Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Thursday 24 March 2022

10.50 am

Watch the meeting

Members present: Baroness Morgan of Cotes (The Chair); Lord Allan of Hallam; Baroness Bowles of Berkhamsted; Lord Browne of Ladyton; Viscount Colville of Culross; Lord Gilbert of Panteg; Baroness Henig; Baroness Kingsmill; Lord Sandhurst; Baroness Taylor of Bolton; Lord Vaux of Harrowden; Lord Young of Cookham.

Evidence Session No. 8 Virtual Proceeding Questions 70 - 79

Examination of witnesses

Ghela Boskovich, David Pitt and Kate Martin.

The Chair: Thank you for attending the second session this morning as part of the inquiry into the Fraud Act 2006 and digital fraud. I am delighted that we are joined for this session by Ghela Boskovich, regional director of the Financial Data and Technology Association, David Pitt, chief executive of Pay.UK, and Katie Martin, markets editor at the *Financial Times*. Baroness Kingsmill has the first question.

Q70 **Baroness Kingsmill:** Good morning. We are looking to you to help us establish the fraud landscape. Perhaps I could start with you, David Pitt. Could you give us an outline of the most common types of fraud that take place using payment platforms? It has probably changed considerably, given that there are so many more mobile payments and faster payments. Perhaps you could give us an idea, too, of how it may change further with the implementation of the new payments architecture.

David Pitt: Good morning and thank you for this opportunity to position where we are on fraud. Pay.UK is a not-for-profit organisation. We operate critical national infrastructure. We have a unique role to help in fraud and help detect and prevent fraud. We provide the opportunity, data and systems for our banks and building societies to detect and prevent fraud. The most common type of fraud is Authorised Push

Payment fraud on payment platforms. And this is where vVictims believe they are making a legitimate payment and request that payment to go through their bank.

We operate 15,000 transactions a second. There are around 10 billion transactions a year. In monetary terms, there are about £7.2 trillion of account-to-account transfers. Fraud, while it is really emotive, and also has a massive financial impact on the victim, and this is not to belittle fraud but, to give a context, represents 0.0067% of transactions.

We are determined to play our part and operate a safe and secure payments platform to reduce and eradicate fraud. You mentioned the NPA—the new payments architecture—which will replace the existing critical national infrastructure and allow us to have a state-of-the-art platform, to increase innovation and to continue to develop our service. However, I have to say that we are not waiting on the new payments architecture. We are acting now. It comes down to how we improve detection, prevention and reimbursement. As you say, we have seen an increase in fraud, with an increase in online transactions; 70% of authorised push payment fraud starts online. It is critical that we think about how we can improve our data to get into detection, prevention and then adequate and appropriate reimbursement.

Ghela Boskovich: To give you some context, the Financial Data and Technology Association is a trade association representing third-party providers engaged in providing open banking under a licence and accredited regime with the FCA. All our members are participants in either account aggregation/account information services or payment initiation services. They are part of the value chain in executing or initiating payments at the very beginning.

In the landscape of fraud, I think a little more context can be provided. Push payment fraud is an emerging type of fraud, but it is not necessarily the most prevalent. Payment card fraud, which happens online or in the absence of the card, accounts for about 45% of fraud in the market. The research has been pulled together by UK Finance, which is a conglomeration of bank representatives. It comes directly from payment service providers.

The other component is remote payment or remote banking, online banking. It also includes mobile banking. It is about 38% of fraud in the market. Authorised push payments, which David mentioned, constitute about 16% of the type of fraud in the market today, but it is a concern because it is incredibly savvy in social engineering. That is probably the root cause of where we are getting most of the growing APP fraud. It is social engineering rather than a data hack or having data compromised in card numbers on files with merchants, or having breaches of those sort of things.

It is very much about how we encourage people to engage in a payment, where they are initiating information based on pressure or persuasion, rather than having a compromise of the payments system itself or the

data being compromised. That is an important thing to keep in mind. Much of what we are talking about in the domain of a new type of fraud is social engineering and not necessarily the technological mechanics involved in the fraud itself.

Baroness Kingsmill: I see that.

Katie Martin: The other two witnesses have already spoken beautifully about payments fraud. From my point of view, crypto fraud splits into two main areas: wholesale and consumer. On the wholesale side, there is money laundering; there are ransom payments that are very often denominated in cryptocurrencies or crypto assets, and there is a lot of illicit activity. On the other side, you have consumer scams.

Money laundering on the wholesale side is relatively straightforward. You take ill-gotten gains from whatever it is—people trafficking or the drug trade—and convert those proceeds into cryptocurrencies and then pull them out of the financial system the other end in currencies that you can actually use for day-to-day life, such as sterling, dollars or euros.

The way that crypto works is that all transactions are visible on a public database, known as the blockchain. The difficulty is in matching blockchain addresses to real humans, to real people. The KYC side—"Know your customer"—is often not there. The big exchanges all claim, quite sincerely, to have quite extensive KYC efforts, but there are gaps, just as there are in mainstream finance. In addition, because this is what we call a decentralised industry, you can cut out the intermediaries entirely. If I wanted to send you some bitcoin or some dogecoin, or whatever it might be, I could do that without necessarily using an exchange and without using a bank. It is difficult, but not impossible, to trace that stuff.

There was a recent case in the US where two people were arrested over their alleged role in the hack of an exchange called Bitfinex in 2016. Their assets were confiscated. The financial seizure was $3.6 billion. It was the biggest-ever seizure in the US. That case dated back, as I say, to 2016, and goes to show that even years later, and even after funds have been sent between different jurisdictions—in this case, allegedly, Liechtenstein—it is still possible to track these people down. None the less, it is a huge area that is very international in nature and it is difficult to track down the real people behind it.

The other main area for concern is consumer scams. One of the main things to remember is that crypto assets are generally not securities. They do not fall under securities regulations. There is a lot of bad behaviour that is not necessarily, strictly speaking, fraudulent or illegal but is, none the less, unsavoury and can lead to severe consumer harm. It takes a number of different forms.

Right now, there is somebody on Instagram pretending to be me, with my picture and my profile, sending people direct messages and trying to get them involved in a crypto trading scheme that has nothing to do with

me. This is extremely common. There is impersonation. There is not having a good grasp of who the people behind these investment schemes are.

There is also what we call rug pulls. You launch a coin and call it whatever you like. Some of these things are named after swearwords, pets, people or whatever it might be. You create some online buzz about it, perhaps by impersonating somebody else or by getting some celebrities on board. You lure people into the schemes. The price of the coins shoots higher, and then the original people behind it pull the rug, get out, take the gains and disappear.

There are people trading on what looks like inside information. It is what we would call trading on inside information in standard securities markets. You find out which coins are likely to get a prominent position on a particular exchange. Again, you get in first, watch the price shoot up and then you pull out. It is not illegal—these things are not shares or bonds—but it causes real harm to people.

There are two more areas. I would call one of them bamboozling. There are financial products that we often refer to as yield products. You can buy perpetual futures in crypto assets. You can buy all sorts of structured products and derivatives around crypto products. We have had people with PhDs in structured finance look at some of these products to try to figure out how they work, and they cannot. They are presented as quite simple investment tools for day-to-day people, but they can just crater, and people can lose all their money incredibly easily.

The other big thing is the misleading nature of a lot of the discourse around crypto coins. There is the idea that the price of bitcoin, the earliest crypto coin, shot to the moon, so that if you get in at an early stage on a lot of other tiny little crypto coins, perhaps you could enjoy those sorts of riches too. It is rarely made clear enough in the advertising around that that you are taking a huge risk with your money and that you could lose all of it. The message from the Financial Conduct Authority that you stand to lose all of your money, which it has said repeatedly and loudly to anybody who will listen, is not cutting through to the general public.

Q71 **Baroness Bowles of Berkhamsted:** My first question was to ask what the business models are for crypto asset fraud, but I think you have trotted through a reasonable amount of that. Then they cash out by taking their money out. I believe it is a legit currency in another jurisdiction, so they escape that way.

Is it not that much different from the frauds that happen elsewhere with real cash but just transferred into a token system? Is it really that different? Ghela, you mentioned, for instance, somebody impersonating you to recommend a cryptocurrency. Identity fraud, in itself, is not criminal, but it lies at the heart of a lot of things and a lot of introductions. It is quite difficult to take action. I have been impersonated. A regulated entity was doing it, so the FCA saw them off,

but what if you are not in that position? If identity theft and impersonation was a criminal offence, Kate, do you think that would help, or are these people beyond touching?

Katie Martin: There are certainly some common areas with other types of fraud. KYC issues are just as prevalent in traditional finance as they are in crypto markets. Impersonation cuts through to what we would call more legitimate and more established parts of finance, but on top of that there is a layer of anonymity that makes tracking down perpetrators much harder.

The National Crime Agency, for example, has called for the regulation of what is called mixing technology, which disguises transactions that could otherwise be traced on the blockchain. It is thought that about 15% of all proceeds of crime were routed through mixers in 2021. In addition to the layer of anonymity, there are specialised services that add extra anonymity on top of that.

Yes, you have some of the same tricks from traditional finance being played in crypto, but it is much harder to find out who is responsible.

Baroness Bowles of Berkhamsted: For example, if market manipulation covered the crypto sphere, that is not going to help you because you would not find out who was doing it.

Katie Martin: That is a tricky concept, in the sense that for it to be market manipulation the whole industry has to be recognised as a market, and they have to be securities that go through all the kind of transparency and reporting requirements that other securities do. Currently, that does not exist and it would be an enormous job.

As I say, there is a lot of activity that is not, strictly speaking, illegal. It does not necessarily break what we would understand to be securities laws, because they are not securities. It falls into a massive grey area.

Baroness Bowles of Berkhamsted: You do not think that you could just widely say that anybody who is operating Ponzi-type schemes, or what is essentially a manipulative scheme, irrespective of what the asset is, is committing a crime. You could not define it as a crime and it would not be possible to pursue it. We only have securities laws, if you like, attached to securities because they name just about everything you can think of, but something else has come up, so why can you not stretch securities law to it?

Katie Martin: It all rather reminds me of the case of Football Index, which collapsed in 2021. It was an online betting company that styled itself as a stock market for football fans. You could buy shares in footballers. It was a gambling service, but it looked like a trading app; they called the participants traders. Those instruments, for want of a better word, paid dividends. It all looked and sounded very much like the stock market that we know, and which exists in a very firm regulatory framework, but it was not. When it collapsed, people lost their money, but it was nothing to do with the Financial Conduct Authority. It did not

fall under its wing at all. That is why you have a grey area where there is nobody looking after this asset class. That is why there is so much scope for bad behaviour.

Baroness Bowles of Berkhamsted: Should somebody be looking after it, and who?

Katie Martin: Regulating the asset class is potentially too difficult a thing to get round quickly. What you can do faster is regulate which organisations are active in the market and how they advertise themselves to the public. They are the easy wins.

The other easyish win is to impose tighter regulation and more scrutiny around what we call on-ramps and off-ramps, the points at which ordinary people get their money into crypto platforms and how they pull it out again. That has to go through intermediaries that interface at some point with standard bank accounts if they want to get normal currencies out to spend on normal things. There is a rising level of scrutiny into who those payment agents, for want of a better word, interact with and whether the platforms are fit and proper. David probably knows more about that kind of space than I do. The points where crypto meets traditional finance are the points where we can intersect.

Q72 **Baroness Taylor of Bolton:** Thank you. Kate, this is desperately interesting and very informative. I know that our other witnesses will want to come in, but can I follow up with you first about the actual perpetrators? Who is it that we are talking about who is actually organising the cybercrime, including crypto fraud? You mentioned that some are operating at wholesale level and some at consumer scam level. Are these groups the same, or are they divided up in a sort of mafia-type organisation where different groups have their hands on one particular type of crime? Where are they based? We have read that a lot of this is based, particularly on the crypto side, in Russia. Is that the case? Can you paint a picture of who has the levers on this kind of crime?

Katie Martin: I would steer you away from thinking that there is someone stroking a white cat in a lair somewhere, masterminding the whole operation. Very much in keeping with the nature of the crypto market, it is decentralised. They can be anybody. Anybody can launch a coin.

For example, there was a coin called Floki Inu, which was named after Elon Musk's pet dog. It put a bunch of ads on the Tube saying, "If you missed out on dogecoin"—the little token that made some people a lot of money—"then you can get floki". It was very difficult to find out who was behind that initiative. The people who spoke to the *FT* about it generally used only nicknames. In the end, the Advertising Standards Authority said that it was exploiting fears of missing out and cracked down on the ads. The truth is that anybody can launch a coin. To a certain extent, anybody can advertise that coin. It really can be anybody. That is the problem.

Baroness Taylor of Bolton: Geographically, is there a particular base anywhere?

Katie Martin: They are everywhere. Crypto mining, which is the creation of coins and the infrastructure behind the coins, has traditionally largely been based in China, Kazakhstan, Russia and places like that—places with cheap energy where you can rip through plenty of coal to power the electricity you need to create the coins.

The scams can be absolutely anywhere. I am not aware of any good data on where they are based. I figure that if we knew that we could find them and stop them.

Q73 **Lord Browne of Ladyton:** Is it true that anybody can transact in this area? From January 2020, firms that carry out crypto asset activities in the UK have had to comply with money laundering, terrorist financing and transfer of funds regulations, and they have to register with the FCA. They all had until the end of December that year to register; 80% of the companies that applied for registration withdrew their applications for registration, with the result that there are 33 fully registered companies and 16 with temporary registration going through the process. The transition process ends at the end of this month.

The FCA has powers. It is a criminal offence to trade without that registration. The FCA has a list of 220 firms, which I suspect are the 80% that withdrew, on the financial services web page, showing the companies that it believes to be trading without registration and without showing that they are complying with anti-money laundering and other regulations.

Here is a question. CryptoUK, which is the self-regulatory trade association in the UK for the asset industry, has 100 members. By definition, they cannot all be compliant with the anti-money laundering regulations because there are not enough that are complying to give them more than 100 members. Why has the FCA done nothing about that? All those businesses should be shut down because it believes they are trading and has provided not only their names but website details for them. In some cases, there are mobile telephone numbers. If I phone somebody and say, "Will you sell me some assets?", and they say, "Yes", they are trading. We should surely be able to at least shut them down. Not everybody can do this. Why are we allowing it?

Katie Martin: There is a lot to unpack there. One of the primary difficulties, as you say, is that the FCA has been imposing quite a thorough and intrusive process on platforms that want to register. A lot of would-be crypto trading platforms have dropped out of that process because it is too onerous.

There is a platform called Binance. At a certain point last year, the FCA effectively had to put its hands up and say, "Look, we can't supervise this entity because it operates in too many different jurisdictions and we don't have enough information about how it works and who these people are".

Binance would tell you, I think sincerely, that they are making efforts to rebuild a relationship with regulators and have accepted that regulation is a thing that they have to take seriously.

If you are in the UK, the UK entity of an exchange or trading platform can be banned, but there is nothing to stop you logging on to the US entity, an entity based in the Cayman Islands, an entity based in the Middle East somewhere or an entity based anywhere outside the UK and still buy the coins. You can go through a VPN and pretend to be somewhere that you are not to trade in the coins. That is why the issue is so thorny. There are so many different jurisdictions that it can at times be extremely difficult to figure out where the exchanges are, where the key executives are, who they are, how to contact them or whether they are fit and proper. That is the nub of the problem.

The other element, which the *FT* has written about in some detail, is that there are platforms that operate in this country and may have all the necessary regulatory documents behind them, but there are children trading crypto. You take an account, pretend that you are your mum, dad, uncle or whoever, and you punt around in these coins looking to make a bit of money. The process of actually figuring out who is trading these things is clearly failing in some instances.

Q74 **Lord Young of Cookham:** Is the payments sector, including all the financial services and the systems providers, aligned in its ambition to tackle fraud? Are there any barriers, regulatory or legislative, that stop that?

Related to that, a lot of the emphasis has been on the banks that send the money out under APP. Should we at some point focus on the banks that are receiving the money, which, by definition, have not done due diligence, because the money immediately disappears? Should they be part of the response to the fraud we have been talking about?

Ghela Boskovich: There is alignment across the industry, at least for those who have signed up to a code and who are part of the reimbursement model. It is not mandatory. There is no regulatory requirement for all payment service providers to be part of a code. There are also some limitations in sharing information across individual institutions.

There is a need for a co-ordinated effort of that information sharing when APP fraud is discovered or when push payment or general fraud is discovered. There is no centralised mechanism in which to report that, so that there is an alert across the entire network. That is missing, but a number of the institutions are part of the code, where they try to inform one another and make sure that individual consumers and small businesses that have been affected are duly reimbursed.

The challenge is that there is no regulatory mandate for that data sharing to exist in a centralised form around fraud. There are efforts across the board to improve some things called transaction risk indicators. Those are at the initiation point for the bank that is executing the payment, for

them to examine whether the context of that payment is within the normal scope or within a standard deviation of behavioural outlines from the merchant to the context of the payment or the purchase itself.

Those things are going through an evolution. We are moving from what we call merchant codes to something more like the payment context code. It will transform a bit of how the risk analysis is performed and the types of flags that will be waved in the risk analysis engines before the payment is actually sent. There is some co-ordinated effort on trying to stop the payment happening before it gets executed, yet post execution there is still no debrief or post-mortem of where the payment went wrong or what the transaction risk indicators might have flagged.

There is some breadth and room to create policy on a centralised information service across payment service providers on the fraud that they are experiencing. Part of it is sensitive commercial strategy, but there are some baseline data points that cannot be shared and should be shared. I think there is absolutely alignment across the industry to make sure that we do as much as we possibly can to tackle it up front. There are incredible losses, not only for the consumers but for the banks that have to make the consumer whole. A liability framework exists for making the consumer whole when something goes wrong with the payment, but prevention of that has better economies of scale and operational efficiency for the industry.

There is alignment, but there is no requirement for data exchange or sharing around fraud itself. There is room and scope for that to be played with.

Lord Young of Cookham: Is GDPR a problem at all in sharing data? Secondly, who is going to drive forward the process you have just outlined, whereby everybody takes part in the new data-sharing experience in which only some people are taking part at the moment?

Ghela Boskovich: Is GDPR adequate coverage or a preventive hurdle in order to make this happen? There is some analysis of the sharing of personal identifiable information and what the consumer owns. The consumer, for example, owns the information around the payment, but they do not own the analysis information or what happens after that information has been processed. That is the remit of the banks. The banks are then, at their discretion and according to their risk and governance structure, able to pull back.

GDPR would not be breached in terms of sharing post-analysis or payment analysis information. It would actually be breached if banks were to share the payment information in its singular form. That data payload alone would be a breach because it belongs to the consumer. The analysis of it belongs to the bank, and therefore it is at their discretion.

As to where the regulatory remit or gift ought to sit, there is an interesting co-ordination between the current regulators that oversee payment systems already—the PSR. To a certain extent, I do not think

the FCA would be in the right position to co-ordinate that, as it looks at individual firms and the supervision of individual actors in the market. The co-ordination of the payment systems as a whole, and those who are on or are part of the value chain of the payment systems, has a natural home at the PSR.

What is interesting is that the PSR is looking at improving the adoption of, or the signing-up to, the code that already exists. It is currently undertaking a consultation on push payment fraud and what it can do not only to strengthen data sharing across the institutions but to promote the code and maybe even push mandatory sign-up for the code. There is still some debate around whether that is in their gift. There is a concerted effort being undertaken by the PSR that merits further examination by this particular committee of what it is doing to ensure that payment service providers across the entire market are acting in a co-ordinated and orchestrated manner around fraud prevention.

Lord Young of Cookham: Thank you very much.

David Pitt: Building on what Ghela was saying, I think there are some salient points in answer to your question, Lord Young. It is really important that we think about how we detect and prevent, as Ghela was saying, before we get to reimbursement. The sharing of the right level of data to allow banks and building societies to detect potential fraudulent payments has to be one of the things we tackle.

We are working closely with the PSR, and we are also working closely with HMT on the right legislation to make sure that there is the right legal framework around the reimbursement. The code just now is voluntary on authorised push payments; Regulation 90 of the Payment Services Regulations 2017 says that if it was an authorised payment there is no requirement around reimbursement. That is why it is a voluntary code.

The code is being looked at, but I have to say that it has to go hand in hand with detection and prevention. We do not want to get into a situation where we are not trying to stop these frauds and payments happening before they hit our payment rails and systems. It has to go hand in hand with reimbursement. It has to be the right legislation. It is about the right sharing of the right data to be compliant, and allowing the AI tools and systems to have adequate data to prevent a fraud or prevent a payment hitting our payment rails and processing it. It would pick up on the point that, when a payment actually does get through, it allows banks and building societies to freeze accounts and hold that payment, to stop it moving, whether it is on to crypto or indeed to another account.

Those will be the important elements that we need to focus on. It is the right detection, the right prevention and the right reimbursement supported by the right legislation to be able to support it. It has to be appropriate reimbursement and it has to be consistent. That also applies to how we educate consumers to take heed of any warnings, and how we help them to understand potential fraud.

Ghela Boskovich: To build on what David just said, there is another component that is voluntary but has an interesting effect on the authorisation component of a payment, which is confirmation of payee. It is currently in place for only a few of the payment service providers in the market, primarily the CMA9—the nine largest banks.

There are warnings before the authorisation is pushed and before we click on the button. To a certain extent they are effective, but they require additional fine-tuning. It is not a matter of being socially engineered to click okay on anything, irrespective of the warning. There have been a number of studies done on the effect of this in confirmation of payee. It has an effect. It is when the warning is triggered, how it is triggered and the frequency with which it is triggered. That merits further examination. It also merits an approach that is not necessarily voluntary. It is the larger banks that are funding the system. We are now looking at scaling up to the second version of confirmation of payee and looking at the scope of payment service providers that will be signed on to it.

There is an essential component around confirmation of payee that is fraud preventive, and it is important. I failed to address the component of the receiving bank being able to take action before the money is either settled or moved elsewhere. There was a quite interesting and well-documented case of a challenger bank being the recipient bank. It was Barclays and Monzo. There were not enough parameters for the receiving bank, or not enough action taken on the receiving bank, to follow through on appropriate KYC and AML compliance requirements.

There is scope for the receiving bank. I am not quite sure how the policy would be framed, but there is certainly the initiator, the executor of the payment, and the recipient of the payment, both of which in a liability framework should be accountable to a certain extent. There is still scope for confirmation.

David Pitt: Just to build on Confirmation of Payee, we have had over 800 million hits on confirmation of payee since we started. That is about 1.5 million hits a day on confirmation of payee. It is not the silver bullet, but it has an impact on APP fraud.

To build on what Ghela said, there is 96% current coverage of the market. That is increasing in phase 2.As we launch that, we have a list of 18 potential additions to confirmation of payee from providers. It is going to cover the majority, if not all, of the market.

Q75 **Lord Sandhurst:** As we have heard, this is all very difficult. We heard how crypto assets are supposedly regulated at national level with the FCA. We have heard about Binance and another 50 or 60 people who failed to make it on to the FCA's list of registered crypto asset people.

The first thing is that some of those may not actually be baddies. How do we bring them into the fold? How do we police them? It strikes me, listening to you all, that there are two levels of operation. There are perfectly bona fide people like me or anyone here today who may want to

have a crypto asset or may want to gamble on cryptocurrencies. We deserve protection, but if I am a villain who just wants to hide my assets under the counter, I do not need protection.

Should we be focusing on having, so to speak, regulation and making it absolutely clear that you are regulated? If you are bona fide but you just want to have a bit of a flutter on this stuff, fine, you deal with them. I am not saying that we should not bother about the rest. That is for the law enforcement people to go after, to seize their assets.

Is that a philosophical approach or a cultural approach that would make protecting the people who need to be protected easier, rather than just going after everybody?

Katie Martin: That is a very sensible way forward. Not all trading platforms are baddies, as Lord Sandhurst put it. Not all potential punters on crypto assets are baddies, by any stretch of the imagination. There is a large chunk of the crypto market—lots of the intermediaries, technology providers and all the rest of it in the market—that are desperate for more regulation because they want to be able to distinguish themselves from the bad actors. I am extremely sympathetic to what they are trying to do.

The fact is that the warnings are not getting through to vulnerable consumers. In 2021, the FCA said that under one in 10 potential crypto buyers heard its warnings about you being liable to losing all your money with no recourse to any deposit guarantee scheme if something goes wrong. About 15% of owners of crypto think they enjoy similar protection to the compensation schemes you would see in other assets. That is the element that worries me.

In January, the Treasury said that it would crack down on misleading crypto promotions, with stricter ad rules and FCA oversight over most promotions, in line with what you would see in, for example, stock markets. Advertising platforms or schemes would have to seek authorisation ahead of time, not just put the ads on the Tube and wait for the Advertising Standards Authority to send them a mean letter. But it is not going to come into place before 2023, and the Advertising Standards Authority has said that it is worried that bad actors will "make hay" in the meantime. Frankly, so am I.

Lord Sandhurst: I have never ventured into this field, so I am going to ask a silly question. You mentioned Binance, but it does not matter who they are. If I want to be up there on the internet, is there a platform that Binance sits on, or is there not? In other words, if I am sitting at home with my laptop and I want to go there, I must go through something to get to Binance. Could we attack or get at the people who allow an unregulated provider and say, "You are strictly liable and unless you let on people who are regulated, and you let an unregulated one on, sorry, you have to take all the losses of people who are defrauded"?

Katie Martin: This has certainly been one of the avenues that the FCA has been using to talk to the payments organisations that are the on-

ramps and off-ramps of putting money into and out of the crypto market. They are regulated entities. This is a point where regulators can have real influence. I am afraid that, once the money has gone into the crypto system in a jurisdiction that we cannot see or that we cannot affect, it gets more complicated.

Lord Sandhurst: I might have gone through an American thing to get to it because I could not get it in London, and I was greedy. Is that right?

Katie Martin: You could have got it anywhere, and you might not even be aware that you are using a service that is domiciled in a different jurisdiction.

Lord Sandhurst: Fine. I will not ask any more. I just wanted to highlight the complexity.

Katie Martin: You sound like you are tempted.

Lord Sandhurst: We could spend time, but I was interested in how one might try to protect the innocent.

The Chair: I hope no one is encouraged to start trading in crypto as a result of this session. We will move on and backwards. Viscount Colville has a question.

Q76 **Viscount Colville of Culross:** I want to look at the way that credit card companies and banks take fraud as part of a cost of doing business. Is there a difference in perception of the risk from fraud depending on the sector? Does that affect the way that companies invest in anti-fraud technology?

Ghela Boskovich: There is a fundamentally different approach between card fraud and direct payment or open banking fraud—the APP fraud—in part because of the insurance that is already built into the card cost itself. There are seven different actors in a card payment. Each one of them has a cost that is associated with fraud or with loss or chargeback. Each one of them passes that cost on to the merchant.

For example, you are probably very well aware of the card fees that come with each payment processing. Those are also passed on to the end consumer. Section 75 of the Consumer Credit Act allows for that chargeback and the protection that, irrespective of fraud happening, the consumer will be made whole. That is a component in a cost structure that is already embedded in the cost of the payment itself, and fraud is accepted as part of that cost. An incredible overhead already exists in the insurance, but that additional cost is baked into the payment. It is borne by the merchant and by the consumer in order to cover those losses.

The open banking payment structures, where they are doing bank-to-bank account, have been designed with a different sense of security. They have secure customer authentication baked in from the very beginning. We now see in cards that a secure customer authentication

component is required, and we have until 14 September for that to be fully live in the UK market.

The cost of the open banking payment is fundamentally different. It is much lower. It is pennies and pence on the pound in comparison to what a card payment would cost. The notion of taking the transaction risk indicators, as well as the fraud analysis and the risk analysis, right up front in the beginning of the payment is a baked-in component of that cost, but it is meant to ensure that the payment is authentic and real and has merit before it is sent across the payment rails.

There is an upfront analysis for that payment, where it is not necessarily happening in a card space. The upfront analysis, along with the security credential requirements in order for that payment to be initiated, are baked in, but the processing of the particular payment is also much lower. The overhead does not exist. There is no equivalent insurance component under Section 75 for an open banking payment, but there is reason for that. It is justified, and in fact the PSR examined that particular question and ruled that it was not necessarily required for the market at the moment. It did not make sense.

There is a fundamental difference in the cost. The CRM—consumer redress model—overhead that exists for open banking payments, alongside the confirmation of payee and the code, is borne by the payment institutions themselves. It is also voluntary, but there is a commitment across the industry for them to make the consumer whole if the payment has been fraudulent. It is a different approach, in the sense that the end consumer is not taxed with the overhead cost of that coverage.

Viscount Colville of Culross: You just talked about the credit card companies passing on the insurance fee to the end consumer. Does having that acceptance of fraud baked into the system make the credit card companies complacent about fraud and about fighting fraud, because they know they already have that payment baked in and dealt with?

Ghela Boskovich: I do not think it makes them any less complacent, but there is a difference in the consumer experience or the customer journey when you are looking at additional barriers to making that payment. For example, with the secure customer authentication journey for cards, a significant number of payments are not finalised because of that. It is between 15% and 26%, depending on the market. We are looking at the UK and Europe. Those particular transactions, because of that additional security requirement, which is supposed to prevent fraud, mean that the payment is not executed or is not happening.

I do not think the card companies are necessarily complacent, but those baked-in overheads are part of the administration cost of having such a complex set of steps in the value chain. The scheme requires an extraordinary amount of administration. Part of the scheme coverage is the card fees. Open banking payments, or APP payments, do not have

the same sort of scheme requirements; those actors do not sign up to the scheme. The banks do not participate in a direct bank-to-bank scheme that requires that overhead and that insurance. Cards do. It is a fundamentally different framework for each of the two sets. I do not think either is particularly complacent about fraud. It is just that the cost of the scheme versus non-scheme is extraordinarily different.

Viscount Colville of Culross: David, do you have anything to say about that, and whether or not more could be done by various sectors to try to introduce a counter-fraud technology?

David Pitt: I agree with Ghela that fraud is in no way accepted. Certainly, the banks and building societies who use our payment rails invest heavily in trying to detect and prevent fraud. On your question about what more we can do, it definitely comes back to sharing the right data in the right manner, to make sure that investments around the right tools are supported by the right data to get the right protection and stop potentially fraudulent payments coming to the payment rails.

There has been a lot of talk about slowing down payments. It is critical that we take a step back to think about how we use the tools in the investment and the data to slow down riskier payments, and control and help investigate those payments. This is not—I am really clear about this—about slowing down the 1,500 payments per second, therefore having a massive impact on the UK economy. It is about identifying payments before they reach the payment rails and holding those payments while making the required investigation to eradicate them.

It also plays back into the point about reimbursement at the end, if a fraud happens, and having a clear, consistent and managed reimbursement policy. Certainly, we have regular conversations; we collaborate, whether it is with the banks themselves or UK Finance. It is critical that we pool that collaboration right across the industry, and beyond, to try to tackle this.

Viscount Colville of Culross: Kate, do you have anything to add?

Katie Martin: It is not really my area, but that all sounds extremely sensible to me. A point that David raised earlier is important, which is about educating consumers to the risks. That is certainly a slice of what is going on in crypto that is exceptionally important because it has just hit the national psyche. People do not quite understand the risks that are out there.

Viscount Colville of Culross: Thank you very much indeed.

Q77 **Lord Allan of Hallam:** I want to pick up on something that you have mentioned a couple of times, David, about using data to find potentially fraudulent transactions. Could you go out on a limb and talk about how much upside you think there is in the use of technologies such as artificial intelligence, particularly in the area of authorised push payments? How much are we betting on it, and what kind of results do you think we

might get from it?

David Pitt: One of the things I would say is that we are working closely with UK Finance. UK Finance are doing a proof of concept on enhanced data and what they are actually doing, which is really important (we collaborate), is looking at past fraud, and if we had more data, would that have prevented it. That will give us some insight.

We all know from our experiences that, if you have good technology and AI machine learning, it is all about the adequacy of the data it is provided with. That will help us not only to prevent and detect but to get into the ring-fencing of funds before they move on. It definitely has to be the way forward, on top of the education piece.

We have seen anecdotally, from things like confirmation of payee, that fraudsters move their business to providers who do not have confirmation of payee. You can see how this all moves around. That is why it is critical that the data is there, so that we can stay one step ahead, detect, prevent and, hopefully, reduce, and that where we cannot we adequately compensate.

Lord Allan of Hallam: Recognising everything you have touched on already, it is a cat and mouse game. As you move, they move. Can you describe the challenge around that and whether you think you can stay ahead of the fraudsters?

David Pitt: I am sorry to use the same example, but confirmation of payee is a great example. It is not a silver bullet. It attacks some APP fraud and helps the victim to check that they are sending the payment to the right place, rather than not having that.

What we have found is that the one step ahead is critical. We have talked about how we use the end-to-end journey. It is not just about the payment journey. It is about the online journey. As I said at the start, 70% of our authorised push payment fraud comes from an online journey. As a nation we are choosing digital first, so the education piece is critical. It is important that we collaborate along the full journey, and not just the financial services part of it, with banks and payment services.

Lord Allan of Hallam: Thank you so much.

Q78 **The Chair:** Picking up on that, David, we have heard evidence from other witnesses about the whole system needing to be involved in tackling fraud. Reading between the lines of what you have just said, I think what you are saying—correct me if I am wrong—is that companies such as the social media platforms, the tech platforms and the telecoms companies have a role to play in all of this as well. I do not want to put words into your mouth, but is that basically what you are saying?

David Pitt: Yes. At Pay.UK, we take fraud really seriously; it is one of my key targets and key focus areas. So do our customers, the banks and building societies. It plays to Lord Allan's point. We have to look wider. To take confirmation of payee, the fraudsters weaponise that and say to

victims, "You will get this prompt". They are almost turning it on its head. That is why, Chair, we have to look at it end to end and collaborate right through the journey rather than just in the financial part of the journey. When it gets to us and we process it, the fraud has already happened. That is why it has to be prevented further up the journey.

The Chair: I accept that. I appreciate that you are not the only payment systems operator. There is a whole payment systems ecosystem, and Pay.UK is part of that. Do you feel a responsibility for helping to tackle that fraud?

In your letter to us that you sent yesterday, you said quite rightly that, although the faster payment system is a huge benefit to the UK, it has also been exploited by the fraudsters. You have just given another excellent example of confirmation of payee, which is also exploited by the fraudsters. You are right to say that fraud is committed up stream, if you like, but the payment systems operators have to be a key part, presumably, in helping to stop or retrieve the money that has been taken away fraudulently.

Do you feel that you and other payment system providers are involved enough in the efforts, whether that is the Economic Crime Strategic Board or the national cybersecurity strategy? Are you involved enough in all those processes and conversations with government and regulators?

David Pitt: Yes. Breaking down your question, first, we take fraud really seriously. At the end of the day, the emotional and financial impact on a victim is unacceptable. Although, as I said at the start, transaction levels on faster payments or in fraud are 0.0067%, that is not to belittle the impact. We take it very seriously.

The Chair: I appreciate that it sounds like a small percentage, but it is billions of transactions. It is a large number.

David Pitt: It is a large number that we must tackle. In the first half of 2021, there were 183,000 transactions. We have to reduce and tackle that. That is why I mentioned collaboration and working across the industry. We are working closely with HMT on the right legislative liability set-up. We are also working closely with the PSR on the right reimbursement approach. It has to come from detection, prevention and then reimbursement. It has to come in that order.

The Chair: Are you working with the Home Office and the police?

David Pitt: There is more we can do there. There is always more we can do. We are willing to get involved. It comes back to the point about the data and how we use the data that we have from our transactions to protect individuals, but use it in such a manner that we can see the trends and use the technology so that we can see whether banks and building societies have trends, and get ahead of that. As you say, we can use that to work more widely with different parts of the ecosystem to help tackle fraud.

The Chair: Thank you. Ghela, do your members feel that they are sufficiently involved? As a trade body, are you involved in the conversations, not just with perhaps the normal people you deal with—the financial services regulators or the Treasury—but with police forces and the Home Office, as required? Do they ask you for assistance and insight?

Ghela Boskovich: To be fair, no. In part, that is because our members that act as payment initiation service providers do not necessarily execute. They inform that a payment should be made. They give an instruction. Their accountability has a finite limit. They are not at the point when the crime happens. They give an instruction and it is on the receiving bank of that instruction to make the decision whether or not the payment goes forward. There is a limited amount of accountability that could be had there.

The payment initiation service providers—the fintechs—have every incentive to work only with merchants that have been vetted. They do an extensive amount of KYC and due diligence on the merchants with whom they work. They have to be connected to those merchants' banks as well. There is an entire structure that provides them with an incentive to work only with reputable merchants. When a merchant offers an online banking option as a payment point, they have gone through a fairly rigorous review.

There is incentive in the market to do the right thing. Those fintechs understand that one bad actor spoils the entire barrel, so there is alignment there. I suspect that working with the police or crime investigation only happens on an individual member-to-member basis. They are not particularly willing to share that with the trade association as a whole, so I have no insight other than that.

Q79 **The Chair:** That is very helpful. Thank you. Finally, is there one recommendation? David, you said several times that you take tackling fraud very seriously. Ghela has just talked about members, rightly, not wanting to be caught up in fraud. Kate has been very helpful in talking about the crypto landscape.

Is there one recommendation in the areas you look after that you think we, as a committee, should make to government or regulators that would mean we begin to tackle fraud, which is now the largest cause of crime in England and Wales?

David Pitt: First, there is the work we are doing with HMT in changing the legislation to make sure that we have the right legal framework to set up the correct reimbursement model with the PSR. That is a clear piece we are working on. HMT has indicated that the right regulations will update and change. I am probably being a bit cheeky, but I would say that that has to be supported, as I mentioned in a number of my answers, by detection and prevention. Therefore, you would have a model of incentive around detection and prevention and the right data, supported by the right reimbursement for victims of fraud.

Lord Sandhurst: Could you send us what you have in draft at the moment, David, so that we can look at it?

David Pitt: I am happy to send you written confirmation of the work we are doing.

The Chair: Terrific. Thank you. Ghela, do you have any key recommendations for the Government or the regulator?

Ghela Boskovich: Yes, I think primary legislation for a framework that encourages data sharing—the prevention component—is absolutely essential, and compulsion to participate for all payment service providers. There is a distinct lack of compulsion when it is market-led and voluntary that does not make for ubiquitous information or complete data sharing. I think that is an important component. The other thing is an emphasis on real consumer education and awareness. Kate mentioned that only 10% are really hearing the message. Something needs to change to improve that.

The Chair: Thank you. Kate, a recommendation?

Katie Martin: Two things, if I can be cheeky. One is that there is a real groundswell of opinion among international banking regulators that enough is enough, and it is time to really tackle the numerous problems with the crypto industry, whether it is around sanctions of Asia and Russia, consumer harm or the environmental impact of crypto. It is crucial that the UK is extremely plugged into what the international community is doing on this. Because of the jurisdiction issue we were talking about earlier, it does not matter if one country manages to do it well. The bad actors can simply move somewhere else. International communication is key.

The other thing is to get on with it. Raise awareness. Make sure that people are aware of the risks that are inherent in crypto. This week, Crypto.com signed up as the sponsor of the football World Cup, which is likely to be a big breakthrough moment in consumer engagement with crypto. It would be a shame if we missed the opportunity before then to get the risks through to people.

The Chair: Thank you all very much indeed for your clear evidence. It has been very helpful. David has already agreed to write to us on something, and if, on reflection, there is anything further you want to make the committee aware of, please feel free to write to us. I now formally end the meeting. Thank you.