Authorised Push Payment Fraud (APP) TechSprint (September 2022) video transcript

Jessica Rusu

You know, when we first started talking about APP fraud, one of the things that we learned about it was that fraudsters have scammed consumers, according to the Justice Committee of Parliament, out of over £1.3 billion last year. And we heard from Professor Levi earlier, that 44% of that is consumer banking losses related to APP fraud. So, the size of this is growing and then let's think about what's happened. So, we saw this taking off during the pandemic. This kind of social engineering and push payment fraud materialising and overpassing card payment fraud. But now as we look into the cost-of-living crisis that is now upon us, it's not time to take it easy, right? It's accelerating and consumers will be even more at risk than they were before. And it's not just consumers, it's small businesses and large businesses as well that stand to lose millions, if not billions from fraud.

Team: ReasonUndefined
Delegate 1

We've spent the last couple of days looking at how to infer payment reasons. First, a bit of background. Payments are currently sent blind. There's work being done currently to develop a new API standard to add information into the payment journey to allow firms to detect and prevent fraud payments. It's backed up by an industry proof of concept that demonstrated considerable benefit to the identification of potential APP scams and associated mule accounts. However, it also indicated the biggest gap in the solution and that is firms inability to identify the reason for payment which is a key indicator of fraudulent activity when combined with other data points.

Team: FortyTwo
Delegate 2

What we're going to talk about is spotting fraud at source in terms of receiver verification. OK. So, what we're talking about here today is really around behavioural analytics, behavioural science. And what we want to do is implement nudges and consumer education in order to really try and change behaviour of those mules. And so, we've called that receiver verification.

Team: The APP Trappers
Delegate 3

The flip side of APP scams is that for every APP scam victim, we have a network of ready money mules that are ready to receive the proceeds of fraud and scams. And that's the bit that we think needs more focus if we want to truly solve the problem. So, we believe as part of our solution that we've developed that we need to combine data from between the sending bank and the receiving bank, and our solution focuses on the development of a real-time prepayment risk score to support decisioning.

Team: Annie
Delegate 4

Annie is a network solution. It uses underlying multiparty computation, which is a type of privacy enhancing technology that enables data to be processed without actually being shared. So, what this means in reality is that Yarrow's bank can run their own risk models (define their own risk models) against the beneficiary bank's data. So, things like account type, things like account open date and transaction velocity, etcetera. And get back a risk on that beneficiary but without (and the really key thing here) that data ever going across to Yarrow's bank and ever being seen.

Jessica Rusu

What we're doing here today is shining a light on the systemic issues and this is the point of the TechSprints that we run. So, whether it's focused on fraud or diversity and inclusion or ESG, the point is to use these events to shine the light on these big systemic issues to inform our thinking as a regulator because it's important that we take that outside in focus that ensures that we are diverse, inclusive and innovative in our thinking.