SYNECTICS SOLUTIONS

HAS APP FRAUD AND PAYEE AUTHENTICATION BECOME ONE OF THE MOST PRESSING CHALLENGES IN 2020 FOR FRAUD TEAMS?

Despite all kinds of fraud and financial crime being a consistently growing issue, one particular type of fraud stands out currently as the issue for many in the UK banking industry. Authorised Push Payment (APP) scams and 3rd party payment fraud have become one of these most pressing issues to address in 2020.

The reason that this issue has rapidly risen to the top of the agenda is down to a number of factors, the main one being the publication of the Authorised Push Payment Contingent Reimbursement Model (APP CRM) as a voluntary code of practice - which is being adopted by a large swathe of the banking sector in the hope of avoiding the need for FCA regulation.

Additionally, media, customer and regulatory pressures have also raised the profile of this problem, such that it has risen on the agenda of things that need to have some kind of industry wide consensus for solving.

In fact when one looks at the losses incurred in recent times by APP scams, 2019 the industry saw a staggering £450million of APP fraud. Within that figure a recent report by UK Finance last year also confirmed that £101.1m fell within the remit of the APP CRM, and of this £41.3m was refunded under the code to customers where the Banks were deemed liable.

£450 MILLION

IN APP FRAUD WHERE BANKS WERE DEEMED LIABLE FOR £41.3 MILLION

Given the difficulty in spotting these type of scams financial criminals have been quick to spot this opportunity, which has meant that this type of fraud has seen significant growth in recent years and unless banks can find better ways to address it the likelihood is it will grow exponentially as an issue. In fact in 2019 there was a massive 29% growth in APP fraud, when compared to 2018.

Obviously prior to 2019 the burden of this type of fraud was being borne by the customers, but now with the introduction of APP CRM, the industry is starting to commit to customers being refunded for these APP scam payments, which ultimately leaves banks and other financial institutions liable for the losses.

A deeper look at the model of an APP scam helps us to understand why it's such a difficult problem to spot and prevent.

When a customer is being socially engineered for the purpose of (APP) Scams because genuine customers are merely accessing their own accounts and passing payments to 3rd parties, at the point of inception of the crime, it is pretty much impossible for a Bank to detect the issue of the APP scam taking place. Resulting in an APP claim being received at a later date which banks are now increasingly liable for.

The sophisticated techniques that are employed to socially engineer customers means that no matter how much awareness raising banks try to do they struggle to break the spell which has been cast over the customer by the scammer. This can often be seen in the high value losses the industry is experiencing despite expensive awareness campaigns directed at customers.

Recent anecdotal research from Synectics in this area also points to the fact that the COVID9 pandemic has only exacerbated this issue. APP scammers are feeding off the vulnerability and confusion that the pandemic has created. One recent example of this is as follows:

A Purchase scam – where a scammer has posed as a supplier of face masks. The customer is asked to send the money via an APP to purchase a bulk delivery, as the customer is looking to sell on the product for a profit. However, the face masks never existed and once the customer has sent the funds, the scammer disappears and the customer is left without the product or the money.

IS THERE A SOLUTION TO THE PROBLEM OF APP FRAUD AND PAYEE AUTHENTICATION?

Understandably there is a lot of effort going on across the industry to try and create a framework or set of tools that will help to prevent or at least mitigate this issue.

DELAYING FASTER PAYMENTS

One of the first initiatives to be adopted by banks was to delay the actual transfer for 'first time payee' transfers by 24 hrs to at least give customers a brief period of time to assess if they have been scammed. While this helps, obviously in the vast majority of cases in can be days or weeks before a scam becomes apparent and so this, while welcome, has never been seen to be the solution.

PAY.UK AND CONFORMATION OF PAYEE - COP

Pay.uk, the UK's retail payments authority have created a system called Confirmation of Payee (CoP). This allows the sender of funds from one account to another to check the name on the receiving account, making sure it matches with the name they would expect. Although this has been welcomed by the industry the feeling is that this is one safety net that sophisticated criminals will be able to circumvent fairly easily before too long.

IDENTIFYING VULNERABLE DEMOGRAPHICS AND PUTTING ENHANCED PAYEE DUE DILIGENCE IN PLACE

Given that certain demographics of customer seem to be more prone to falling victim to APP scams, such as the elderly or those suffering with certain health issues, one possible method would be to put greater due diligence around payments and transfers from customers who fall into these risk categories.

Synectics is currently working with the Vulnerability Registration Service on helping those who self-identify as being in a vulnerable group and can then notify banks and other financial institutions of this status. Its early days yet but this type of shared intelligence could become part of a useful set of 'risk flags' that would help banks with their APP due-diligence.

CREATING A 'TRUST SCORE' FOR APP-PAYEE RISK ASSESSMENT/ AUTHENTICATION IS THE ULTIMATE SOLUTION

To deliver a much more thorough resolution to combat the issue of APP fraud, and provide the kind of payee authentication that will really address the issue, we at Synectics think what is really required is a solution that allows a bank processing payments to be in a position to properly risk assess a variety of data points for the recipient account of any payment.

By providing a bank issuing payments with the ability to obtain immediate intelligence on a range of recipient account details, in real-time, prior to transferring funds they will be able to complete a thorough, holistic risk review of the payment prior to transfer of funds.

Furthermore by building up a syndicated intelligence resource of both trusted and 'adverse' payment profiles a trust model could be derived that associates a payee authentication trust score against different combinations of markers.

Ultimately this will allow the issuing bank to complete a fast and holistic review of the transaction which is being processed, when coupling the trust score and any other internal risk markers that are created through the customers logon journey.

Synectics is currently working with a range of intelligence providers and adapting its Data Marketplace as part of its research into delivering the necessary intelligence and syndicated trust framework that could provide such a solution to help banks with APP and Payee Authentication.

Banks or any other financial institution's interested in having a deeper conversation on our research and development in this area should get in touch with our Product Development team and either email us via **ben@synectics-solutions.com** or or call **0333 2343 415**

SYNECTICS SOLUTIONS