Santander

Tackling Authorised Push Payment Fraud

October 2022

Contents

Part 1:

Foreword

Online fraud and scams are now one of the main crimes in the UK, with over £600m stolen in the first half of 2022, according to UK Finance figures published in October 2022. Over half (£360m) was the result of authorised push payment (APP) scams, where criminals trick customers into authorising payments. The Covid-19 pandemic heralded a boom in APP fraud that shows no signs of abating, with fraudsters now exploiting the cost-of-living crisis and creating ever more sophisticated tools and techniques to target their victims online.

With fraud and online scams now posing a serious threat to the customers that we serve and to the integrity of our banking system, we need radical thinking and a new plan of action. Drawing on the experience of the 'Chip and Pin Moment' in the early 2000s which addressed rising levels of card fraud, we believe that there are immediate steps the banking and payments industry can and should take.

This time round though, any such 'Chip and Pin Moment' cannot be delivered by banks and payments providers alone. To truly protect customers there will need to be an alliance across all the sectors that facilitate or use digital interaction, from banks and fintechs to large tech firms, social media companies and telecoms companies. Given the cross-cutting nature of digital technologies, there also needs to be greater leadership, accountability and investment from regulators, policymakers and law enforcement agencies.

Written by Santander's fraud and payments experts, this report sets out how APP fraud has proliferated in the UK before setting out a series of proposals for dealing with the problem.

Summary of recommendations

- Update the payments system to introduce new data sharing standards
- Ensure all payment providers follow a specific set of fraud rules
- Provide a more tailored approach to payments
- Prevent fraudsters from reaching people in the first place
- Greater collaboration between Law Enforcement and Industry
- Provide clear and accountable leadership

[1]Annual Fraud Report 2022_FINAL_.pdf

Part 2:

How we got here: what has driven the recent exponential growth in fraud and scams in the UK?

In 2022 APP fraud is expected to become the most common type of fraud, overtaking card fraud for the first time. Contrary to conventional wisdom, this type of fraud doesn't discriminate by age. Santander's own data from 2021 shows that there was a 175% increase in the volume of purchase scams that originated online among 19-34-year-olds compared to 51–65-year-olds. These frauds are highly sophisticated, and anyone of us could reasonably fall victim to them. There are several reasons why the UK has experienced a particular increase in APP fraud:

An increasingly diverse online shopping and advertising landscape, providing multiple venues for fraudsters to recruit victims

As online technology platforms have expanded, they have created online marketplaces in which consumers can pay other businesses or, in many cases, individuals, via bank transfer rather than by card. These platforms also make it easier for criminals and fraudsters to reach potential victims. Some search engines allow individuals to place adverts on their platform, with little in the way of identity verification.

Santander data shows that over 70% of purchase scams originate on social media (Facebook 54%; Instagram 15%; Snapchat 4%) . Making it harder for fraudsters to target consumers on these platforms will be vital to stop fraudsters at source. Recent Santander research found that 63% of UK consumers believe that technology companies should play a role in reducing volumes of fraud and scams .

In addition to online scams, text and call scams remain at high levels. These were particularly prevalent at the height of the pandemic. With more people now shopping online, more people are receiving deliveries at home, and fraudsters have been adept at mimicking delivery texts to scam customers. UK Finance's 2021 Fraud Report found that telecoms scams have endured even as restrictions have eased . More needs to be done to crack down on fake texts and calls, and the Government needs to work with the telecoms industry to provide fresh impetus to tackle this growing problem.

A complicated investment landscape, with consumers desperate to chase higher returns

After purchase scams, investment scams are the second most common type of fraud. Consumers have chased higher returns in a (up until recently) prolonged low interest rate environment and are now in a period of high inflation. This has coincided with the rise of cryptocurrencies – an under-regulated sector which has opened a door to criminals and fraudsters. Last year, Santander customers reported on average £1 million worth of cryptocurrency scams each month, with the average investment scam totalling almost £13,000[5].

A decentralised payments landscape with no clear leadership on fraud

There has been a huge change in the UK payments landscape in recent years, fuelled by technological innovations, new entrants and the introduction of Open Banking. There is currently no central body operating across this disparate landscape to oversee fraud. Instead, a wide range of bodies are partially responsible for mitigating the risk of fraud and protecting consumers. These include UK Finance, the Lending Standards Board (LSB), the Payment Services Regulator (PSR), Pay.UK and the FCA.

This disparate landscape, without clear system leadership, means that solutions which have been rolled out to date are often patchy, and don't cover all market participants. Confirmation of Payee (CoP) was introduced to prevent mis-directed payments and is now seen as one tool in the fight against APP fraud. Meanwhile the Contingent Reimbursement Model (CRM) Code was created to set out consumer protection standards to reduce APP fraud. Despite both initiatives, fraudsters can still find other points of entry into the system by banking with firms that aren't covered by these schemes.

The lack of hard rules built into the Faster Payments scheme

Faster Payments was successfully launched in 2008 and allows UK consumers to send money directly to other individuals' bank accounts in just a few seconds. In recent years Faster Payments has been heavily targeted by fraudsters, enabling them to drain bank accounts within seconds. 'Authorised Fraud' is a growing concern in a number of other countries. In the USA, Zelle payment fraud is a growing concern, with some recent reports suggesting that $440 million was lost by consumers in 2021. Australia, whose own Faster Payments scheme was introduced in 2018, is similar to the UK's is also now seeing a rise in e-commerce payment fraud[8].

Inconsistent approaches across industry

There are inconsistent approaches to fraud prevention across the industry. The rapid growth of new digital and neobanks poses a challenge, with some choosing not to participate in current voluntary schemes such as the CRM code or CoP. An FCA review found weaknesses in some challenger bank's controls and it is possible that their compliance controls could fail to keep pace with their rapid growth . Sophisticated criminals who look to maximise their opportunity to defraud victims will exploit any opportunities offered and will continually exploit the weakest links in the banking sector.

Case study – Mrs X, 61

Mrs X, 61, fell victim to a friendship scam. After spending over a year playing an online game with another player, Adam*, and building a friendship, Adam manipulated Mrs X, persuading her to transfer him money in order to pay his fictional workers at his company.

Mrs X, who was threatened heavily by Adam, continued to make numerous payments over the course of 18 months. Due to fear of reprisal, Mrs X took out a number of loans and borrowed off friends and family. In total, she transferred over £80,000 to Adam. Throughout the payments being made, Mrs X was told to lie by Adam about the reasons for the payments. She only flagged to Santander that she had been the victim of a scam – and the impact on her mental health - once she started to experience financial hardship. We have since refunded Mrs X in full and have referred her to our specialist customer support team to check on her welfare and support her going forward.

[2] Data source tbc
[2] One Poll, March 2022
[4] Fraud The Facts 2021
[5] https://www.santander.co.uk/about-santander/media-centre/press-releases/santander-cautions-against-crypto-cons
[6] (UK Finance, 2021)
[7] (JP Morgan, 2019)

Part 3:

Recommendations: how does the banking industry introduce a 'Chip and Pin moment' to help tackle fraud and protect UK consumers from online criminals?

Banks and payments firms have dealt with the threat of fraud before. One of the biggest challenges to date was resolved in the early 2000s through the introduction of chip and pin, when this little heralded personal element of everyday banking made it much harder for criminals to defraud customers' cards.

We need the same impetus now. Banks, Payment Service Providers, industry groups, and regulators have the opportunity to work together again to deliver a new 'chip and pin moment' to protect consumers from online fraudsters, focusing not on the management of fraud after it has happened or reimbursement models, but on designs to remove fraud risk in the first place. Mandatory reimbursement is a key first step to protecting consumers should they fall victim the fraud, however we have set out three recommendations that we believe would result in a new 'Chip and Pin' Moment and which would help tip the balance back in the favour of the customer against the criminal.

Recommendation 1: Update the payments system to introduce new data sharing standards

A new system should be designed that puts preventing consumer fraud at its heart. Data should be shared between sending and receiving banks as part of the Faster Payments scheme and before the New Payments Architecture (NPA) is implemented. This would mirror the 'Chip and Pin Moment' that the card industry underwent in the early 2000s, where industry rules and practises were reformed to eliminate fraud.

We must resolve the problem that customers who fall victim to APP fraud think the person they are paying is genuine, and the key to doing this will be data. Push payments capture very little data in the transaction, and the data that is captured is only sent from the sending bank, without full verification by the recipient bank. There needs to be significant changes made to the way PSPs capture the information from a sender, transmit it to the receiving bank, respond to the receiving bank and process the credit to the recipient. There are significant changes on the horizon, including the NPA and new standards (ISO20022) which open sizable opportunities for the industry to ensure fraud prevention mechanisms are embedded by design.

Alongside other banks, Santander UK has been working to develop new data sharing standards to tackle fraud, but there will need to be support from regulators and scheme operators to ensure these are properly designed, implemented and regulated across all PSPs. By adding in extra data captured in any real-time payment transaction, payment providers will be able to work together and be much better equipped to stop fraudulent transactions from occurring, effectively 'designing out' APP fraud from the payments system.

To do this, these additional datapoints would be used to assess the intent behind each payment (see appendix for examples). Information like the type of account (personal or business, type of business, length of time in operation, usual activity, type of product) would enable us and the recipient bank (who would receive data such as payment type and classification) to add all of this to our fraud detection, or even into fraud warnings or CoP journeys.

For example, if a customer tried to send a solicitor firm payment to what is a personal account, these additional datapoints would enable us to identify that the customer isn't paying who they intended to and as a result we could suspend it and prevent the fraud. Equally, we know that mule accounts are often recently opened, using pre-paid cards. Having additional data points on these types of accounts would be extremely helpful to assess intent when they make payments, not having to infer it from sort-code alone.

Additional data points could be included in future designs of the NPA, but given this is still a few years from delivery, we believe there are data points that could be shared already alongside Faster Payments transactions, using processes similar to those developed for Open Banking. By adding in this extra data captured in real-time payment transaction, payment providers will be much better equipped to stop fraudulent transactions from occurring, effectively 'designing out' APP fraud from the payments system.

Recommendation 2: Ensure all payment providers follow a specific set of fraud rules

We should enable consistent monitoring, reporting and oversight at an industry level. Firms that fail to adhere to these industry rules should be made liable for consumer losses.

We need clearer leadership within the payments landscape on fraud to achieve standardisation of fraud controls across all PSPs. At present there is no consistent regulation or legislation that is applicable to all financial institutions in this space, and there is no single body centrally managing this at 'payment system' level in the UK, to bring together the risks, technology and expertise needed to really make a difference and protect consumers from harm.

In an ideal model, every single bank that allows their customer to make or receive 'push payments' should be required to adhere to a set of specific fraud rules:

- Those rules should cover technical designs, policy and how they should process payments to reduce fraud. These must be very specific and consistent, and should be overseen by the scheme centrally, not solely by a regulator;
- That scheme oversight is to maintain consistency, monitoring, oversight, reporting and to enable independent development and monitoring to reduce fraud and design APP fraud away from the network; and
- Non-adherence to those rules should result in their absolute liability for any loss a victim may take. There must be a legal framework in place that removes liability on a bank to manage risks taken by their client in terms of payments to businesses which may not provide goods and services.

Recent proposals from the PSR on requiring reimbursement are welcome and defining a detailed operating model and code of conduct that all payment service providers must comply with is clearly the logical next step. Reimbursement alone however is not a solution, and our approach as an industry must be one of further use of data-sharing, universal standards, and technical innovation to design APP fraud out of the payment system.

We also entirely agree with the PSR that CoP needs to be extended to all market participants to close gaps in which fraudsters are able to operate. Payments without a full CoP match are still allowed, and like the APP CRM, not all PSPs are signed up to it, meaning fraudsters are able to exploit those who are not. The information (whether a CoP match or not) is then not fed into the payment, it is just used by the customer. Finally, there should be consistency of fraud warnings across all PSPs, with best practice and consistency enforced by a central body.

Recommendation 3: Provide a more tailored approach to payments

All transactions don't necessarily need to be treated equally. Industry should consider how it can introduce helpful friction to significant transactions such as house deposits, without impacting low-risk daily payments.

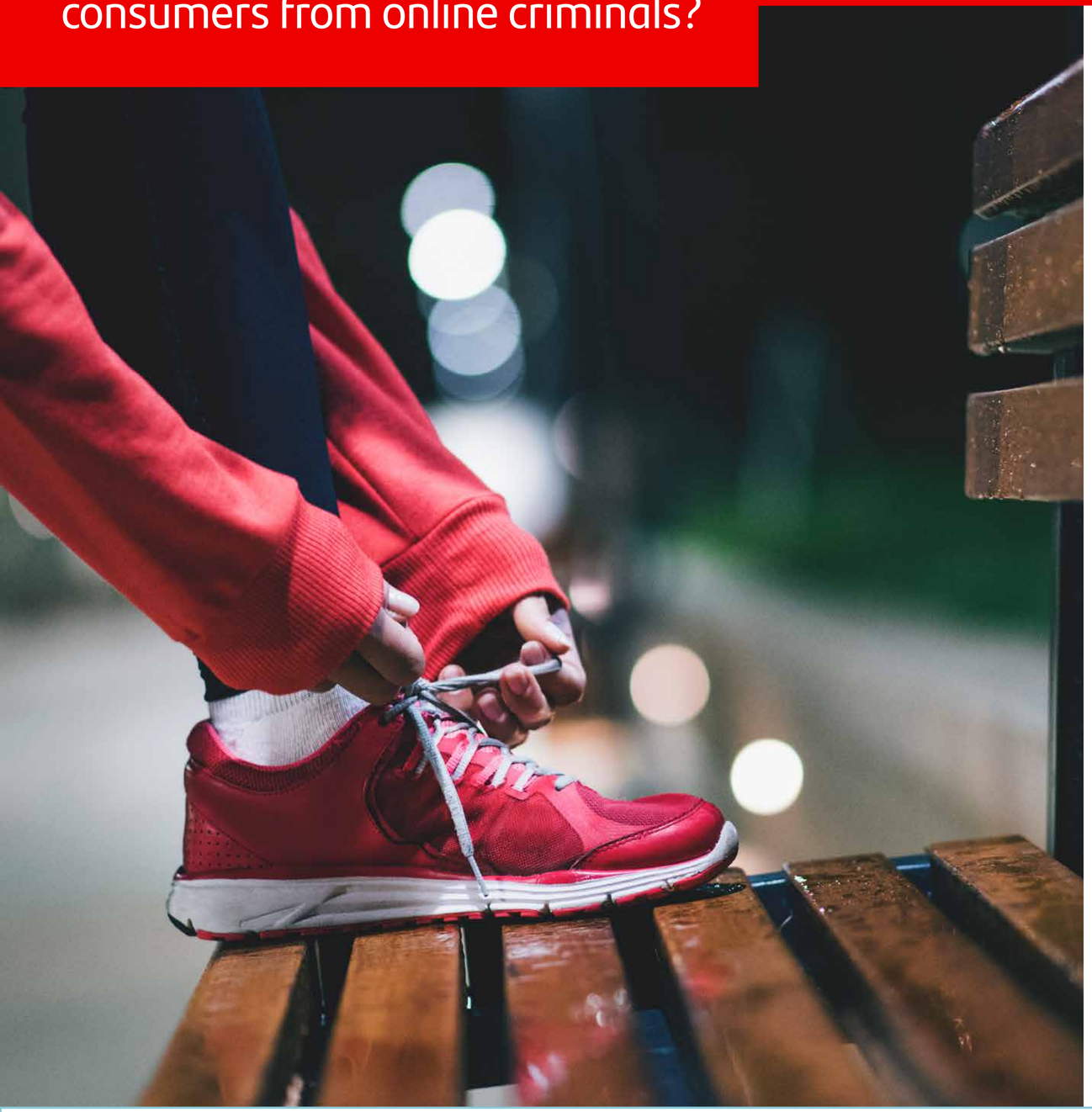
We believe that there should be serious industry discussions about what additional friction could be added into the payment process, including for high value payments, to help prevent fraud. This includes a time delay, which could be used by banks to do additional CoP checks, consult the FCA register and contact the payer independently. Fraud professionals from banks could also use the time to give advice to the customer.

Clearly there is a balance to be struck here, as the speed at which Faster Payments enables consumers to make payments is welcome progress, but there is a case that for higher value payments, consumers may accept the tradeoff that these are slightly slowed down to allow banks to perform additional fraud checks.

> *"We must all act together. Banks, big tech, the Government and law enforcement need to make it our priority to do what we can to support and protect consumers. This is our 'chip and PIN' moment, and we mustn't let it pass us by."*
>
> Dave Lowe, Direct of Fraud ,Santander UK

Part 4:

Recommendations: how can policymakers and non-banks play an active role in tackling fraud and protect UK consumers from online criminals?



While the section above sets out some of the changes that can be made to the payments system to help protect customers from fraud, ultimately there is only so much that banks and the payments sector can do. Tackling APP fraud will require action from other private sector organisations, law enforcement agencies and government. Below we set out three further recommendations in this area:

Recommendation 4: Prevent fraudsters from reaching people in the first place

The most effective way to stop online fraud is to prevent fraudsters from reaching their potential victims in the first place. Fraudsters now target the majority of their potential victims through social media platforms, search engines, or via telecoms channels. Technology and telecoms firms therefore need to do much more to cut fraud off at the source.

Much of the policy debate around fraud has understandably focussed on addressing reimbursement, however, measures which can both reduce victims being targeted in the first place and restrict platforms where fraudsters can recruit victims is also vital.

In recent months, social media companies have made a number of welcome moves to help tackle fraud, with Google providing the FCA with free credits to advertise anti-fraud services, but significantly more needs to be done to close off points of entry for fraudsters. Tightening regulation around fraudulent advertising and content is vitally important, and it is crucial that the Government brings forward the measures proposed in the Online Safety Bill to tackle user-generated and paid for advertising used by fraudsters. If scams continue to originate from vulnerabilities on these platforms, then there should also be a future discussion on bringing them into the reimbursement process.

Given the spate of scams through telecoms channels during the pandemic, Government and regulators need to look at fresh interventions in this area to compel telecoms firms to do more to shut down fake texts and root out criminals using their networks more effectively.

For data sharing, there should be greater encouragement and ability for social media platforms and telecoms firms to provide relevant data to payment providers. This could be aligned to [Recommendation 1] and allow for a much richer dataset for payment firms to spot and ultimately prevent fraud.

Part 4:

Recommendations: how can policymakers and non-banks play an active role in tackling fraud and protect UK consumers from online criminals?

Recommendation 5: Greater collaboration between Law Enforcement and Industry

Given the exponential rise in online crime, law enforcement agencies need to look closely at how they allocate resources to tackling fraud and scams. There is currently no consistency in how fraud is reported to the police by banks, no centralised reporting system to the payment scheme, and there is no centralised bank to police reporting system. It is the responsibility of a customer to report fraud to both Action Fraud, the UK's national reporting centre for fraud and cybercrime, and their bank. Reporting it, however, does not mean that it is investigated. In addition, the key elements of how a scam originated (such as via a false advert or SMS) are rarely investigated, and could be the key element to link many hundreds of cases together across many victims and banks.

Different police forces have varying levels of resources committed to tackling online fraud and there is a significant lack of specialist training available. While dedicated Regional Organised Crime Units (ROCU) have been established to tackle the highly organised criminal gangs that perpetuate APP fraud, there still only a handful across the UK.

For example, recent collaborative projects that have targeted their focus on Investment Fraud have shown that dedicated police resource applied to specific crime types can yield excellent results and intelligence which can be used to further prevent crime; more of this activity should be encouraged and supported. This could be combined with 'real time' recovery action by fraud investigations teams at banks in order to prevent more funds from reaching scammers and showing a united front in the fight against scams.

Recommendation 6: Provide clear and accountable leadership

Responsibility for the environment that facilitates online fraud sits across multiple Government Departments, including HMT, DCMS, and the Home Office. Similarly, there are multiple regulators and industry bodies with partial responsibility, but there is no single body in overall control. Given the increasing frequency of online scams and the impact they have on individuals, a single government committee should be given the power to work cross-department and with industry.

'We stand ready to work with stakeholders across industry and government, and would encourage you to contact Publicpolicy@santander.co.uk to learn more'?

Annex

The below table illustrates some of the additional data points which could be included in future designs of the NPA, but given this is still a few years from delivery, we believe the additional data points should already be shared alongside Faster Payments transactions, using processes similar to those developed for Open Banking:

Payment reason	Personal payments; paying for a service; paying for goods; moving money to your own accounts
Payment Reason Sub-category	More detail on the payment reason e.g. if paying for goods, the sub code could be: buying a car
Payee Name	COP outcome to be included in payment message
Payment stage/ value exchange	Code to indicate if a payment is a refund, goods/ services already received
Recipient account type	Personal or business account
Recipient business second	Business type
Recipient Collection Account Flag	Returned by the sending bank to indicate if the account is a 'collection' account rather than for a unique entity
Utility flag	If recipient is a known utility provider
Channel indicator	Indicator as to how the customer requested the payment – e.g. digital banking or face to face
Warning flag	Indicating what warning codes have been provided to the sender e.g. warnings around making investments

By adding in this extra data capture in any real-time payment transaction, payment providers will be much better equipped to stop fraudulent transactions from occurring, effectively 'designing out' APP fraud from the payments system. To do this, these additional datapoints would be used to assess the intent behind each payment. Information like the type of account (personal or business, type of business, length of time in operation, usual activity, type of product) would enable us and the recipient bank (who would receive data such as payment type and classification) to add all of this to our fraud detection, or even into warnings or Confirmation of Payee journeys.