Transpact.com – Written evidence (FDF0061)

Fraud is the act of gaining a dishonest advantage, often financial, over another person. Under the Fraud Act 2006, a person can commit fraud by false representation, by failing to disclose information, or by abuse of position.

Fraud Landscape

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

A) Individuals

- Fraud by impersonation over telephone by fraudsters pretending to be the victim's bank (exacerbated by inability to fully stop number spoofing in the UK before 2025, but a critical problem even when number spoofing has been halted).
- Fraud by impersonation over the telephone by fraudsters pretending to be the Police or other authority.

  The reason for the above two vulnerabilities is that individuals and businesses have been 'groomed' by UK banks and UK utilities to receive a phone call from the bank/utility and for the bank/utility to ask the call recipient to divulge confidential information for data protection reasons to prove the call receiver's identity.

  This is disastrous practice, as neither an individual (nor a business) can know whether they are being called by the genuine bank/utility or by a fraudster impersonating them.

  All such organisations must institute a change of practice, whereby when they wish to speak to a customer by phone, they contact the customer (by phone or other means) and ask the customer to phone back on a phone number that the customer can obtain independently and securely (say off the organisation's public website or off an old invoice).

  A reference should be given, and the call-back must be answered promptly (without hours of waiting in a queue) to avoid customer inconvenience.

  Only when consumer and business practice is changed to make this the norm will impersonation fraud be ended, as then individuals will only ever speak to genuine organisations, and the current plague or phone impersonation will no longer be possible.
- Fraud by website impersonation - most individuals are not able to distinguish a genuine website from an impersonating website (understanding a url is beyond most individuals, and even for experts, similar characters can make imposter websites almost unstoppable). An example of the former would be fake website Natwest.BadSite.com/internet-banking - most individuals would not spot this as a fraudulent link, whilst an expert would immediately know this was dangerous.

  An example of the latter is L1oydsBank.com - where even an expert may not notice that one of the letters has been changed to a similar looking character.

- Fraud by unregulated companies.

  The UK regulatory environment has a perimeter that leads to products being designed so that they fall just outside the perimeter, and individuals who believe they are protected by regulation are not.

  For example, investment in wines, which is completely unregulated.

  The FCA does not seem particularly bothered by the confusion, and whilst it makes noises to mention that it does not and cannot take action against firms operating outside the regulatory perimeter, this message is not understood by most individuals who as a result stand ripe for fraud.

  The responsibilities of the FCA need to be increased to mandate the FCA to ensure that the public is clearly knowledgeable about the FCA's perimeter.

  It would be even better to extend the FCA's perimeter specifically with an anti-fraud remit to include all cases of investment, whether regulated or unregulated, so that individuals would know that the FCA was acting to prevent fraud from occurring in otherwise unregulated areas where most individuals naively expect the FCA already to be acting.

- The Payment Services Regulations 2017 requires the FCA to register and regulate all online-marketplaces which handle client payment (with a very few exceptions). Doing so would obviously assist in the prevention of fraud through these online marketplaces, which are becoming the mainstay of current commerce.

  The FCA has failed in its legally required mandate, and there are a very large number of online marketplaces in the UK handling client payment without FCA registration and regulation.

  The FCA needs to be held to the requirements set on it in law by the Payment Services Regulations 2017.

<u>B) Government</u>

See also notes on banks and utilities in A) above, which also applies to Government

<u>C) Businesses</u>

- All points mentioned in A) above also apply here.

- Specifically to UK banks - a very large amount of fraud is due to banks having to accept UK Driving Licences as proof of identity.

  A UK passport has an encrypted chip in it which is cryptographically verifiable to assure the passport is genuine. The chip also has a copy of the holder's name and photo and date of birth embedded into it, so with a UK passport (or similar trustworthy other foreign passport) the identity of an individual presenting such a passport can be verified with close to certainty.

  However, some people do not have a passport, and so a driving licence is commonly supplied to prove identity instead of a passport.

  Driving licences have no embedded chip, and are relatively easy to forge.

As a result, by presenting a forged driving licence or similar document, it is relatively easy to defraud a bank and open a bank account using false identity.

Only when UK driving licences have embedded chips in them similar to passports will false identity bank account opening end in the UK - as then the vast majority of documents provided (passports and driving licences) will be verifiable.

Any account opened with other documentation (to prevent de-banking of those without passports and without driving licences) should be treated as at-risk.

Until the security of driving licences are improved to the standard of passports, fraud will proliferate in the UK as fraudsters will continue to be able to open UK bank accounts with false identity.

2. 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?

Two areas of greatest concern due to technological development currently known and expected are:

- The ability of technology to make a remote fraudster appear and sound in every way like another person being impersonated - even over a live video link.

  This will make it harder and harder to establish safe communication and instruction between client and supplier.

- Global finance depends today on the assumption that a very large number, which is made up of two very large numbers multiplied together, cannot be broken down into the two large numbers which are its only two factors.
  For example, all commerce over https (much of the modern world's commerce and communication) relies on this assumption.

  At some point, this assumption will fail, as quantum computers will become able to trivially solve these problems.

  There is a significant chance that this point will occur within the next 10 years.

  If so, mass fraud will immediately become possible and expected, as all secure communication over the internet will immediately become open and interceptable and readable and changeable.

3. Is fraud and its victims treated as a priority? If not, what are the reasons for this. The Committee is particularly interested in responses that can explain any barriers preventing effective counter-fraud cooperation within Government, law enforcement, the public sector and the private sector.

The largest barrier to effective counter fraud is the fact that a significant (probably majority) segment of fraud perpetrated on UK victims takes place from overseas via the internet and phone.

UK police and regulatory bodies have close to zero enforcement powers overseas, and certainly cannot perform effective investigations on fraud committed in the UK from there.

As a result, if UK fraud involves an overseas component (and many and probably most do) the Police and regulatory bodies mostly will not spend any resources at all investigating, and will simply write-off the fraud, as they expect that investigation will be too difficult.

Of course, the fraudsters know this and see this as a green-light to continue and expand their frauds, which they do.

Only when a significant and well funded special law-enforcement team is set up by UK Government/Police dealing with overseas fraud perpetrated in the UK on UK citizens, will such fraud begin to stop. Note the cost of this team, whilst huge, would be much, much less than the amount the UK is currently haemorrhaging to overseas fraudsters annually, so economically this step is indisputably necessary.

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

Barriers:

a) UK regulators absolute power stops at the geographical border; the fraud doesn't - See Question 3 above.

Action to Tackle Fraud

5. How effective is the current structure for policing fraud? How successful are the City of London Police, including Action Fraud and the National Fraud Intelligence Bureau, at executing their role as the lead police force for fraud?

6. Are sufficient resources available to Government organisations (such as the Serious Fraud Office and Crown Prosecution Service) and wider police forces to tackle fraud and support victims, and how should this be addressed if not? Answers need not be limited to financial resources.

Knowledge of the tiny percentage of frauds that are taken forward after reporting to ActionFraud answers this question (the vast majority of the rest are simply ignored for effective purpose).

7. 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?

The inability of large social media companies to stop themselves receiving revenue for posting adverts for fraudulent investment schemes proves that the private sector generally will act to maximise its own revenues and not act to effectively protect consumers.

It took an enormous amount of protest for the hopefully forthcoming Online Safety Bill to prevent large social media companies from continuing to do so.

So despite many private sector organisations 'talking the talk' to prevent digital fraud, in reality Government regulation is required to make them 'walk the walk'.

Specifically with respect to private sector banks, when private sector banks allow digital fraud to occur they often end up money laundering the proceeds of crime through their accounts.

The FCA has been particularly weak in performing its legally mandatory role of ensuring that the banks do not money launder these funds - the FCA has looked the other way, and allowed the UK's banks to continue laundering these funds.

8. 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?

9. 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?

Legislative Remedies

10. What is your assessment of the Fraud Act 2006? What has been the impact of the Act and is it having any unintended consequences; if so, what are these?

11. 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

Allowing FCA authorised financial and payment firms to communicate together to share fraud information to prevent crime would be a huge step forward to help prevent and stop and remedy fraud.

At the moment, due to 'tipping off' laws, each financial and payment firm must keep suspicion of fraud information to itself, and cannot share.

This is necessary to a small extent to prevent the fraudsters from learning that they are under investigation, but the damage caused by the siloing of information is much greater than the benefit.

12. Is the current system in place for prosecuting fraud cases working effectively? If not, what are the key barriers to prosecution?

Authorized Push Payment (APP) fraud is one of the main and largest frauds occurring in the UK today.

Authorized Push Payment (APP) fraud is one of the main and largest frauds occurring in the UK today.

At this time, for nearly all APP fraud cases occurring today, the payee's bank is at least partly at fault for the APP fraud.

This is because the payee has either opened an account at the payee's bank with false ID, or the payee is operating as a mule account.

In the first case, the payee's bank accepted false ID, and is therefore partly at fault in the loss.

Now that machine readable passports are commonplace, which allow verified identity conformation and photograph to be read off the passport with high certainty and confidence (as they are digitally and cryptographically signed), there is no reason why any BANK should today open an account with false ID. It

should be extremely difficult for a criminal or fraudster to do so – way beyond the capabilities of the ordinary crook.

The Government needs to be lobbied so that driving licenses also become machine readable and crypto-signed, as at present driving licenses are easily faked. This is a Government weakness, and the Government should immediately address this issue, so that bank accounts can be opened for customers who have a driving licence but no passport).

In the second case, the payee is acting as an account mule.

Account mules are always caught by the Police, as they are committing crime in the open and do not hide their crime – that is the nature of an account mule.

The defence in Court by account mules – which is effective at present – is they did not know they were doing wrong.

As a result, the Courts will not prosecute, and as a result the Police will not act (it is not worth their while, with no expected penalty resulting).

And as a result, account mules are free to continue unabated in a tsunami of fraud.

This is all the result of banks' failure to alert their clients to the illegality of account muling.

This author has never received any communication from any of the various banks I personally bank with (and I personally bank with a few, to help me understand consumer experience with their banks) instructing me that I cannot receive a payment in to my bank account for another party.

If I was instructed by my bank that I can only receive payment into my bank account on my own behalf, and never for another person or another party, and that such receipt was actually potentially illegal and money laundering, then I would be aware that account muling was illegal. If I was told at the same time by my bank that such receipt can well lead to fine or prison sentence, then I would take note.

But I have never received such a message from any of the many banks I bank with.

As soon as banks take action to directly inform all their clients that the client is not allowed to receive payment into their bank account for another party, and that such receipt may be money laundering and subject to fine or prison sentence, then Courts will immediately on the basis of these warnings start prosecuting account mules with significant sentences (as the defence of 'I did not know' will no longer be available).

And Police will immediately start arresting and taking to Court account mules, as the Police know they will have an easy conviction (and this will make them look effective, and greatly improve their crime statistics).

And account muling will stop, because no account mule will continue knowing they are committing crime in the open, and will be certainly caught and prosecuted.

As payee banks have not made clear to their clients that account muling is not allowed and potentially illegal, the payee banks are all at fault if their accounts

are used for account muling (the bank is also in breach of the Money Laundering Regulations 2017 – but that is a different matter).

So if an APP fraud takes places, and the payee turns out to be an account mule, then it is correct that the payee's bank should be liable, as the payee's bank did not warn and make crystal clear to the payee that acting as an account mule was not allowed and possibly could cause fine or imprisonment (which in turn allowed the account to be used to defraud the original payer).

The upshot is that a payee's Bank is currently almost always at fault (at least partially) in an APP fraud (whether due to false ID or account muling).

13. Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful? Respondents may choose to refer to penalties imposed by the judicial system or by specific sectors.

See answer to Question 12 above.

Best Practice

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

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

Improve UK driving licences so that they have a similar encrypted security chip (with encrypted and digitally signed name and photo) as UK passports do - this will largely eliminate impersonation fraud when opening a bank account with false ID.

And force the FCA to prevent money laundering by account mules in the banks that the FCA regulates, by the FCA forcing the banks to educate their customers that account muling is illegal and can lead to a prison sentence.

26 April 2022