encouraging innovation** – for others and themselves.

Accentuate the positive

Let me give you an example; I spoke to a banker in Asia whose organisation already had over 400 Third Party Payment Providers (TPPs) connected to its systems using the bank's own open Application Programming Interfaces – more commonly referred to as APIs. As we've discussed before, direct access like this often bypasses the fraud and compliance safeguards banks place to identify potential wrongdoing early without alerting criminals to their presence. The banker could see probable cyber threats as they emerged from this soup of third parties, but the fraud threat was hard to detect – and many of the banker's existing tools were bypassed by Open Banking. That said, they remained positive about the benefits, which were huge from a business perspective. They were now working with a real variety of types of organisation, from aggregators to internal innovation teams to Fintech incubators – the list goes on. For a global bank the benefits of a worldwide initiative are significant. Yet this opportunity also represents interesting times: Open Banking and open innovation represent many banks' biggest challenges, even pain points.

The thing is, even if your institution isn't directly affected by Open Banking, it will feel the impact. Open Banking represents a global trend, and that means all kinds of business – including the big tech companies – are wise to its opportunities. That spells all kinds of problems; you may not be affected directly, but the likes of Apple and Facebook may well become very significant competitors very soon – and may end up obliging banks in regions without Open Banking to compete on a less than level playing field.



Their innovation at the cost of your reputation?

Let's look at a recent example: ApplePay. As the payment facilitator, Apple got all kinds of kudos from customers; paying for something by tapping your phone on the merchant's Point of Sale (POS) device makes many peoples' day to day transactions about as painless and admin-free as you could possibly hope it to be at this point in our history. Yet ApplePay could be used by fraudsters to manipulate those very same POS transactions – and this had a massive impact on banks. Yet in the eyes of users, this was nothing to do with Apple. The reputational impact lay fair and square on the banks.

The thing with ApplePay was that Apple built it with minimal consultation from banks or industry experts. At launch, While Apple went on about how good the encryption was, and how secure the platform was they did not consider how the technology could be used by criminals to monetise their existing cache of stolen credit and debit card details.

Credit and Debit Card details are easy to steal, however the challenge has always been about how to turn those digits into cold, hard cash. Card Not Present (CNP) fraud has delays built in that make it possible for merchants and banks to spot that something is wrong before the goods arrive in the hands of the buyer. But ApplePay was different; since Apple didn't consider verifying the person entering all those card details into their system was the actual keeper of the card. A criminal with a phone in their hand could add 20, 30, 40 sets of card details and walk out of shops with goods up to the value of $50 every time. Apple took a phone and made it into an auto card device – but the card companies took the hit, because $50 was under the chargeback limit.

The argument as to which side is ultimately responsible is likely to continue[1]; in the mean time, Apple has launched its own credit card in partnership with Goldman Sachs.

When third parties innovate, banks must be incredibly careful to ensure the right controls and checks are in place – or they can end up on the hook for huge volumes of fraud.

---

[1] https://www.forbes.com/sites/thomasbrewster/2019/03/27/millions-are-being-lost-to-apple-pay-fraudwill-apple-card-come-to-the-rescue/#746522c9622f

Not all doom and gloom

There have to be benefits for something this disrupting, and there are. The speed of innovation is boosted. With all kinds of other people designing products, time to market is a fraction of what it once was. Products can be designed, iterated and offered in an incredibly nimble fashion that many banks would struggle to emulate. It's now possible to tailor products to specific demographics and have a third party do the heavy lifting. If your institution is capable of spotting customer personas and identify things they'll pay a premium for, chances are there's someone able to meet that need, and do so very quickly. You might want to cater to the needs of, say, parents of newborn children, particular professions or trades, or just target that lucrative subset of deep sea sport fishermen. Now you can.

Then there's information consolidation. Banks in the UK are offering customers a single dashboard for all of their products – regardless of where they've bought them from. They may have three pensions with three different suppliers, a savings account in one place, credit cards with providers at different ends of the country and insurance with five different carriers – but now, for the very first time, it's possible to log in to a central dashboard and understand the state of your finances at a glance. Even better, you can then work out what needs to go where – and make it happen. This is powerful stuff.

The idea of Open Banking may be to disintermediate banks, but it creates new intermediaries in the process, and they've no access to anti-fraud professionals, and no confidence they can communicate properly with fraud professionals either. All of this innovation, in the meantime, is only possible because of advances in counter-fraud practice and technology. There's a lot to be said for being the facilitator that helps tackle fraud and make the innovation possible in the first place.

Profile

Gareth Evans

Senior Fraud and Financial Crime Prevention Consultant at BAE Systems

Gareth has over 20 years' experience at some of the UK's leading Financial Services organisations and software vendors. Gareth started his career with HSBC, before joining the UK credit card revolution at Bank One International, after many years within the credit card industry focussing on both card payment fraud and application and post application fraud, Gareth moved into application fraud software product development. In 2007, Gareth joined Lloyds Banking Group to implement their non-plastic fraud strategy in time for the UK's Faster payments initiative.

Now at BAE Systems Applied Intelligence, Gareth helps Financial Institutions shape their Fraud Prevention strategies.

How we can help

Proactive White-listing

Build an accurate picture of your customers by identifying and scoring people, places, events and other attributes using machine learning and predictive analytics to uncover how they are connected. By linking atomised behavioural patterns, rather than focusing on individual symptoms, a more reliable and complete profile of actors is dynamically created and continuously updated. These aggregated entities ensure full transparency of a potential criminal action before it becomes a serious problem.

Open Banking / PSD2 Fraud Controls

Uncover and understand new fraud threats by monitoring of Transaction Risk Analysis (TRA) thresholds and rapid adjustment of detection models. In order to lower their average fraud rates and thereby reduce the frequency of Strong Customer Authentication (SCA) checks some payment providers are considering offering incentives to large merchants that have a low-risk profile.

Digital transformation and Data Services

New applications and products are the norm for banks these days – and it's often difficult to identify the route customers take when using an ever-expanding set of products that are increasingly digital-first and face-to-face second. Digital transformation is a never-ending task during periods of evolution, and a key practise for any institution to exercise.

For more information go to: www.baesystems.com/bankinginsights

Contact us

E: learn@baesystems.com
W: baesystems.com/bankinginsights

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com