Callsign Ltd – Written evidence (FDF0038)

Introduction

1. As a British technology company and a global pioneer in digital identity and authentication technology, with a track record of supporting the UK banking sector in preventing and tackling fraud, Callsign is delighted to have the opportunity to respond to the Fraud Act 2006 and Digital Fraud Committee's inquiry. We have centred our answers on sections relating to the fraud landscape and the regulatory and legislative frameworks in place to tackle fraud.
2. We would be delighted to discuss our submission and the issues that we have raised in greater detail, should that be of interest. We would also be delighted to give oral evidence to your Committee and to provide further details on our experience of working with regulators, governments, and the banking sector to prevent and tackle fraud.

About Callsign

3. Callsign is a British technology company and a global pioneer in digital identity. We are committed to working with government, regulators, and our clients to combat financial fraud; and make the UK a world leader in the implementation of digital identity solutions that support innovation and maximise consumer protection. Since 2012, we have grown from an ambitious start-up of two passionate British entrepreneurs to a thriving global company employing over 450 people and working with leading international businesses to tackle existing fraudulent threats and identify new, emerging issues. In the UK, we work with leading retail banks including Lloyds and HSBC, supplying the first identification platform that uses AI to build digital DNA for the recognition of users – right down to the way users type and swipe.
4. Our layered intelligence solutions build a digital DNA picture of every user to positively identify individuals in a privacy preserving manner. This is done with unparalleled accuracy during interactions on digital banking platforms and services, with the most advanced technologies reducing fraud due to digital impersonation by 83%. This, coupled with the use of other factors such as document verification and background checks, accurately verifies users' identity and interactions, helping to root out suspected fraudulent activity from the outset, without impacting legitimate claims and user journeys.
5. We are committed to research and development in the UK, we invest heavily in R&D, and as part of our partnership with London Metropolitan University's Cyber Security Research Centre, we fund a dedicated fraud & malware prevention research office. In line with the government's ambitions to make the UK a world scientific superpower, we have also launched partnerships with leading universities such as the University of Oxford and University of Manchester to develop new fraud prevention

technologies and provide high quality apprenticeship and internship opportunities to help the next generation foster genuine digital skills and play a part in the development of new ground-breaking authentication and fraud prevention technologies.

Fraud landscape

Q1. What fraud risks are UK a) individuals, b) the Government and c) businesses particularly vulnerable to today, and what are the reasons for this?

6. Fraud is rife across the UK. The National Crime Agency reports that fraud is the most commonly experienced crime nationally[1], while a recent study from the financial services firm Crowe and the University of Portsmouth estimated that fraud losses cost the UK economy over £137 billion each year[2]. In 2020 alone, over £1.26 billion was lost by banking customers to fraudsters due to social engineering and scams[3], while last year the value of alleged fraud cases exceeding £100,000 that reached UK courts was £445 million[4]. In the public sector, Lord Agnew within his resignation speech stated that over £30 billion is lost to fraud each year, while the Public Accounts Committee recently estimated that this figure may be as high as £51 billion.
7. Below, we have outlined our experience of the main fraud risks to individuals and government.

Individuals

8. A major fraud risk for individuals is the growth of Authorised Push Payment (APP) fraud, with the issue set to become even more prominent in the years to come. According to the financial services trade body UK Finance, APP fraud increased by 71% between the first six months of 2020 and 2021, costing UK consumers over £350 million[5] . We expect that despite the forthcoming introduction of new rules by the Payments System Regulator (PSR) and legislation that will force payment service providers (PSPs) to publish APP scam data and reimburse victims, APP fraud will continue to rise and become the top fraud category for both reported losses and customer impact.
9. This is likely to incorporate a range of APP scam types, with the extent of the increase dependent on customer demographics, the banking channels provided, and PSPs' individual approach to authentication. At Callsign, our primary focus and overall objective is to help our clients mitigate against the potential impacts of fraud by detecting and preventing APP scams in real-time, ultimately reducing losses to both the PSP and the customer. However, whilst we recognise that there is

[1] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime
[2] https://f.datasrvr.com/fr1/521/90994/0031_Financial_Cost_of_Fraud_2021_v5.pdf
[3] UK Finance Fraud The Facts 2021: UK Total 2020 fraud Losses
[4] KPMG Fraud Barometer: Annual Report 2021
[5] https://www.finextra.com/blogposting/22075/app-fraud-is-a-growing-problem-for-banks

no silver bullet to stopping losses in their totality due to the volume, variety, velocity, and veracity of APP scams, we believe that a greater focus is needed on preventing scams from happening in the first place, with solutions required that take into account each stage of the customer journey and the unique user experience of each bank.

10. For instance, data shows that 70% of scams originate on online platforms[6], with consumers unable to distinguish between legitimate and scam messages and adverts. While we welcome recent efforts to strengthen the Online Safety Bill to ensure that the largest platforms put in place proportionate systems to prevent fraudulent adverts being hosted or published, we await the upcoming codes of practise which will outline the steps that online platforms that host user generated content and search engines should take to comply with this new duty. We firmly believe that, in complying with this duty, such platforms should apply learnings from the banking sector, where Strong Customer Authentication (SCA) checks are used to authenticate users and prevent fraudulent activity from taking place.

11. For example, we have developed controls that are specifically designed for our banking clients, and which are applied across the transaction lifecycle, maximising data collection and customer engagement opportunities to help them to identify suspected fraud and stop malpractice from taking place. This includes performing proprietary behavioural analytics that assess how a user interacts with their digital channels, to flag anomalous behaviour when they make a payment that results from an APP scam. This analysis is combined with PSPs' transaction risk analysis scores and beneficiary analysis from third party intelligence sources to provide a robust profile of the transaction and recommended treatments.

Government

12. As noted above, tens of billions of pounds are defrauded from government each year, from the £4.9 billion confirmed to have been wrongly paid out in coronavirus business support schemes, to the record £5.5 billion that was lost by the Department for Work and Pensions to fraudulent Universal Credit claims last year. These figures dwarf the £1.3 billion lost by banking customers to fraudsters in 2020, which caused the PSR, with the support of HM Treasury, to bring forward proposals to force banks to take action, including to publish scam data and introduce new mandatory reporting measures. In our view, government must take further steps to root out fraud across the public sector. This includes developing a more joined-up approach to tackling fraud and encouraging procurement authorities to work closely with industry to design and implement technologies that keep pace with, and prevent, novel forms of fraudulent activity.

13. From our experience, fraud is like water – it finds the smallest cracks in the system, building up over time, before creating problems of a significant scale. This is particularly true for public services, where an absence of a centralised authentication system, or joined-up

[6] https://www.ukfinance.org.uk/press/press-releases/over-two-thirds-of-all-app-scams-start-online%E2%80%93new-uk-finance-analysis

approach to tackling fraud, leaves it vulnerable to abuse. For instance, from the start of the pandemic to the end of May 2021, government departments had delivered 69 new digital services, with a further 46 services in the pipeline. Many of these services, such as the Bounce Back loan scheme, are well documented to have been subject to fraud; while others, including the NHS contact tracing application, generated privacy and inclusivity concerns.

14. Whilst we understand that these systems often need to be created at great speed, we urge the government to work closely with industry on the design of any future schemes, utilising best-in-class technologies that are already widely deployed across the economy to provide protection to legitimate users, whilst rooting out criminal activity and preventing abuse. This approach has been used successfully in other countries such as Belgium and Canada, with detail provided in response to Q14.

15. The use of One Time Passcodes (OTPs) across government and public services also creates avenues for fraud to occur. These OTPs are twice as expensive to implement as behavioural biometrics and provide additional points during the authentication process for potential interference and manipulation by bad actors. Every time these transactions take place, an increasing number of external parties are involved to carry out each stage of authentication. In the case of an OTP, this could include a citizen's bank or payment service provider, SMS gateway and network operator. As more of a consumer's data is shared around the ecosystem, the risk of it being intercepted increases by a factor of 1, opening up public schemes to potential manipulation and fraud.

16. Moreover, in the case of business fraud in government, there are considerable opportunities to implement multi-layered authentication processes that bring together information from various government databases, such as HMRC, Companies House and HM Treasury records. APIs could be used by government to check and authenticate the identity and financial affairs of company directors, rooting out shell companies and bogus claims within minutes. These APIs are already readily deployed in the banking sector and could be easily implemented across government departments, with scope for consideration within the upcoming reform of Companies House and delivery of economic transparency legislation.

Q2. What future economic and technological developments are likely to impact how fraudsters seek to commit crime over the next five to ten years, and how might these be prepared for and mitigated? What role can technology and tech companies play in combatting fraud across this timescale?

17. From our experience of working to tackle fraud, we have identified three key developments that fraudsters may seek to leverage in the coming years. Combined, these developments have the potential to increase fraud exponentially as methods become more readily adoptable and targets become more ubiquitous as new market values and methods of online engagement become pervasive.

Development of new technological platforms and markets

18. We believe that the rise of unregulated financial markets, services and trading capabilities will become repeated targets for either direct fraudulent activity, the continued funding of fraudulent activity or the obfuscation of fraudulent activity. Traditionally, fraudsters launder money through bank money mules (willing or otherwise) or gambling accounts, with the Gambling Commission currently operating a Gambling Anti-Money Laundering Group to spot suspected fraudulent activity. More recently, we have seen activity extend to crypto-trading platforms, and we anticipate that there will be an increase in the number of avenues of trade and commodities used to commit fraud as emerging technological markets and products become more popular.

19. For example, non-fungible tokens (NFTs), and value placed in digital "things" will cause increasingly greater re-appreciation for targets. We envisage that more value and access to purchasable digital assets will lead to traditionally physical burglary or petty theft being replaced by a ubiquitous electronic equivalent. In fact, the law firm Pinsent Masons recently reported that 10 cases of NFT fraud were reported in 2021[7] (up from two in 2020), with many further cases expected as more retail investors become interested in the space.

20. Equally, the so-called 'Metaverse' will introduce more populist methods to interact with one another, consume goods and trade. This will not necessarily establish new fraud methods but will create additional avenues for existing fraud methods to be applied. The issue of identity and trust online will remain, but the increased diffusion of where this can take place will create wider opportunity for criminal behaviour. This is particularly the case if digital identity solutions and checks are not implemented to confirm the identity of individuals using the Metaverse.

21. If identities are not confirmed, a challenge of fraud data processing will develop, alongside the creation of necessary 'fraud forensic' roles. These roles will be needed to initially evaluate the complexity of emerging fraud cases that occur across multiple, new and emerging novel online environments.

Fraud-as-a-Service technologies

22. As identified previously, fraud is a business. Fraudsters therefore operate in markets and against organisations that have good returns of success and use methods that are commensurate in cost to the potential value that can be gained. Technologies used to commit fraud are becoming more sophisticated, cheaper and more readily available, making it easier for fraudsters to operate.

23. It is evident that linear levels of sophistication go hand-in-hand with the evolution of technology. Looking ahead, we anticipate that the reduction in technology costs will lead to more fraudulent activity. Unskilled fraud actors who have traditionally relied on programmes or scripts created by others to commit fraud – known colloquially as 'script kiddies' – will have increased access to more sophisticated fraud

[7] https://inews.co.uk/inews-lifestyle/money/nft-fraud-is-growing-in-the-uk-with-scammers-taking-advantage-of-consumers-with-little-investment-experience-1528395

services on black markets at low prices. This may lead to a potential increase in the avenues available to commit fraudulent crimes.

24. We have already seen this in action, with the TalkTalk cyber-attack and data breach that occurred in 2015, implemented by a 17-year-old using pre-produced hacking software that scanned for security vulnerabilities online. This ultimately led to 15,000 customers having their detail stolen, with attacks of this nature likely to increase in incidence as technologies develop.

Disruptive data

25. The continued proliferation of sensing technology and smart devices means more and more interactions will be processed by advanced modelling that converts signals into predictions and outcomes. Today, in the financial services industry, interactions at account opening are evaluated against known lists of devices, IP addresses or behaviours synonymous with fraud. With acute awareness of "signals" being the default processing method of data, we will start to see more and more disruptive techniques used to augment signals, change data points, mimic identities and "replay" trust.

26. We have seen a very obvious example(s) of this with synthetic identity creation (application fraud) and deep-fakes to aid scams or attempt to beat biometric tests. However, future developments will lead to more subtle and more prevalent and accessible mechanisms to beat-the-system either through evasion, confusion or complication.

The role of technology and tech companies in tackling fraud

27. Tech companies must collaborate to implement mechanisms that help to establish trust online, and root out fraudulent activity. This includes:

    a. **Diversity of authentication mechanisms**: Companies must provide and layer multiple authentication mechanisms to enable equal choice, robustness and optionality, and mitigate against vulnerabilities that facilitate fraud. Systems and technologies that authenticate users based upon the business context (i.e., what action is the user doing? What have risk signals indicated about the validity of the user?) will be best suited to adapt to new and emerging digital channels and markets.

    b. **Signal based risk and authenticity assessments**: In-channel, and in-product, interventions should be introduced that process signals that a user's identity, session, transaction or device has been compromised and is at risk of fraud. This is particularly relevant for responding to instances of social engineering, such as APP scams, in a manner which is minimally obtrusive to customer engagement. We currently work with several leading banks to provide tailored, dynamic fraud messages to users when there is a suspicion of fraud. These messages, which require active engagement from customers, are used for several purposes, including to capture additional information on the purpose and context of the payment; provide additional user interactions for behavioural analytics; and to help providers and/or customers to identify that a scam is taking place. These messages are fed back

to our clients' transaction monitoring services to enrich their fraud models and drive operational intervention via their case management capabilities, removing the need for further portals or the duplication of generated alerts within the operational area of the bank.

c. **Verified credentials frameworks**: Industry must collaborate to facilitate the digitisation of credentials ('verified credentials') and develop a supportive technical framework. This is a set of emerging technical standards that aims to establish a trust model between issuers, holders and verifiers of credentials by:

   i. Establishing trust through a digital tamper-proof set of claims made by an individual/company about something they claim to have (a possession), or something they claim to be (inherence) to a third-party completing verification checks. This includes attestations as to the authenticity of the credential as well as guarantees around the authenticity of the issuer of the credential and the holder of the credential.

   ii. Developing a model that sets out the owner of verified credential, and their right to choose who to release information to.

   iii. Ensuring privacy protocols to minimise the data that is shared with verifying agencies, such as only supplying date of birth to online off-licences to attest that a consumer is old enough to buy alcohol.

28. There is also a clear role for government and third parties to contribute to the development of an ecosystem that builds digital trust and tackles fraud. We welcome the recent action that the Department for Digital, Culture, Media and Sport has taken in this regard as part of the development of its digital identity and attributes framework, and look forward to further constructive engagement on the implementation of its proposals.

29. However, we need to ensure that we create a diverse set of suppliers that can perform digital identity checks, with opportunities not concentrated in the hands of a select few tech giants with the potential to monopolise the space. As the industry develops, it will be essential that we have a market that can respond at pace to novel forms of fraud, leveraging skills and best practice from the financial services sector, which has been successfully innovating to tackle fraud for several years. We urge government and regulators to work to create a truly competitive market for digital identity, enabling innovative solutions that help to tackle fraud and increase consumer protection to be sourced from organisations of all sizes.

Q4. What is the role of international actors in the UK's fraud landscape? What are the barriers to tackling borderless fraud?

30. Fraud is a borderless industry, with fraudsters able to facilitate crimes in the UK from abroad or encourage victims to make international transactions. In fact, fraud is only set to become more

global in nature, with limited traceability of international money transfers and many of the future economic and technological developments that we have outlined in Q2 occurring online across borders with limited audit trails, including financial flows relating to cryptocurrencies and NFTs. There is undoubtedly a clear need for enhanced and more coordinated action between the UK, foreign governments and multilateral bodies to identify loopholes in current fraud frameworks and share best practice on the identification and treatment of fraudulent crimes.

31. The UK has taken great steps in working with international actors in other areas of policy such as digital taxation, driven by the work of the OECD, and cybersecurity through the work of the World Economic Forum's Global Future Council on Cybersecurity. We must now ensure that the UK takes on lead on fraud internationally and helps to drive forward the development of a global standard for tackling fraud, underpinned by common legislative frameworks and partnerships that help to prevent, detect and tackle fraud.

32. This includes working to introduce global accountability for tackling international fraud, and ensuring that we consider fraud prevention when negotiating co-operation and international trade deals with our partners and allies. For instance, the UK and Switzerland have successfully cooperated since 2013 to recover unpaid taxes from offshore accounts as part of the Account Disclosure Pact, with scope for this agreement to be extended to cover fraudulent activity and be used as a blueprint for future bilateral and multilateral agreements. Such agreements could include commitments to bring forward asset sharing arrangements, recouping and splitting the proceeds of identified fraudulent activity between relevant authorities. This will help to stop criminals accessing the profits of fraud and disincentivise criminal activity from taking place.

33. We must also introduce an international standard for authenticating cross-border financial flows and ensure that data is shared between banking authorities when transactions are made. Regional initiatives such as the European Banking Authority's Single Euro Payments Area (SEPA) – used currently by the EU, European Economic Area and UK post-Brexit - have undoubtedly helped to increase the efficiency of financial flows for legitimate customers, whilst also increasing the traceability of transactions and harmonising payments standards, with scope for such schemes to be rolled out across the globe. These schemes could also be used to oversee the expected increase in cashless transactions, such as those involving cryptocurrencies, in the years to come.

34. Moreover, we must build on the invention of GDPR and work on a global basis to regulate the management of personal data and provide greater privacy and protections to banking customers. Data has become a new form of currency and where legislation and regulation has improved over the years to protect Payment Card Information, this could and should be extended to personal data, to more closely control the storage, movement, and access of data. This includes introducing a common framework for how the owners and

processors of data are able to access information, and ensuring that users have the right to be informed when data is transferred between entities. Further detail on data protection is set out in the relevant section below.

Action to Tackle Fraud

Q7. What are the responsibilities of the private sector in protecting the public against digital fraud? How can a balance be achieved between the need to tackle digital fraud whilst supporting the growth of these sectors? To what extent is work done to combat fraud across the private sectors undermined by siloed or independent working practices?

35. The private sector has a clear role in tackling fraud, working transparently in accordance with requirements set out in legislation and regulation, and proactively collaborating to share intelligence and data on fraud trends and cases. For instance, we wholeheartedly agree with the proposals recently set out by the PSR to require banks to publish data on the value of APP scams and scam rates, and to create a Joint Working Group to improve intelligence against fraud and share details on the nature of transactions.

36. However, fraud must be treated in the round, with government, the private sector and third-party organisations working together to tackle fraud. Government has made significant strides in engaging with industry in other areas of digital and financial services policy, creating numerous bodies to consider areas for greater cooperation in the development and enforcement of regulations. This includes the Artificial Intelligence (AI) Public-Private Forum to consider the future use of AI in financial services, the forthcoming Digital Identity Working Group to implement digital identities and the Digital Regulation Cooperation Forum to consider the challenges of online regulation.

37. However, there is no single body in place that effectively brings stakeholders together to discuss fraud and build an understanding of the technologies that are utilised to both commit and prevent fraudulent crime. Last October, the Home Office's Joint Fraud Taskforce was relaunched to counter fraud through public-private sector partnerships, but we have seen limited output from the group since then. We urge government to work more closely with the group to identify fraud threats, expand its remit beyond the Home Office, and bring forward innovative solutions that can be implemented across the fraud landscape.

38. Moreover, government needs to ensure that it takes a holistic view when engaging with private sector and considers solutions that can be deployed across government. Currently, as noted by Lord Agnew following his resignation from government, government's fraud prevention agencies work in silo from one another, engaging with the private sector independently on issues specific to individual departments. We would urge government to ensure that it creates new avenues for data and best practice from the private sector to be shared across government, with an entity overseen by a single minister established to lead engagement with industry and coordinate the work of different fraud prevention agencies and taskforces.

Q9. What is the role of the individual in relation to fraud? Are consumers well informed about the risks of fraud and how to prevent them? If not, which bodies or organisations should do more to ensure this? What are the most effective methods of educating the public about fraud crime and prevention?

39. Whilst educating individuals on risks, and encouraging vigilance against fraud, are important elements in the pursuit to tackle fraud, the ultimate onus and responsibility must be placed on organisations due to the scale of fraud attempts and deployment of novel techniques. As noted above, scams are becoming more and more sophisticated, with fraudsters increasingly successfully replicating the brand and channels of public organisations, companies and banks. As a result, upskilling individuals about fraud will only go so far, with organisations needing to act agilely to identify and respond to new threats.

40. For example, recent Ofcom data shows that scams are indiscriminately targeting all age groups, with individuals unable to avoid fraud attempts. In the three months to October 2021, 44.6 million adults in the UK (over half the national population) reported that they had received a suspicious text, message or phone call to a landline or mobile device, with 75% of 16-34s reporting that they had received a scam text and 61% of over 75s saying that they had received a suspicious phone call.

41. During the pandemic there was also an uptick in scam phishing texts and e-mails that mimicked government agencies, offering payments for self-isolation, vaccine uptake or testing in a bid to steal consumer's banking information or identity, with individuals unable to distinguish between these scams and legitimate alerts. In the first two weeks of lockdown alone in March 2020, Age UK identified over 200 new phishing e-mails, with these specifically targeting the vulnerable and elderly and resulting in over £800,000 being lost to fraudsters in a single month[8].

42. Moreover, studies have revealed that even the savviest of consumers are unable to spot scams, with data from Verizon outlining that 25% of data breaches in companies are caused by phishing, with 85% containing an element of human error[9].

43. As a result, we urge government to focus resources on ensuring that organisations are made responsible for tackling fraud. This includes introducing tailored warnings that help consumers to identify fraud attempts, with current warnings often being generic and easily ignored, or used as a mechanism for fraudsters to coach consumers into transactions. These warnings are also presented too frequently, with alerts delivered during legitimate journeys creating undue friction to consumers as messages are perceived to be a common stage in the transaction process. This ultimately decreases users' sense of the importance of warnings, encouraging them to click through without due consideration of the message's contents.

Legislative remedies

[8] https://www.ageuk.org.uk/notts/about-us/news/articles/2020/coronavirus-covid-19-related-scams/
[9] https://www.verizon.com/business/en-gb/resources/reports/dbir/

Q8. What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For example, to what extent does General Data Protection Regulation (GDPR) limit data sharing?

Q11. Is existing legislation effective in tackling the increase in modern forms of fraud? If not, is there a legislative remedy, or should fraud be addressed primarily through implementation of existing provisions? Answers may refer to existing mechanisms such as increasing the scope and powers of regulators. You may refer to any legislation and are not limited to the Fraud Act 2006

44. Existing regulations place a significant emphasis on data privacy and protections, with this limiting the ability to develop signals online that can detect suspected fraud. In the UK, this has largely been driven by legislation concerning GDPR, which seeks to increase transparency on data collection and impose controls on data use to counteract risks associated with data beaches and handling. This has led to the largest tech giants - such as Google, Apple and Amazon – and platforms – such as W3 – generating default privacy settings and mechanisms that reduce the uniqueness of signals observed online.

45. As a result, a rather binary implementation of data privacy and data handling techniques has developed, without an appreciation of the wider implications for tackling fraud:

    a. OS and Web vendors have closed off APIs, mindful of the desire to increase privacy and reduce advertising tracking and the collection of cookies. This has led to a reduction in the signals available to detect fraud, such as device identification and behaviour recognition.

    b. GDPR has created a concern of data sharing between parties even where public interest could be identified, limiting the ability of industry to work together to share information on fraud and detect patterns of activity and novel techniques.

46. As such, legislative and regulatory clarity is required on the use of fraud data, and the sharing of data for fraud detection to open-up access to private APIs, and support those with clear use-cases validated by authoritative bodies.

47. Equally, when we consider that online interactions will become increasingly complex, as outlined under Q2, it would be beneficial to appreciate both how fraud has been committed, and the value extracted, with this mapped to evolving technologies. It is evident that more mechanisms to trade gives fraud actors additional avenues to obfuscate, hide and confuse the trail of digital breadcrumbs left from a fraud attempt. When appreciating this, the only real answer is to more greatly enable business entities to share data and facilitate cohort-based and industry-wide analysis and enforcement action.

48. Moreover, there is a need for industry to be able to share data unrelated to specific fraud events, but that enables fraud trends and correlations to be identified. Bodies involved in data protection, such as the Information Commissioner's Office, regulators including the Financial Conduct Authority (FCA) and trade associations should work together to explicitly

codify the grounds for sharing data, in order to facilitate greater cooperation across industry and tackle fraud more quickly.

49. Government and regulators should also assess the remaining weaknesses in authentication journeys and identify areas where customer protections can be improved. For example, recently the FCA decided to not incorporate the European Banking Authority's (EBA) opinion on the inherence element of Strong Customer Authentication (SCA) and to expand its definition to include behavioural analytics such as spending patterns. We believe that this risks replacing customer authentication with fraud identification, and in turn causes friction in the customer experience.

50. This is the case as spending patterns are an easily learnt behaviour that can be subject to manipulation by bad actors and which must be supplemented with either a knowledge or possession factor (most likely an SMS One Time Passcode (OTPs)) to deliver a fully SCA compliant authentication event. Not only has Multi-Factor Authentication via SMS OTPs proven to be expensive, cumbersome, and far from invulnerable (as outlined in Q2.), but working remotely, fraudsters can misdirect an authentication check or SMS without suspicion. As such, we urge the FCA to review its decision and ensure that we implement a robust regulatory framework that maximises consumer protections and deters fraudulent activity from occurring.

Best Practice

Q14. What lessons can be learned from effective policy interventions and schemes both in the UK and overseas?

51. Other nations have made great strides in working with the private sector to create world-class digital identity schemes that help to prevent and tackle fraud, with the noticeable difference being how those governments have worked with the private sector. For example, in Belgium, the government took the lead from the private sector and integrated solutions developed by the banks into its identification services, with users now on average completing six banking transactions and three e-government transactions per month using the safe and secure service. In 2020, the government also introduced new electronic identity cards with additional protective layers built into it to prevent duplication, including digital fingerprints and QR codes, with these set to be rolled out across the country by the end of 2024.

52. Moreover, in Canada, progress has been made through coordinated and determined collaborative work between the public and private sector following the creation of the Digital ID & Authentication Council of Canada to propel innovation and tackle fraud. We welcome the UK government's formation of a new Digital Identity Advisory Group, but urge ministers to go further and implement a similar model as it develops its own digital identity framework, engaging with industry at every opportunity to ensure that solutions to fraud prevention maximise consumer protection and incorporate the latest technologies.

Q15. Can you suggest one policy recommendation that the Committee should make to the Government?

53. Government must take decisive action to tackle fraud and appoint a single minister who is wholly responsible for overseeing fraud prevention strategies across the public and private sectors. Currently, there is no joined up approach for tackling fraud, with policy developed in siloes and limited interaction between government departments, agencies and the private sector.

54. This minister, accountable to the Prime Minister, should be given remit to bring forward a new cross-government fraud prevention strategy, requiring government departments to upskill their capabilities to identify fraud risks and implement technologies that keep up with the latest techniques deployed by fraudsters. This strategy should draw on the expertise of the private sector, including the use of identify solutions deployed in the banking sector to verify users and identify suspected fraudulent activity from the outset.

22 April 2022