appg financial crime and scamming

YOUNG VICTIMS OF FINANCIAL CRIME INQUIRY

2018 REPORT

www.appgfinancialcrime.org

FOREWORD

FRAUD IS THE VOLUME CRIME OF THE 21ST CENTURY AND, UNLESS STEPS ARE TAKEN TO ARREST ITS GROWTH, THIS CRIME WILL CONTINUE TO GROW.

The most recent Office of National Statistics England and Wales Crime Survey showed that there were over three million incidents of fraud in the year ending March 2018[1].

Fraud is the volume crime of the 21st century and, unless steps are taken to arrest its growth, this crime will continue to grow.

The common perception is that it is the elderly who are most at risk from scams. This is not the case. In fact it is young people in the UK who are one of the most susceptible and at risk age groups to online fraud and scams.

This is a worrying development when you consider that young people are also the most frequent users of the internet. Over 99% of 16-24 year-olds in the UK were recent internet users compared to 41% of adults aged 75 years and over[2]. Evidence would suggest that just because young people are digital natives and comfortable online, does not mean that they are fraud savvy, with young people estimated to be losing up to three times as much to fraud compared to their parents[3].

Moreover, figures from Cifas show there has been a 24% increase in young people under 21 being involved in fraud either as a victim or perpetrator from 2015 to 2017.

This is why the All-Party Parliamentary Group on Financial Crime and Scamming decided to look into the issue of young victims of financial crime.

From the evidence gathered from written and oral evidence sessions, this report puts forward six recommendations for government, the education sector, law enforcement, industry and individuals to help prevent more young people falling victim to fraud and scams.

I commend this report and its recommendations to politicians and policymakers of all hues. The scale of this threat is too large, and the risks to young people too great, to be ignored any longer.

Conor Burns MP

Chair, APPG – Financial Crime and Scamming

[1] *Cottrill, and Nina. "Statistical Bulletin: Crime in England and Wales: Year Ending March 2018." Office for National Statistics, 2018, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018*
[2] *Statistical Bulletin: Internet Users in the UK: 2017." Office for National Statistics. Accessed July 20, 2018. https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017*
[3] *https://www.getsafeonline.org/news/caught-on-the-net/*

EXECUTIVE SUMMARY

The recommendations set out below arise from the inquiry undertaken by the All Party Parliamentary Group on Financial Crime and Scamming.

The background to the inquiry is the significant increase in the number of young people who have fallen victim to fraud together with an increase in young people drawn into crime who allowed their bank accounts to be used to launder the proceeds of crime[4].

The APPG has been keen to focus on how to educate young people so that they have an increased awareness of the danger of oversharing information and are more wary of adverts on social media that promise "easy money" by allowing their bank accounts to be used to transfer monies.

The inquiry received evidence from 12 organisations including financial institutions, law enforcement, a consumer group, an identity assurance provider, and a charity.

As a result, the following five recommendations have been made:

1. That a greater focus on education and awareness programmes is given by the education sector, government, industry and the third-sector.

- Counter-fraud education should be introduced into the national curriculum across all UK schools for those aged 11-16 years old (Key Stage 3 and above).
- Parenting courses – available from a range of providers - should include a module on protecting their children from financial abuse.
- Government should work with industry to make preventative advice available to parents of students attending full-time education.
- Educational establishments should consider holding counter fraud events at teachers' open evenings.

2. Social media platforms should be proactive in preventing scams from being promoted on their platforms and raise awareness amongst their users:

- Social media organisations should do more to warn young people of the dangers of oversharing information online and of the practice of those who recruit 'money mules' through social media channels.
- Social media channels should also be more proactive in vetting advertisements promising "easy money".

3. Law enforcement should have dedicated resources focused on the investigation and disruption of money mule networks.

MONEY MULES

Money mules are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts. Money mules receive stolen funds into their accounts, which they are then asked to withdraw and transfer to a different account, keeping some of the money for themselves[5].

4. That the Sentencing Council should issue an amended guideline on fraud identifying the corruption of a young person recruited as a money mule" as an aggravating factor for the purpose of sentencing.

5.That young people should be encouraged to report instances of fraud, either where they are a victim or where they are being groomed to take part in fraud such as a being a money mule. This will help to develop a better understanding of fraud in the way it impacts young people.

[4] *Fraudscape 2017. Cifas, 2017, www.cifas.org.uk/secure/contentPORT/uploads/documents/reports/External-Fraudscape%20report%202017.pdf*
[5] https://www.actionfraud.police.uk/fraud-az-money-muling

INTRODUCTION

This is the first report to be produced by the All Party Parliamentary Group on Financial Crime and Scamming and is published at a time when official UK government statistics show that fraud is now the most prevalent crime in this country with over three million frauds committed in England and Wales alone[6].

In recognising that fraud is at epidemic levels there are undoubted challenges for law enforcement as well as the private and public sectors, government and citizens.

The thrust of the recommendations in this report are on delivering protective and preventative counter-fraud messaging to young people at a time in their lives when they are susceptible to a range of influences, both good and bad, through peer pressure and their interaction on social media channels.

Young people are being exposed to fraud either as a victim or perpetrator at a much younger age, driven by their online activity. Between 2014 and 2016, there was a 34% increase in the number of young victims[7].

As evidence from Yoti shows, young people are also much more likely to lose important identity documents. This could result in them being at increased risk of identity crime and fraud.

We are aware that more young people are allowing their bank accounts to be used for the movement of money that is the proceeds of crime[8] . Those so doing are often referred to as 'money mules'. Cifas reported a 27% increase in 14-24-year-olds acting as money mules[9], the term for those who allow their accounts to be used for the transfer of illegally obtained monies.

In facilitating the movement of illicitly-obtained monies, young people are acting as the conduit to transfer criminally obtained funds often out of the country. Such monies may be used to fund a range of criminality, including terrorism[10].

The consequences for young people being caught providing money mule facilities perpetrating fraud are wide-ranging. As well as the potential for prosecution in front of a criminal court it can affect their ability to gain credit, open a bank account, obtain a mortgage or, more likely of more immediate concern to young people, can affect their ability to buy mobile phones or get car insurance.

Young people need to be acutely aware not only of the danger of falling victim to fraud but also of becoming ensnared in crime through becoming a money mule.

To help understand the young person's perspective and the role of parents and guardians, we undertook a public consultation in the form of an inquiry to help us to gain a better understanding of the factors that drive and influence a young person both in protecting their financial information and in taking a path which may lead to fraudulent conduct.

We are very grateful to those organisations and individuals who responded to the inquiry. Their written submissions, together with evidence provided in oral evidence, has helped us to identify the issues and focus on educational outcomes that we believe provide a once in a generation opportunity to positively change the behaviour of young people.

[6] *Cottrill, and Nina. "Statistical Bulletin: Crime in England and Wales: Year Ending March 2018." Office for National Statistics, 2018, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018*

[7] *Fraudscape 2017. Cifas, 2017, www.cifas.org.uk/secure/contentPORT/uploads/documents/reports/External-Fraudscape%20report%202017.pdf*

[8] *Fraudscape 2017. Cifas, 2017, www.cifas.org.uk/secure/contentPORT/uploads/documents/reports/External-Fraudscape%20report%202017.pdf*

[9] *https://www.telegraph.co.uk/personal-banking/current-accounts/fraudsters-target-cash-strapped-students-use-money-mules/*

[10] *FTI Consulting. SMALL CRIMES CAN LEAD TO BIG CONSEQUENCES: Raising Awareness of Cybercrimes and Links to Terrorism, 2016.*

Terms of reference

The Terms of Reference for the inquiry were to consider:

- The frauds and scams young people in the UK are falling victim to and perpetrating;
- What different bodies are doing to educate and protect young people from financial crime, and
- What more could be done to help prevent young people becoming involved or victims of fraud, scams, and other financial crime.

The following sectors, industries and bodies were in-scope in this inquiry:

Industry, charities and the voluntary sector, the education sector and universities, trade bodies, government departments and bodies, and law enforcement and the public.

A young person was classed as being under-25 for the purpose of this inquiry.

The inquiry asked the following questions:

1. What assessment have you made of the amount of young people:

a) Falling victims to fraud, scams and other financial crime?

b) Being involved as a perpetrator or willing accomplice to fraud, scams and financial crime?

2. What are the reasons why young people are falling for certain online frauds and scams?

3. What are the reasons why some young people are becoming perpetrators of fraud and economic crime? In particular money mules?

4. What measures are already in place – across the public, private and third sectors – to help prevent young people from falling victim to financial crime and scams? How effective do you consider these to be?

5. What measures are already in place – across the public, private and third sectors – to help prevent young people from getting criminally involved in financial crime and scams? How effective do you consider these to be?

6. What further measures should be in place to prevent this type of crime amongst young people?

7. What more should government and industry being doing to protect young people from predatory fraudsters and scammers?

8. What methods in this space are considered good practice and should be replicated more widely?

9. How could the law enforcement response to these issues be improved?

Inquiry Process

We are grateful to those to the organisations who responded to the APPG inquiry.

A full list of respondents can be found in Appendix 1, with their responses in Appendix 2.

Alongside the written evidence, one oral evidence session was convened in order to better understand the issues and explore possible options and outcomes.

We are grateful to the following speakers who gave evidence at the oral evidence sessions.

Oral Evidence Session One – 6 March 2017

This evidence session heard evidence from Detective Constable Dawn Wood and Detective Inspector Sue Grimmer from the Metropolitan Police Falcon team, and evidence from Jenny Fox, Subject Specialist from the PSHE Association.

This evidence session was not recorded at the request of the Metropolitan Police, but it expanded on themes found within the written evidence submitted from both organisations which can be found in the Appendix.

The clear message from this session was that both organisations felt there was a genuine need for better education in schools on fraud, scams and money mules and that industry should be doing more to raise awareness of fraud and scams before young people take out financial products and services, or share information online.

Key Statistics

- 41% of money mule accounts are linked to young people aged 25 or below[11].
- Research shows that 80% of 18-24 year olds are willing to share their email address online with their friends, and as many as 29% are willing to share their mother's maiden name[12].
- Beneficiary mule accounts held by those aged 25 and under increased by 14% to 52%[13].
- In 2017 there was a 27% increase in the number of 14-24 year olds being used as money mules[14].
- Figures from Cifas show there has been a 24% increase in young people under 21 being involved in fraud either as a victim or perpetrator from 2015 to 2017
- Figures from Cifas show a 58% increase in identity fraud victims aged 21 and under from 2015 to 2017.

Key Findings

There was a marked degree of agreement, and a number of common themes, arising from the consultation.

The central theme arising from the responses to this consultation is the need to put in place structured learning in our schools and colleges for young people on the means to keep themselves safe online from fraud and the dangers and consequences of being inadvertently drawn into money laundering.

This finding is underpinned by a wealth of evidence that young people tend to be naïve and overshare information online without understanding or appreciating the possible consequences for so doing.

> "[It] is simply a lack of awareness. Young people tend to 'live online' through social media channels and as such are less cautious about sharing personal information. The YouGov research showed that over 80 per cent of 18-24 year olds are willing to share their email address online with their friends, and as many as 29 per cent are willing to share their mother's maiden name (a commonly used security question). This contrasts with just 60 per cent of over 55s willing to share their email address, and only 12 per cent willing to share their mother's maiden name."
>
> *RBS response to APPG Financial Crime and Scamming Young Person Inquiry, 16 March 2018.*

Naivety may be exacerbated by the technology divide between young people and their parents. Young people may not always be supervised or adequately cautioned by an informed parent when accessing the internet at home.

There is also a suggestion by one respondent of collusion, pointing out that parents may be condoning fraudulent behaviour. For example, they allow a young person to lie when seeking car insurance, claiming the main driver is the parent when it is in fact the applicant seeking to lower the insurance premium.

This points to a need to educate parents in the dangers posed by an active online presence, to their parenting responsibilities and to what constitutes fraud. This may have additional consequential benefit for the parents as they increase their own awareness of fraud and scams, but should be primarily focused on enabling parents to help better advise those in their care. We believe that there needs to be a toolkit for parents on how they can keep their children safe from fraud and identity theft.

Education should not stop at schools or the home and the findings suggest that social media channels have a role to play in dynamic messaging to warn potential victims of the dangers of oversharing and advertisements which promote "easy money". Similarly social media should be more proactive in challenging and removing such adverts from their platforms.

One respondent pointed to the fact that manufacturers of internet enabled devices should ship such devices with antivirus software that cannot be circumvented by users. We agree that there is a viable argument that manufacturers rightly have a part to play in protecting the users of their internet enabled devices.

The suggestion of structured education is not new and we are conscious that The All Party Parliamentary Group on Financial Education for Young People looked at the issue and published their report in 2016[15]. Nothing that we say in this report undermines their findings and recommendations.

In fact, in broad terms the two reports are mutually supportive and underline the need to do more in schools through the education of young people in order to drive behavioural change. Therefore, taken in the round, we now have substantial and convincing evidence to call for counter-fraud education to be embedded in the national curriculum.

Whilst the educational messaging is important, it is also a finding that law enforcement need to be given the tools and resources to tackle those who prey on young people and draw them into criminality through the use of their bank accounts.

In the court context, where a person is convicted of luring a young person to act as a money mule, this should be acknowledged by the Sentencing Council as an "aggravating factor" as far as the sentence of the court is concerned. Such corruption of a young person is a serious issue and should be treated as such from a sentencing perspective.

One respondent also suggested that young people may take more notice of paper-based statements than online material. While it is not suggested that the industry revert to a paper-based policy, nonetheless choice is important and there will always be those who manage better where they have the information before them in paper-based form.

A law enforcement response highlighted the fact that UK policing have little data and evidence on young victims of fraud and a big part of the reason for this is underreporting of this crime by young people. This response showed the need for young people to report fraud and financial crime to Action Fraud. However, any moves to increase reporting should not reduce individual's personal responsibility to help protect themselves from online fraud and scams.

Finally, we agree with those respondents who raised the point that any education programme needs to take into account those whose first language is not English.

Any guidance or educational content produced should be available in multiple languages in order to ensure that minority groups in our society also understand how better to protect themselves and are not left vulnerable to fraudsters.

Evidence held by different organisations such as the Home Office, City of London Police, education authorities, local authorities and other relevant bodies on the minority groups most at risk to financial crime, would help inform the decision on what languages the educational material should be in.

There is currently a pre-existing wealth of material that schools and other education establishments can use to teach students about fraud, financial education and online identity protection. Amongst many others, City of London Police, My Bnk, Cifas, Friends Against Scams, Barclays Life Skills, Money Sense and the PSHE Association all have teaching materials designed to target young people.

As many respondents to the inquiry have stated, to introduce fraud education across all UK schools, the Department for Education and the wider education establishment should not have to re-invent the wheel in producing counter-fraud materials. They should considering drawing from the wealth of good practice and materials already on offer but which are not currently compulsory, ensuring consistent messaging across all programmes.

[11] UK Finance – Written Evidence Submission to the APPG on Financial Crime and Scamming Young Victims of Financial Crime Inquiry
[12] Young People More Likely to Become Victims of Online Fraud. Royal Bank of Scotland, 2017, www.rbs.com/rbs/news/2017/11/young-people-more-likely-to-become-victims-of-online-fraud.html.
[13] Barclays - Written Evidence Submission to the APPG on Financial Crime and Scamming Young Victims of Financial Crime Inquiry
[14] Fraudscape 2018. Cifas, 2018, www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Fraudscape%202018-Final.pdf.

[15] Financial Education in Schools: Two Years On – Job Done?" Young Money, All Party Parliamentary Group on Financial Education for Young People, 2016, www.young-money.org.uk/sites/default/files/APPG%20on%20Financial%20Education%20for%20Young%20People%20-Final%20Report%20-%20May%202016.pdf.

SUMMARY OF RESPONSES

PSHE Association

We found the written submission by PSHE compelling. They identified the lack of digital literacy as key concern despite young people being seen as 'digital natives'. They confirmed that young people suffer in the same way as adults in not being able to manage information appropriately and in deciding what information should be kept private and what shared.

They also acknowledge the role of parents and state that "parents can often feel ill-equipped to deal with the complexities of the online world and so expect schools to play an important role." In fact, they quote that 92% of parents believe all schools should teach PSHE education.

They quote from the House of Lords Communications Select Committee which found that "the skill and knowledge to critically understand the internet…sit alongside reading, writing and mathematics as the fourth pillar of child education[16]."

Dom Educational Group

Dom are an established training provider already delivering classroom based financial education in Schools and Colleges.

Their insight confirms much of what was asserted by PSHE, identifying the need for financial education but highlighting concern around those young people who may be being recruited as money mules. Tellingly their experience is that "…some young people may not even realise that they are being recruited."

They also emphasise the need to identify and act upon the early signs of money laundering and made helpful suggestions as to the need for impactful campaigns using social media channels and YouTube rather than mainstream television and radio.

Julie Lloyd, Hertfordshire Police

Julie is a police officer in Hertfordshire police however, the response is her personal experience and not the force's official submission. Nevertheless her views are insightful.

She speaks of young people falling for fraud and scams from "naivety" and possible being "overly confident." As for the reasons they commit such crime Julie asserts: "Less life experience, hence less empathy for victims."

Julie supports the call for input through schools and speaks of "standard lessons plans for different age groups." She also calls for more warnings on auction sites and through online banking.

Perhaps worryingly she asserts that, "local officers and PCSOs have no idea of the levels of fraud in their areas as fraud is no longer on local police station systems all fraud records being kept at Action Fraud." She also claims that "hardly any online frauds get investigated."

[16] *Growing up with the Internet. 2017, publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm.*

Royal Bank of Scotland (RBS)

The submission refers to RBS research from 2017 which showed that "younger people are less likely to be cautious online prepared to older generations."

Crucially, RBS also state that: "the increase of fraud and scams is strongly connected with the rise in internet usage."

The assertion that fraud is "prevalent among Young Potentials (18-35) with modest incomes and 18-25 year old students" underpins the views of others who made written submissions.

Interestingly, the bank submits that most customers start their relationship with the bank as genuine customers but are "enticed by posts on social media forums which suggest they can earn money very quickly with no risk to themselves." This grooming of young people plays to the naivety referred to by Julie Lloyd and inferred from other submissions.

NatWest are also active in the education arena through NatWest Money Sense and, as with other submissions, "we believe fraud education from a young age is vital."

RBS chair the industry Money Mule Working Group at UK Finance.

Keep Me Posted

The organisation champions pro-consumer choice and for consumers to have the choice to receive paper bills and statements.

The submission makes the points that "one fundamental tool particularly lacking for younger consumers is access to paper bills and statements which, in turn, increases the chance of financial mismanagement, disengagement and a greater chance of being susceptible to fraud."

They point to the fact that "the greater the importance attached to a document, the greater the likelihood of young people preferring to receive the document in paper format to a digital format." Keep Me Posted highlight a survey from 2017 which found that 47% of young people surveyed agreed that they found it easier to manage their finances when in receipt of a paper bill or statement.

They conclude that: "young people are disproportionately affected by the switch to digital e-billing which increases the risk of falling victim to scams and fraud."

Barclays

Barclays is active in the educational space through Digital Eagles and community based initiatives.

They state that: "our research proves that young people falling victim to fraud and scams is a growing trend, exemplified by the now commonplace example of young people serving as money mules.

"Insight shows that millennials and younger families are more vulnerable to these crimes than ever before." They go on to say that: "[the number of] young people involved in financial crime has increased by 14% between 2016-17."

They also echo RBS' comments around social media: "We've seen a number of social media articles offering earnings for being a Money Service Agent (e.g. on Facebook and Instagram) which appeal to a younger age group."

They support the drive to build financial education into the curriculum and suggest “PSHE, Maths or Citizenship” as the teaching vehicles.

The bank concludes that they “would like to see the rise of financial fraud and scams properly prioritised and resourced across law enforcement in the UK.”

UK Finance

The organisation is a trade association representing leading number of firms providing finance, banking and payments-related services in or from the UK.

They reflect the views of RBS and Barclays and give one of the reasons why people are falling for online frauds and scams as: “simply a lack of awareness and compulsory education in schools and universities on financial crime and how to operate securely online.”

The also reflect Julie Lloyds’ view that: “young people also tend to have less experience of the real world and therefore may be more naïve with regard to how typical frauds and scams operate.”

UK Finance agree that the most effective way to prevent this type of crime amongst young people is to focus on mandatory financial education “prior to becoming financially active.”

They go on to state that: “education should focus on financial literacy more widely [so that] young people fully understand the repercussions of financial crimes in terms of financial curtailment, criminal sanctions and outcomes for victims.”

City of London Police

City of London police operates Action Fraud, the national reporting centre for fraud and cybercrime. They also have created Cy-Fi Juniors, a fraud and cyber-crime educational programme for 9-11 year-olds delivered by volunteers in policing. They also work closely with Get Safe Online and other charities such as Age UK in the preventative and the protective arena.

City of London Police provide statistical insight into fraud both impacting and perpetrated by young people:

- Young people (0-19) make-up around 3% (over 8,000 of 280,000) of Action Fraud Reports in 2016/17.
- 72% of these reports were cyber-enabled
- The most commonly reported fraud in this age group is online shopping and auction and ticket fraud.

They confirm the views of other submissions in that: “young people are often less cautious online which can result in them being particularly vulnerable to scams… The focus of protect advice should be around staying safe online and the use of websites.”

They state that: “encouraging young people to submit reports of suspicious websites, social media pages or accounts through the Action Fraud online portal will improve the law enforcement response by providing a more comprehensive picture of the threat.”

City of London Police state that young people are primarily targeted through their use of websites and encouraging a change in behaviour on how they use the internet could lead to a reduction in victims of fraud.

They highlighted a recent joint campaign they undertook with Get Safe Online and the Society of Ticket Agents and Retailers. This campaign aimed at directly changing young people’s behaviour by tricking them into buying fake music event tickets – those who clicked through to buy the tickets were told they were unable to buy them and giving advice on how not to fall victim to ticket fraud in future.

Lastly, their response highlighted the need for more to be done to improve the reporting of fraud and financial crimes young people fall victim to or are involved in to Action Fraud and wider law enforcement. Their response stated if they had more evidence and data on young victims of fraud the law enforcement response could be better targeted to responding to these crimes.

Association of British Insurers (ABI)

The ABI acts as the voice of the UK’s insurance and long-term savings sector. As with other organisations who submitted evidence, they are active in the counter fraud arena and their counter fraud efforts detected £1.3 billion of attempted claims fraud in 2016.

Anecdotal evidence from the ABI suggests that “young people may act as willing accomplices in fraudulent activity in engaging with illegal insurance advisers (ghost brokers) in the knowledge that the information has been misrepresented in order to fraudulently reduce the cost of their quotes or premiums.”

“Some people may also be complicit in the practice of motor insurance fronting. This occurs when another person, often a parent or other older relative, is proposed as the main driver in order to obtain a lower premium whilst a younger driver is subsequently identified as the main driver or owner of the vehicle.”

Again, mention is made of social media as being a forum through which introductions are made to fraudulent brokers. The ABI go on to state: “We would welcome further cross-sector campaigns to educate young people about common frauds and how to protect themselves against them.”

Metropolitan Police (FALCON)

In 2017, the Metropolitan Police Service received reports of 8,041 fraud related crimes of which 1,057 (22%) included were victims under the age of 25 years.

They state: “with social engineering… we are left with individuals who openly provide private information without thinking about the consequences. Where technology has advanced with such rapid speed over the last 20 years, there is a distinct divide of lack of knowledge from parent to child learning.”

“There appears to be limited coverage in respect of online safety specific to fraud and cybercrime within our Education system, combined with a lack of personal desire to learn how to protect yourself, provides the fraudsters with an open ended supply of victims.”

Finally, the Metropolitan Police suggest that financial institutions have a considerable role to play too: “Financial institutions can play a part in deterring money mules and preventing money laundering by young people by having in place suitable policies for any new accounts for under 18 year-old customers.”

Fraud Advisory Panel (FAP)

The Fraud Advisory Panel "strongly believe that prevention should be front and centre in tackling fraud and financial crime within wider society and, more specifically against young people."

FAP raise an interesting point not picked up by the other responders, namely the affordability of anti-virus software: "This may make it an optional (perhaps unaffordable) extra rather than a "must-have" safeguard."

They also speak of the fact that consumers and young people don't change out-of-the box security settings on devices which play to the advantage of hackers.

They state that: "fraud and financial crime should not be seen in isolation and closely relates to other existing initiatives within schools such as safeguarding and online "stranger danger" education."

"There needs to be a consistent and unified approach to reaching out to young people through schools and universities."

The FAP also speak of the need to produce prevention advice in various languages which addresses the point that for some young people and parents English may not be their first language.

The FAP ask a pertinent question: "when a young person lets their bank account be used by a "friend" or acquaintance without realising it was for criminal purposes – are they a victim or a perpetrator, or both?"

As with other responders, they also point out that the financial consequences of committing a fraud offence, "could be powerful and stark reminder that there are negative consequences to an action they may only consider as a small risk."

Yoti

Yoti is a digital identity platform, who believe that there is a strong potential for technology and innovation to assist those combating economic crime.

Yoti highlighted figures from the Driver and Vehicle Licencing Authority which show that almost one million driving licences were lost by UK drivers last year and that young people disproportionately applied for a replacement licence – 82% of 16-24 year olds of those surveyed.

They raised concerns that young people are more likely to lose their identity cards and documents, such as driving licences and passports, partly because they need to carry around these documents as ID in the night-time economy as an example.

Yoti said the PASS scheme (The National Proof of Age Standards Scheme)[17] needs to be expanded and have more take up across the UK. Yoti believes there needs to be an update to legislation to allow wider access to proof of age cards and digital age checks to be performed across a range of sectors to help young people losing their identity documents and subsequently being targeted by fraudsters.

[17] *http://www.pass-scheme.org.uk/*

RECOMMENDATION & CONCLUSION

We reiterate how grateful we are to all those who responded to this inquiry and who have contributed and informed our findings.

Based upon the evidence and findings of this consultation we wish to make five recommendations:

1. That a greater focus on education and awareness programmes is given by the education sector, government, industry and the third-sector.

- Counter-fraud education should be introduced into the national curriculum across all UK schools for those aged 11-16 years old (Key Stage 3 and above).
- Parenting courses – available from a range of providers - should include a module on protecting their children from financial abuse.
- Government should work with industry to make preventative advice available to parents of students attending full-time education.
- Educational establishments should consider holding counter fraud events at teachers' open evenings.

2. Social media platforms should be proactive in preventing scams from being promoted on their platforms and raise awareness amongst their users:

- Social media organisations should do more to warn young people of the dangers of oversharing information online and of the practice of those who recruit 'money mules' through social media channels.
- Social media channels should also be more proactive in vetting advertisements promising "easy money".

3. Law enforcement should have dedicated resources focused on the investigation and disruption of money mule networks.
4. That the Sentencing Council should issue an amended guideline on fraud identifying the corruption of a young person recruited as a money mule as an aggravating factor for the purpose of sentencing.

5. That young people should be encouraged to report instances of fraud, either where they are a victim or where they are being groomed to take part in fraud such as a being a money mule. This will help to develop a better understanding of fraud in the way it impacts young people.

We believe that there is now substantial evidence that makes it essential and urgent to introduce structured counter fraud programmes across our educational establishments.

Prevention is better than cure and if we are not educating young people – our next generation – with the skills and tools they need to defend themselves against this new volume crime we have no hope in preventing it from spreading further.

With more and more young people operating their social and financial lives online action is needed now, more than ever, to educate young people about the risks of being drawn into financial crime and the implications of falling victim to it.

APPENDIX 1: LIST OF RESPONDENTS

Association of British Insurers (ABI)

Barclays

City of London Police

Dom Educational Group

Fraud Advisory Panel (FAP)

Julie Lloyd, Hertfordshire Police

Keep Me Posted

Metropolitan Police (FALCON)

PSHE Association

Royal Bank of Scotland (RBS)

UK Finance

Yoti

APPENDIX 2: WRITTEN EVIDENCE

Association of British Insurers (ABI) response to the All-Party Parliamentary Group on Financial Crime and Scamming inquiry into "Young Victims of Financial Crime"

About the ABI

The ABI is the voice of the UK's world-leading insurance and long-term savings sector. A productive, inclusive and thriving sector, we are an industry that provides peace of mind to households and businesses across the UK and powers the growth of local and regional economies by enabling trade, risk taking, investment and innovation.

Executive Summary

1. The insurance industry is committed to tackling all forms of insurance crime and protecting honest customers from fraudulent activity and rising costs as a result. For this reason the industry invests, and will continue to invest, significant resources in deterring and detecting insurance fraud.

2. In 2016, insurers detected 125,000 dishonest insurance claims valued at £1.3 billion. It is estimated that around £2bn of insurance fraud goes undetected each year. This is why insurers invest at least £200 million each year to identify and combat fraud.

3. Fraud cuts across all products within insurance. At one end of the spectrum, fraud may be committed by opportunists, where people encounter an opportunity to invent or exaggerate a claim or to deliberately or recklessly provide false information when applying for insurance. At the other end, there are highly organised criminal gangs, for example fraudsters involved in 'crash for cash' or 'ghost broking' scams. Tackling insurance fraud therefore remains a strategic industry priority.

4. The insurance industry invests significant resources to help prevent people from falling victim to, and getting involved in, financial crime and scams. In addition to improving their own anti-fraud systems to protect customers and firms, insurers also fund a range of industry initiatives aimed at preventing, detecting and prosecuting fraudsters.

5. Awareness is a proven defence against fraud, and we would encourage further cross-sector campaigns to educate young people about common frauds and how to protect against them.

6. Despite significant ongoing investment from the insurance industry in the Insurance Fraud Enforcement Department (IFED) within the City of London Police, there is insufficient current police resource available to respond to and manage the number of cases of suspected fraud for investigation and enforcement. This has been compounded by regional police forces over recent years reducing their resources allocated to fraud and financial crime.

7. A key way to disrupt organised fraudsters is to deprive them of their (often lucrative) lifestyles. The asset recovery process is still unnecessarily protracted and the Home Office should keep this under review.

Inquiry Questions

Question 1: What assessment have you made of the amount of young people:

(a) Falling victims to fraud, scams and other financial crime?

(b) Being involved as a perpetrator or willing accomplice to fraud, scams and financial crime?

8. Insurers continually assess the risk of their customers falling victims, or becoming perpetrators or accomplices, to all types of financial crime. For example, the Insurance Fraud Bureau works with the industry to develop an Industry Strategic Threat Assessment which documents key risks faced by the insurance sector and makes recommendations to mitigate those risks.

9. The ABI collects information annually regarding detected fraud to provide its members and wider stakeholders with an indication of the extent of fraud that the industry faces at both the application and claims stage. This information provides an indication of the level of detected fraud impacting on the insurance industry as a whole.

10. In 2016, insurers detected 125,000 dishonest insurance claims valued at £1.3 billion. The average value of each fraudulent claim has risen to £10,196, an increase of £3,000 in 10 years. There are now 343 fraudulent claims (worth approximately £3.5m) made every day.

11. Individual insurers have their own mechanisms for understanding their own exposure to fraud and taking steps to mitigate the related risks. Evidence suggests that many young people, in particular young males, are prone to falling victim to illegal activity and ghost broking. Insurers work individually and in collaboration with the industry's counter-fraud utilities (see question 4) to raise awareness of scams and assist customers who may have fallen victim to illegal activity.

12. While the industry's assessment of fraudulent activity is not broken down by age, there are a number of factors which are known to impact young people in particular, including the increasing cost of motor insurance (see question 2).

13. There is some anecdotal evidence to suggest that many young people may act as willing accomplices in fraudulent activity in engaging with illegal insurance advisers (colloquially known as 'ghost brokers') in the knowledge that their information has been misrepresented in order to fraudulently reduce the cost of their quotes or premiums.

14. In addition, some young people may also be complicit in the practice of motor insurance 'fronting'. This occurs when another person, often a parent or other older relative, is proposed as the main driver in order to obtain a lower premium whilst a younger driver is subsequently identified as the main driver or owner of the vehicle.

15. In order to identify and combat such activity, insurers will use a variety of measures, including the use of scorecard indicators (such as the order of listing of drivers or the mismatch of main user and premium payments). Insurers continue to highlight that such activity is fraudulent and try to raise awareness of the consequences of fronting.

£1.3bn

detected fraud

Over 125,000 detected cases of attempted claims fraud in 2016 - a 5% decrease in volume compared to 2015.

£780m

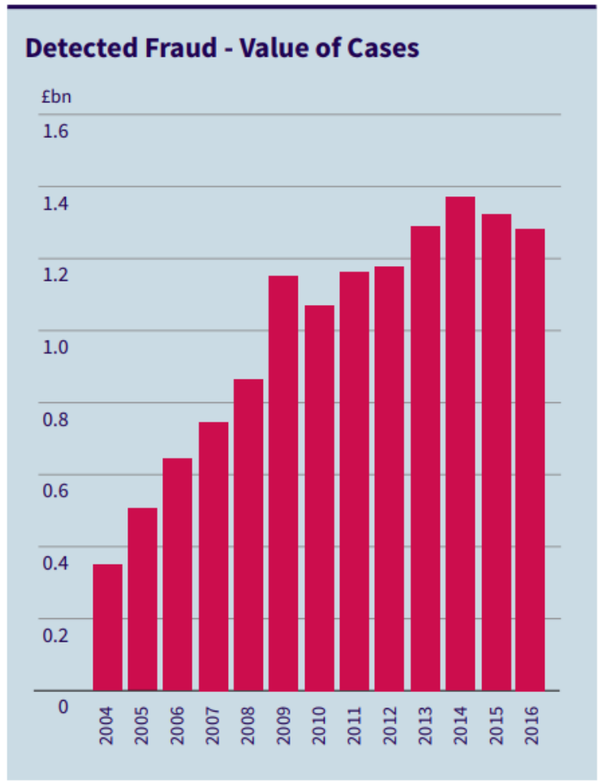
motor fraud

Fraudulent motor claims were the most common, with over 68,000 cases in 2016.

£372m

liability fraud

Volume of fraudulent liability claims is down 4% in 2016, with 25,000 cases valued at over £372m.



ABI Fraud Statistics 2016

Question 2: What are the reasons why young people are falling for certain online frauds and scams?

16. ABI data shows that motor premiums are at a record high. Drivers in nearly all age groups are paying record amounts for their car insurance but those aged 18-20 paid the highest average premium at £973. Our analysis shows that 10% of the average salary of drivers aged 18-21 now goes on paying their motor insurance bills - an average of £973 for comprehensive cover. This is more than five times the average proportion among all other drivers. This highlights that younger drivers are feeling the impact of rising motor insurance bills, caused by factors such as the way compensation pay-outs are currently calculated and a resurgence in whiplash-style claims, the hardest. The high cost of motor insurance acts as the catalyst for some younger drivers to purchase insurance from 'ghost brokers'.

17. The term 'ghost broking' is used to capture the range of tactics used by fraudsters to sell fraudulent car insurance. This is typically carried out in one of three ways; they will either forge insurance documents, falsify details to bring the price down, or take out a genuine policy before cancelling it soon after and claiming the refund plus the victim's money.

18. From November 2014 – October 2017, Action Fraud, the national fraud and cyber reporting centre, hosted by the City of London Police, received more than 850 reports linked to ghost broking, with reported losses for both individuals and organisations totalling £631,000. On average, each individual victim lost £769. Analysis by the City of London Police's Insurance Fraud Department (IFED) shows that men aged 20-29 are most likely to be targeted by ghost broking.

19. Most commonly, ghost brokers will make initial contact with people through social media, particularly Facebook, Instagram and Snapchat. They often advertise on student websites or money-saving forums, university notice boards and marketplace websites such as Gumtree. As young people are more likely to use these websites or applications, they are more likely to be exposed to fraudulent motor insurance policies.

Question 3: What are the reasons why some young people are becoming perpetrators of fraud and economic crime? In particular money mules?

We have no comments on this question.

Question 4: What measures are already in place – across the public, private and third sectors – to help prevent young people from falling victim to financial crime and scams? How effective do you consider these to be?

20. The insurance industry invests significant resources to help prevent people from falling victim to, and getting involved in, financial crime and scams. In addition to improving their own anti-fraud systems to protect customers and firms, insurers also fund a range of industry initiatives aimed at preventing, detecting and prosecuting fraudsters.

21. The **Insurance Fraud Bureau (IFB)** is a not-for-profit company established in 2006 focused on the detection and prevention of organised fraud. The IFB supports the insurance industry and law enforcement by providing intelligence and assisting investigations. The IFB also raises public awareness of insurance fraud scams: how they work and how to spot them, so that the chances of being caught out are reduced. The IFB currently has 63 application fraud investigations under management, 60 of which are ghost broker-specific.

22. The **Insurance Fraud Enforcement Department (IFED)** is a specialist police unit dedicated to tackling insurance fraud. Established in 2012, IFED is funded by the ABI and Lloyds of London members, and is hosted by the City of London Police within the Economic Crime Directorate. IFED's team of detectives, financial investigators and police staff act with operational independence while working closely with the insurance industry. IFED targets established criminality – motor insurance fraud, commercial and public liability fraud – while at the same focusing on emerging threats, such as illegal insurance advisers (including ghost brokers). Since its inception in 2012, IFED has secured more than 340 convictions.

23. The unit is also uncovering and dismantling organised crime gangs that are responsible for an increasing amount of today's insurance fraud, and changing the public perception that committing small time 'opportunistic' fraud does not really matter.

24. In February 2018, IFED launched a campaign (#SteerClearOfFraud) to encourage drivers to be wary of heavily discounted prices on the internet or cheap prices they are offered directly for car insurance, as they may well be ghost brokers.

25. The case studies below demonstrate how insurers and industry-funded initiatives collaborate to help prevent young people from both falling victim to, and getting criminally involved in, insurance fraud.

Case study 1: Danyal Buckharee

In 2015, the Old Bailey ordered for £658,460.84 to be confiscated from a 'ghost broker' currently imprisoned for masterminding what is believed to be the UK's biggest fake car insurance scam.

The action came on 25 June 2015 after City of London Police's Insurance Fraud Enforcement Department (IFED) applied to the court to recover the profits of his crimes in 2013 after its investigation saw him jailed for three years. This was on top of four-and-a-half years given for a separate fraud investigated by the Metropolitan Police Service.

Buckharee duped 600 drivers, including many students, into buying worthless car insurance between May 2011 and April 2012, pocketing £658,460.84. He created four websites offering 'cheap' car insurance – Aston Midshires Insurance, Astuto Insurance, Car Insurance Warehouse and First Car Direct Insurance.

Aston Midshires Insurance first came to the attention of the Motor Insurers' Bureau (MIB) in late 2011 when the bureau began receiving complaints from drivers who had been stopped by police for driving without insurance. The MIB passed the complaints onto the Insurance Fraud Bureau (IFB) for further examination and when IFED launched in January 2012, the complaints were handed to the new unit.

Case study 2: Azeem Mahmood Hussain

In 2016, Azeem Mahmood Hussain, a 19-year-old man from Walsall was sentenced to 12 months' imprisonment for selling fake motor insurance to unsuspecting customers, leaving them uninsured and illegally driving on the roads.

Hussain's deception first came to light on 9 July 2013 after a man who unwittingly used Hussain's service to insure his van was stopped by police in Northern Ireland. Checks on the vehicle revealed it was uninsured, but the driver protested and said that he was insured, having paid £200 into a bank account for the policy in response to a Gumtree advert. The case was eventually passed on to IFED, where officers made enquiries and identified the account as belonging to Hussain.

On 9 October 2013, IFED officers executed a search warrant at Hussain's address, seizing mobile phones, a laptop, bank statements and debit cards. Officers found over 100 templates and forged documents on the laptop and the phones matched the numbers from the Gumtree adverts.

Detectives matched the accounts into which the victims had paid money to statements, debit cards and cheque books found at Hussain's address. Officers found over £14,000 had been paid into one of the accounts, with £2,250 into the other. Most of the deposits into the accounts had references of names or registration numbers.

Hussain is one of the youngest people ever that IFED dealt with for insurance fraud and his story demonstrates how young people can exploit members of the public by getting involved in ghost broking.

Question 5: What measures are already in place – across the public, private and third sectors – to help prevent young people from getting criminally involved in financial crime and scams? How effective do you consider these to be?

26. Research commissioned by the ABI in 2015 reveals that most instances of opportunistic offences do not involve a high degree of planning. Opportunistic fraudsters seldom consider to any great extent the risks of their crime and any measures that improve public understanding of the consequences of their actions may help prevent young people from getting involved in financial crime.

27. The Government's Modern Crime Prevention Strategy highlights a number of areas where work is being done both to educate young people about crime and put in place measures to help prevent young people from getting criminally involved in financial crime and scams. Chapter 3 ('Character as a Driver of Crime') contains particularly pertinent information regarding young people's propensity to committing opportunistic crime.

28. In November 2013, the IFB, IFED, and ABI partnered with Crimestoppers to launch a campaign: Getarealdeal. The campaign, which centres on consumer advice relayed in an animated video, provides a simple guide to buying legitimate insurance, tips on keeping motor insurance premiums down and outlines the grave consequences of being scammed by a ghost broker.

29. Strategies which focus on measures which will prevent crime by building positive character traits and increasing young people's abilities to make good decisions will help reduce the impact of all crimes, including insurance fraud and other scams.

Question 6: What further measures should be in place to prevent this type of crime amongst young people?

30. As outlined above, fraudsters are opportunistic, creative and innovative; quick to identify new targets and vulnerabilities and to adopt new tools and techniques.

31. Given that awareness and profile raising is a proven defence against fraud, insurers and other public and private organisations are already working hard to promote fraud awareness across all sectors in the UK. We would therefore encourage further cross-sector campaigns to educate young people about common frauds and how to protect against them.

32. One of the many complex challenges faced by the industry is identifying ways of interrupting dishonest behaviour while reassuring honest customers and avoiding any barriers to the timely payment of legitimate claims. Opportunistic fraud is believed to account for a significant majority of the total value of undetected fraud which could cost the industry as much as £2 billion. Tackling this type of fraud has been a long-standing challenge to the industry and forms one of the key recommendations of the Government's Insurance Fraud Taskforce (IFTF) report.

33. As part of the industry's commitment to developing a communications strategy to tackle opportunistic insurance fraud, the ABI and the IFB has appointed behavioural experts to

carry out research into the impact of various interventions in the customer journey that could change attitudes and behaviours towards insurance fraud, reduce the propensity of some people to be dishonest, and reduce the cost of fraud without disrupting the vast majority of honest customers.

Question 7: What more should government and industry being doing to protect young people from predatory fraudsters and scammers?

34. While insurers are already working work hard to promote fraud awareness across all sectors in the UK, we would welcome further cross-sector campaigns to educate young people about common frauds and how to protect against them.

Question 8: What methods in this space are considered good practice and should be replicated more widely?

35. As part of the Government's modern crime strategy, in December 2018, Amber Rudd announced a new National Economic Crime Centre within for the UK. The ABI is supportive of such initiatives and, given that many crime problems will have more than one driver (e.g. opportunity, character, profits, drugs, etc.), this requires a coordinated approach. The best way to tackle crime – particularly organised crime – is to bring together the expertise from across government, law enforcement, regulators and the private sector, and to share intelligence to help make the UK a more hostile environment for committing crime.

36. Tackling financial crime and fraud requires a collaborative approach involving various agencies working in partnership. The insurance industry fully supports cross-agency collaboration.

37. It is conservatively estimated that ABI members spend at least £200m pa on measures to combat fraud that focus on the 3 core pillars of prevention, detection and enforcement. This includes funding a number of core counter fraud initiatives that have led to a sea-change in the way that insurance fraud has been tackled over the last 12 years.

38. The ABI was also a member of the Government's Insurance Fraud Taskforce which issued a report (January 2016) that made a number of core recommendations to make the UK more resilient to insurance fraud.

Question 9: How could the law enforcement response to these issues be improved?

39. As outlined above, the insurance industry has worked with City of London Police to establish and fund IFED, a police unit dedicated wholly to combatting insurance fraud. Since its inception in 2012, IFED has secured more than 340 convictions, issued more than 425 cautions and seized assets valued in excess of £1.5m. Insurers would welcome increasing the numbers of convictions for insurance fraud.

40. Despite significant ongoing investment from the insurance industry in the Insurance Fraud Enforcement Department (IFED) within the City of London Police, there is insufficient current police resource available to respond to and manage the number of cases of suspected fraud for investigation and enforcement. This has been compounded by regional police forces over recent years reducing their resources allocated to fraud and financial crime and having no objectives to devote resources to such criminality.

41. Furthermore, the approach of the judiciary towards sentencing is inconsistent. The ABI welcomed new sentencing guidelines a couple of years ago which recognised the serious harm that insurance fraud can cause and put sentencing periods on a par with crimes that had traditionally seen tougher sentences (e.g. banking fraud or confidence fraud). However, we are seeing evidence of many convicted insurance fraudsters receiving suspended sentences and other non-custodial sanctions (e.g. community service orders). This undermines the impact of the industry's counter fraud strategy and messaging.

42. Finally, a key way to disrupt organised fraudsters is to deprive them of their (often lucrative) lifestyles. We recognise that the Serious Crime Act 2015 introduced changes designed to make the asset recovery process simpler and more effective. This is moving in the right direction. However, the process is still unnecessarily protracted. It can take years to confiscate and return proceeds to the owner. As such, the Home Office should keep this under review.

Barclays
1 Churchill Place
London
E14 5HP

barclays.com

16 March 2018

Cifas,
6th Floor, Lynton House,
7-12 Tavistock Square,
London, WC1H 9LT,

To whom it may concern,

Barclays Submission – APPG on Financial Crime and Scamming's Inquiry into Young Victims of Financial Crime

Introduction

Barclays recognises that as financial fraud and crime becomes increasingly common, young people – those typically considered most savvy in their use of digital channels, are in fact particularly vulnerable to fraudsters and scammers. Our research proves that young people falling victim to fraud and scams is a growing trend, exemplified by the now commonplace example of young people serving as 'money mules'.

Given this growing trend, there is a considerable amount of work underway at Barclays and across the industry to tackle it. However, we recognise that more can be done, both by Government and the private sector, to help young people understand what being involved in a financial crime actually looks like, what the implications of this are, and how it can be avoided.

1. **What assessment have you made of the amount of young people:**

a) Falling victims to fraud, scams and other financial crime?

Whilst common perception is that older people are most vulnerable to fraud and scams, our insight shows that millennials and younger families are more vulnerable to these crimes than ever before. Within Barclays, this group account for 70% of scam victims, with the average scam valued at less than £1,500. Within this growing trend, we would highlight the following:

- Growth of young people affected by digital fraud and scams: Our research shows that the percentage of young people involved in financial crime has increased by 14% between 2016-17, with the figures set to rise further. Despite this group being perceived as digitally savvy, their reliance on digital channels also means that they are increasingly vulnerable to digital fraud and scams.
- Emotional impact: Barclays' research with the victims of fraud and scams revealed that the biggest impact of such occurrences is emotional, with customers experiencing shame and guilt, and often even keeping the incident from friends and family.

- Vulnerability: There is an inherent element of dynamic vulnerability in most cases. Dynamic vulnerability is the personal situation any individual is experiencing, from being fatigued to experiencing bereavement. Momentary distractions or lapses are often all it takes for people to drop their guard enough to fall victim to a sophisticated scam. Our insights also show that customers who struggle financially are more exposed to being a victim of a scam.

b) Being involved as a perpetrator or willing accomplice to fraud, scams and financial crime?

While our research indicates a marked rise in the number of young people now involved in financial, we also know that not all of these young people are knowledgeable or willing participants of the crime they're partaking in, with some being forced or coerced into having their accounts used for this purpose. Our data points below provide an overview:

- In 2016, c. 38% of beneficiary mule accounts identified at Barclays were aged 25 or under, and 20% of those were 21 or under.
- By comparison, in 2017 the number of beneficiary accounts held by those aged 25 or under increased by 14% to 52%, with 36% of those aged 21 or under - an increase of 16%.

2. **What are the reasons that young people are falling for certain online frauds and scams?**

Our analysis shows that there are three core techniques used to dupe customers. Each factor in isolation may not have the desired impact, but depending on the sophistication of the case, a combination of the following often have the desired impact:

- Building relationships: The fraudsters commonly attempt to build relationships with the victim, by establishing a rapport which creates a sense of trust. The personal nature of interactions that customers have with fraudsters plays a significant role in their willingness to subsequently act on their guidance or advice.
- Conforming to category norms: Scams utilise known payment norms to signify authenticity and avert suspicion. Mimicking genuine processes and meeting customer's expectations of how the arrangements of a transaction will be made can delay, and even prevent, customers realising that they've been scammed.
- Creating time pressure: Tight timelines and/ or creating a sense of high demand are leveraged to pressure customers into acting without due diligence. Customers can feel forced into acting quickly, rather than considering the context of their interaction and the long-term implications. Scammers are adept at driving immediate and emotional, rather than considered and rational responses.

3. **What are the reasons why some young people are becoming perpetrators of fraud and economic crime? In particular money mules?**

- Social media targeting: We've seen a number of social media articles offering earnings for being a 'Money Service Agent' (e.g. on Facebook and Instagram), which are targeted to appeal to a younger age group. The promise of cash for relatively low effort is also positioned as an obvious benefit.

- A sense of disenfranchisement: Young people may feel a stronger sense of disenfranchisement, especially if they're struggling to find work or feel detached from the education system.
- Lack of cognizance of the crime and implications: There is an evident lack of knowledge among young people about what is and isn't a financial crime. This lack of awareness about the characteristics of financial crime, and the implications of taking part in one, leads to the success of fraudsters and scammers, who we understand are provide an illegitimate sense of legitimacy about the activity.

4. **What measures are already in place – across the public, private and third sectors – to help prevent young people from falling victim to financial crime and scams? How effective do you consider these to be?**

At Barclays we undertake a significant amount of work, both internally and across industry to reduce levels of financial crime.

Barclays work:

- Operating a new process that monitors 'out of character' incoming payments. As part of this, we are supporting discussions about Project Freeze that will hope to develop an industry solution for the 'hold' on suspicious payments.
- Creating a sophisticated state of the art fraud system to spot when a transaction could be deemed suspicious for a customer.
- Barclays LifeSkills: Fraud modules are available within our MoneySkills lesson plans to help build awareness amongst young people in order that they avoid risks. The digital safety module is set to be launched later this Spring.
- Barclays utilizes its interactions with young people during University recruitment campaigns (e.g. fresher fairs, seminar engagement, and Digital Eagle interactions) to educate students about the threats posed by fraud, scams, and becoming a money mule. In 2017, this proactive outreach has already impacted on average over 40 students at each seminar of the 11 universities visited across the UK.
- Financial Wings is a Barclays platform to help people manage their day-to-day finances. With c10,000 people across the UK signed up, it has specific fraud and scam content to educate users about how to avoid falling victim in the first instance.
- There's a huge focus in building awareness on fraud and scams across our branch network. In 2017 alone over 2,000 digital safety events took place across the UK.
- Our £10million Digital Safety Campaign was launched in 2017 to educate people across the UK on fraud, scams, and how to avoid them. The impact of this has resulted in over 26.5 million interactions since H1 2017 which includes hub visits, media partnerships, media coverage, social media, and colleague engagement.

Industry work:

It's important to acknowledge the wide range of work taking place across the industry to help protect young customers from financial crime. In order for this work to have the fullest impact across the UK, we believe that all parties that could impact the financial crime journey should participate. This includes social media platforms, dating sites, and new open banking entrants. Current work that Barclays participates in across the industry includes:

- PAS 17271: This was written by the British Standards Institute (BSI) to help financial providers adopt a set of principles to ensure that they're protecting their customers and treating them fairly when they do. Barclays was a member of the Publicy Available Specification (PAS) Steering Group.
- Take Five: Barclays have been heavily involved in the development of Take Five to encourage consumers across the UK to think before completing a transaction, and informing people not to be fooled when someone approaches them to potentially become a money mule.
- Joint Fraud Taskforce (JFT): Barclays is a keen contributor to the Home Office's Joint Fraud Taskforce – a collaborative effort across industry to tackle fraud and financial crime. As part of this, we have specific responsibility for the victim and susceptibility workstream, which looks at how the industry can create 'in the moment' support for customers before they make a transaction.

6. **What further measures should be in place to prevent this type of crime amongst young people?**

As mentioned, we believe that if this type of crime is to be sufficiently tackled, the whole eco-system must be involved. For example, social media platforms, online auction houses and dating sites all have a fundamental role to play in combatting fraud and scams amongst young people. Further measures could include:

- Education about financial crime: Building education on financial crime into the curriculum may be a useful exercise given its noteworthy rise in recent years. This could be most suitably incorporated into subjects such as PSHE, Maths, or Citizenship.
- All Payment Service Providers (PSPs) taking on all of the key industry work. This includes Project Durham, which is the mules tactical insight work that will alert financial institutions of suspect mule accounts.
- Project Freeze: As mentioned, we've seen success in monitoring out of character incoming payments proactively (Project Freeze) and believe the industry will see benefit by adopting it.

7. **What more should government and industry being doing to protect young people from predatory fraudsters and scammers?**

The government has a fundamental role to play in helping to protect young people from fraudsters and scammers. We recommend three core focusses for the government when aiming to achieve their desired outputs:

- Engaging broader industry partners: Involving a broader range of industry stakeholders (other than just financial institutions) when seeking to implement change in this space
- Education about financial crime: Building greater levels of awareness of financial crime into the curriculum, as above.
- Police prioritisation: Working with the police force across the UK to ensure financial crime (and rising digital crime) is properly prioritised, and resourced, in line with rising incidences.

8. **What methods in this space are considered good practice and should be replicated more widely?**

- External codes: The Scam Industry Standards which went live in October 2017 meant that customers who had fallen victim to scams had a consistent experience between banks. The development of this code to branch out to preventions and education would be beneficial across the industry.
- Education campaigns: Education Campaigns are a useful way to engage large amounts of people at once. Barclays Digital Safety Campaign was well received by stakeholders, and while we welcome Take Five and the Home Office's Cyber Aware Campaign, it would be interesting to explore whether a joined up effort may be worthwhile.
- Digital Eagle sign up- With c18,000 digital eagles who work with Barclays, and a further 450 signed up externally, using this peer to peer education and awareness could have huge benefits for the prevention of financial crime.

9. **How could the law enforcement response to these issues be improved?**

Barclays would like to see the rise of financial fraud and scams properly prioritised and resourced across law enforcement in the UK. It is currently unclear how law enforcement works with Action Fraud to tackle the rise of fraud and scams, and whether it is consistently and appropriately prioritised within individual units.
We have an existing relationship with law enforcement, which includes:

- Suspicious Activity Reports (SARs) work: Greater intelligence sharing by law enforcement with the private sector in relation to scam and fraud threats and typologies. By supporting the SAR regime, it would be useful for law enforcement to update financial institutions as appropriate when they become aware of criminal individuals or networks.
- Education and outreach: We've worked closely with police forces across the country to educate customers about financial crime. We'd like to encourage the continuation of this local activity across the whole industry to ensure that all young people have the awareness required to prevent themselves from falling into financial crime.

We welcome the focus of the APPG on this issue, and would be happy to discuss further as is useful.

CITY OF LONDON POLICE

ALL PARTY PARLIAMENTRY GROUP ON FRAUD AND SCAMS

YOUNG PEOPLE INQUIRY

City of London Police operates Action Fraud, the national reporting centre for fraud and cyber crime. In 2016/17, Action Fraud received over 280,000 crime reports from businesses and the public. Analysis of these crime reports, alongside data shared by Cifas and UK Finance, shows that reports by young people (0-19) make up around 3% (over 8,000) of Action Fraud reports. Young males and females are equally represented. 58% of reports involved a loss of £100 or under.

The low volume of crime reports relating to young people could be because they are targeted less frequently due to having lower disposable income, have a propensity to use an adult's bank account or card to purchase items or could indicate a lack of willingness of this age range to report fraud.

72% of these reports were cyber enabled and the first method of contact to young people is predominantly through a visit to an online sales platform (24%). The most commonly reported crime in this age group is online shopping and auction fraud, particularly by 16-19 year olds. This is probably due to this age range having greater access to disposable income to spend on online shopping and auctions, and access to an account or card to pay for these goods online.

Young people are also more commonly victim to crime involving ticket fraud than the general population. A number of these reports are cyber enabled with 38% of victims first contacted via a web forum or chat room and 36% reporting their first contact being via a visit to a website. Facebook is commonly used by suspects to advertise fraudulent tickets and provides a contact method for victims to engage with the fraudster.

In this age group, social media hacking and computer virus / malware / spyware are also prevalent. This is likely due to many young people being active on social media[1] and the internet, with young people spending on average, over 27 hours a week on the internet[2].
In addition young people are often less cautious online[3] which can result in them being particularly vulnerable to scams. However, it is not known if the prevalence of social media hacking and computer virus / malware / spyware in this age group is due to poor cyber security, use of illegal streaming websites[4], social engineering or more sophisticated cyber attacks.

[1] http://uk.businessinsider.com/99-of-young-british-people-use-social-media-every-week-2016-8?r=US&IR=T

[2] http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/11597743/Teenagers-spend-27-hours-a-week-online-how-internet-use-has-ballooned-in-the-last-decade.html

[3] http://www.actionfraud.police.uk/careless-generation-are-more-concerned-about-their-Facebook-profile-than-falling-victim-to-fraud

[4] https://www.theguardian.com/sport/2017/apr/25/illegal-streams-live-sports-sports-industry-group

City of London Police has not conducted research specifically into the motivation of young offenders. However, a joint research project with Cardiff University, University of Portsmouth and the University of Warwick that reviewed the motivation of 91 fraud offenders from 18-76 years identified the overwhelming purpose was to secure money for a materialistic lifestyle.

As young people are primarily targeted through their use of websites, the focus of protect advice should be around the staying safe online and use of websites, giving easy and simple guidance on how to check its legitimacy. Encouraging a change in the way that young people behave on the internet can affect whether they become a victim of fraud.

There is a range of fraud and cyber crime prevention advice provided to young people by law enforcement and other partners through engagement with schools and universities, and the Joint Fraud Taskforce has developed free lesson plans for secondary schools that focus on awareness of fraud, common scams, identity theft and money mules.

The North West Regional Organised Crime Unit has been developing young prevention ambassadors by working in collaboration with students to deliver presentations to elderly members of the community on how to stay safe online and some of the common scams targeting the older generation. The Yorkshire & Humber Regional Organised Crime Unit is rolling out a programme of crime prevention advice for teens aged 16-18 to schools in the region following a successful pilot with a local academy.

City of London Police has created Cy-Fi Juniors, a fraud and cyber crime education programme for 9-11 year olds, which is being delivered in partnership with Volunteers in Policing. The aim is to reduce the likelihood of young people becoming victims of fraud or cyber crime and to create ambassadors for online safety. It also aims to divert young people from criminal pathways and become a feeder for programmes such as NCSC's Cyber First programme. The initiative is being piloted in the Sir John Cass Primary School in London and will be rolled out nationally through the Mini Police infrastructure.

Several police forces, regional organised crime units and other law enforcement agencies are developing partnerships with universities for volunteers or student placements / internships to assist with fraud and cyber crime initiatives which will raise awareness of fraud and cyber crime and divert young people from criminal pathways.

Crime prevention advice on threats affecting young people is delivered through national social media campaigns. These include the #PhishyFriday campaign to raise awareness of the increasing sophistication of phishing emails and the importance of safeguarding data and installing software and app updates.

City of London Police in partnership with Get Safe Online and the Society of Ticket Agents and Retailers recently undertook a campaign which aimed to directly change online behaviour by demonstrating how easy it is to be tricked into buying fake tickets online. During a series of Facebook flash sales over 1,500 people tried to purchase music tickets from a fake ticket sales website called Surfed Arts. Surfed Arts purported to be a secondary ticket provider and Facebook adverts were targeted at people living in specific areas where there were sold out music events. Those who clicked through to the Surfed Arts website were immediately told they were not able to purchase the sold out event tickets and advised on how to protect themselves from falling victim to real ticket fraudsters in the future.

Legislation has recently been proposed which may prevent the use of 'bots' buying tickets to re-sell at inflated prices, but the threat of bogus ticket outlets remains. Sites like Surfed Arts do not have any tickets to sell in the first place. Buyers pay for what looks like tickets to concerts, festivals or sporting events only for the seller to disappear with the victim's money or send them counterfeited tickets that are not valid for entry. Creation of a national corporate identity assurance mechanism would allow consumers to check legitimacy of "corporate entities" before transacting with them.

Encouraging young people to submit reports of suspicious websites, social media pages or accounts through the Action Fraud online portal will improve the law enforcement response by providing a more comprehensive picture of the threat. It will also enable law enforcement to take action against websites and accounts suspected of enabling fraudulent activity. In 2016/17 City of London Police submitted over 15,000 requests to shut down websites suspected of enabling economic crime.

1. What assessment have you made of the amount of young people:

- Falling victims to fraud, scams and other financial crime?

We are Dom Education Group, we are a training provider of Financial Capability. We deliver classroom based Financial Capability sessions into Schools/Colleges. We have educated over 5000 young people from the ages of 7 – 18 in Kent

In our delivery sessions, the understanding on these topics varies, and in our evaluation process it there is a pattern at the lack of understanding on what these topics are and how they can protect themselves both again fraud/scams/gangs. Also, parent's are unaware of al the issues young people are challenged with.

We have recently introduced a light touch on Money Laundering for Secondary/College students starting with the AML checks for opening bank accounts through to gang grooming and Cuckooing, which are filtering out to Kent/South East from London.

Typically, some areas within Kent and Coastal Towns have high deprivation areas with students/families on very low incomes, leaving them vulnerable to these topics.

- Being involved as a perpetrator or willing accomplice to fraud, scams and financial crime?

  - Lower income families – the need for fast cash
  - Young people do not realise the implications of their actions and are unware that they are taking part in money laundering

- What are the reasons why young people are falling for certain online frauds and scams?

  - Lack of awareness
  - Low income
  - Peer acceptance
  - Low confidence and low self-esteem
  - Money incentives and gifts
  - Vulnerable adults seeking acceptance – wanting a family/stability, (sense of belonging)
  - Peer-pressure, (thinking it is cool to be a part of a gang)
  - Not realising they are assisting an offence
  - Being persuaded online, gangs glorifying money, popularity and gang culture
  - Negative and rebellious attitudes and behaviours
  - Previous history of crime
  - Vulnerability in understanding how criminals are manipulative

- What are the reasons why some young people are becoming perpetrators of fraud and economic crime? Money mules?
  - They are young and vulnerable
  - Targeted marketing through social media
  - Some may come from low economic/disadvantaged backgrounds
  - London gangs targeting other areas to expand into
  - By not having any previous understanding or knowledge of gangs
  - School aged children are being approached outside of school gates
  - Young people do not realise what they are doing – the money that they help to make 'clean' can fund illegalities such as trafficking and terrorism.

- What measures are already in place – across the public, private and third sectors – to help prevent young people from falling victim to financial crime and scams? How effective do you consider these to be?
  - Websites with information –. Not very effective – young people need to be **shown** the consequences of money mules.
  - Don't be Fooled Campaign – good video but not widely used in schools
  - Kent Police Online Information – good resource but most young people will not access
  - NCCU – good resources/information for educators
  -
- What further measures should be in place to prevent this type of crime amongst young people?
  - We are developing a short online learning course on Anti Money Laundering which we aim to deliver to secondary schools/colleges/universities.
  - Information to be shared in schools about Money Mules via video's, activities, social media and previous experiences.
  - Financial Education such as DOMEG to deliver bespoke programmes in school
  - PCSO's to be part of process, informing young people of the serious subject – the school engagement process which was effective has changed and they are unable to fulfil this now
  - ***Students*** *to be made more aware of the importance of money safety and avoidance of criminalisation caused by gangs*
  - **Parents/Teachers/Practioners/Consultants** *to familiarise themselves of early signs of criminalisation upon young people to prompt for necessary intervention. (Parents to be informed about Money Mules at Parent's Evenings) Parents are unaware themselves on the scams/perils so unable to educate their children.*

- What more should government and industry being doing to protect young people from predatory fraudsters and scammers?
  - Informing young people of the consequences by providing first hand experiences of those that have been convicted.
  - Telling young people how money mules are recruited as some young people may not even realise they are being recruited.
  - A website/place where young people can go if they feel they are being recruited by money mules and report it.
  - Nationwide tour of schools offering assembly awareness to whole schools
  - Internet providers to provide families with safer security online
  - Telephone providers to improve security through phones
  - Social Media providers – being more responsive in shutting down adverts to groom young people into gang/crime/drugs/money laundering
  - Police – to support high target schools with a dedicated PCSO
  - Police – to run campaigns from parent's social media e.g. twitter/Facebook.

- What methods in this space are considered good practice and should be replicated more widely?
  - Young people often do not watch tv,news, read newspapers as majority of their media is through social media or YouTube so student friendly campaigns.
  - Current methods include information available on the internet, but it is not usually read by young people as they physically must search for this issue, that they might not even know exists.

- How could the law enforcement response to these issues be improved?
    - Identify and act upon early signs of money criminality
    - Improve powers to shut down social media companies allowing adverts to groom young people into crime
    - Go into schools to receive on the ground information
    - Provide resources to show that crime does not pay

Deborah Domican

Dom Education Group
0330 058 0153
deb@domeg.co.uk
www.domeg.org

FRAUD ADVISORY PANEL

FRAUD ADVISORY PANEL REPRESENTATION 03/18

RESPONSE TO ALL-PARTY PARLIMENTARY GROUP ON FINANCIAL CRIME INQUIRY INTO FRAUD AGAINST YOUNG PEOPLE IN THE UK PUBLISHED ON 14 FEBRUARY 2018.

The Fraud Advisory Panel welcomes the opportunity to comment on the *All-Party Parliamentary Group on Financial Crime and Scamming's inquiry into fraud and scams against young people* published by the All-Party Parliamentary Group on Financial Crime and Scamming on 14 February 2018, a copy of which is available from this link.

This response of 23 March 2018 reflects consultation with the Fraud Advisory Panel's board of trustees and interested members from our fraud prevention and detection group, Future Fraud Professionals Network and our student members. These groups bring together representatives from the public, private and voluntary sectors who have specific interest, experience or expertise in this area.

We are happy to discuss any aspect of our comments and to take part in all further consultations on the issues we've highlighted in our response.

Contents **Paragraphs**

The Fraud Advisory Panel (the 'Panel') is the UK's leading anti-fraud charity.

Established in 1998 we bring together fraud professionals to improve fraud resilience across society and around the world.

We provide practical support to almost 300 corporate and individual members drawn from the public, private and voluntary sectors and many different professions. All are united by a common concern about fraud and a shared determination to do something about it.

For more information, please contact info@fraudadvisorypanel.org

www.fraudadvisorypanel.org

INTRODUCTION

1. With more young people online[1] never has the need been greater to protect them from the growing risks of fraud and financial crime.

2. We remain concerned, however, about the continued use of the word 'scams' to describe fraud which we consider lessens both the seriousness of the crime and its harmful effects on victims. Our use of language in this area is crucial to ensuring that positive initiatives such as this one and the examples provided herein are given the priority and attention they deserve.

3. As part of our deliberations we have identified several overarching themes relevant to this inquiry's questions. Therefore to eliminate the risk of repetition we have grouped our response into two main categories:

   a. young victims of fraud and financial crime; and
   b. young perpetrators of fraud and financial crime.

4. Whilst we have tried to respond to the consultation as fully as possible we have not had the opportunity to give the consultation as much detailed consideration as we would have liked. We would, therefore, welcome the opportunity to be involved in further discussions around what more can be done on this important subject.

RESPONSE TO INQUIRY

A. YOUNG PEOPLE AS VICTIMS

Cyber security by design

5. We strongly believe that prevention should be front and centre in tackling fraud and financial crime within wider society and, more specifically, against young people. The efforts of everyone involved in this space need to be focussed on trying to stop these crimes from being committed.

6. In doing so, one important consideration is the financial circumstances of young people and impact this may have on their online security. For example, for some students starting university or other forms of higher education one barrier could simply be the affordability of anti-virus software which is often sold at an additional cost. This may make it an 'optional (perhaps unaffordable) extra' rather than a 'must-have' safeguard.

7. Government and law enforcement can play an important role here by encouraging organisations to 'do the right thing' and think more seriously about security and protecting people as part of the design process itself – especially for internet enabled devices and social media platforms that can be exploited by fraudsters, but also new banking products.

8. As we noted in our 2017 special report, *Businesses Behaving Badly*, 'in the headlong rush to be first with new products at low prices manufacturers' decisions to cut corners with security

[1] Ofcom (29 November 2017). *Children and Parents: Media Use and Attitudes Report*. Available from https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

and safety are already coming back to bite us. Hackers know that these things are perfect targets; unsecure out-of-the-box thanks to the most basic password security and then largely ignored by their owners.'[2]

9. Many of us are also a bit lazy or lax in changing factory settings so we should make it that people don't need to by encouraging manufacturers to make the default security settings on these devices set to the highest level. Many users would be unlikely to change these and those that did would have to do so manually and accept the risks associated with lower security levels.

10. We should seek to learn from successful crime reduction initiatives used for other crime types to see whether these can be adapted and applied to fraud and financial crime. For example, the UK police flagship crime prevention initiative 'Secured By Design' (SBD) aimed at improving the physical security of new homes. The scheme has been rolled out to some 3,000 properties and over the last 20 years is believed to have resulted in 87% fewer crimes.[3] We see no reason why similar initiatives can't be created for the prevention of online crime and note that there have already been some positive moves in this direction by Government to get businesses to think about 'safety by design' in order to make social media platforms safer to under 18 years olds[4] and urge this work to continue at speed.

11. The endorsement of products which are 'cyber secure by design' by law enforcement in a similar way to the SBD initiative could be a step in the right direction – not only for ensuring a consistent standard for cyber security in the UK, but to also build the visibility and trust of law enforcement among young people.[5]

Tailored education and awareness

12. According to Ofcom nearly all young people aged 8-15 years who use the internet recall being told about how to stay safe online, usually from a parent or teacher. Many also know how to use technical measures to stay safe, such as blocking messages or changing social media settings, but not all have done so.[6]

13. With technology almost second nature to younger people the implementation of fraud and financial crime awareness throughout the education system is paramount. We commend the four anti-fraud lesson plans created by Cifas and the PSHE Association for 11-16 year olds.[7] However fraud and financial crime should not be seen in isolation and closely relates to other existing initiatives within schools such as safeguarding and online 'stranger danger' education. We would encourage fraud to be integrated within these.

[2] Fraud Advisory Panel (2017). Businesses Behaving Badly. Available from https://www.fraudadvisorypanel.org/wp-content/uploads/2017/06/Businesses-Behaving-Badly-July-2017.pdf (page 6).
[3] Secured by Design (March 2018). *21st century crime prevention unveiled as Secured by Design expands its crime prevention initiatives*. Available from http://www.securedbydesign.com/news/21st-century-crime-prevention-unveiled-as-secured-by-design-expands-its-crime-prevention-initiatives/
[4] Department for Digital, Culture, Media and Sport (17 November 2016). *An Internet for Children and Young People*. Speech by Baroness Shields to the Internet Governance Forum. Available from https://www.gov.uk/government/speeches/an-internet-for-children-and-young-people. Also see Department for Digital, Cultural, Media and Sport (07 March 2018). *Secure by Design: Improving the cyber security of consumer Internet of Things report*. Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
[5] Hough, M (2012). *Researching trust in the police and trust in justice: a UK perspective.* Available from http://eprints.bbk.ac.uk/5039/1/5039.pdf
[6] Ofcom (29 November 2017). *Children and Parents: Media Use and Attitudes Report*. Available from https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf
[7] Cifas (2018). *Anti-fraud lesson plans - Working together to teach young people about fraud.* Available from https://www.cifas.org.uk/insight/public-affairs-policy/anti-fraud-lesson-plans

14. In order to be truly effective, awareness and preventative campaigns and advice aimed at the younger population must be tailored to their needs. Advice should be targeted in a ways that it is easily relatable, easily accessible (for example using popular social media platforms like Snapchat or TV which is still used by more children than any other device for watching content[8]) and easily understood. Complex language and messaging are unlikely to encourage engagement.

15. According to the Department for Education about one-fifth of pupils in primary schools are potentially exposed to a language other than English in their home; for secondary schools this is about 16%.[9] Therefore it might also be advantageous to consider the production of prevention advice in various languages.

16. Parents play a vital role here and need to be equipped with the latest information available. According to research by Ofcom parents often use a combination of approaches to manage their children's internet use including regularly talking to them about staying safe online, using technical tools, supervising their child and using rules. While two-fifths use home network-level content filters one-in five think their children will be able to bypass them.[10]

17. Finally we note that education is a life-long process and does not just stop with young people. We should therefore encourage fraud education for all segments of the UK population. We, along with others, have repeatedly called for a well-funded and sustained public education campaign to help people understand and tackle fraud risks online and in the real world[11] and to empower them to protect not only themselves, but also their family, friends and work colleagues.

Opportunities to promote safeguarding messages

18. We would like to see preventative information being provided at the point of purchase of any new internet enabled device. Other delivery channels could include the use of advertising on public transport and peer group interactions. The latter is, we believe, ideally suited to the education system and could include collaboration between peer groups and law enforcement to disseminate the prevent message. We are aware that this is already happening in at least one university.

19. There needs to be a consistent and unified approach to reaching out to young people through schools and universities. Students will have their own bank accounts and will need to manage their own finances and may therefore become more vulnerable to various forms of fraud and financial crime.

20. Why do young people take the risk of oversharing information online? One explanation could be that they receive a high level enjoyment in the activity itself because of the sense of social inclusion it affords them.[12] This needs to be addressed in any awareness raising or educational activities.

[8] Ofcom (29 November 2017). *Children and Parents: Media Use and Attitudes Report*. Available from https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf
[9] The Department for Education (2017). *Schools, pupils and their characteristics: January 2017.* Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650547/SFR28_2017_Main_Text.pdf
[10] Ofcom (29 November 2017). *Children and Parents: Media Use and Attitudes Report*. Available from https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf
[11] Fraud Advisory Panel (2016). *The Fraud Review: Ten years on*. Available from https://www.fraudadvisorypanel.org/wp-content/uploads/2016/06/The-Fraud-Review-Ten-Years-On-WEB.pdf.
[12] Lévesque, F.L., Fernandez, J.M. and Batchelder, D., 2017. *Age and gender as independent risk factors for malware victimisation.* Available from http://hci2017.bcs.org/wp-content/uploads/BHCI_2017_paper_60.pdf

B. YOUNG PEOPLE AS PERPETRATORS

21. According to Cifas figures there was a 75% increase in the misuse of bank accounts involving 18-24 year olds during the first nine months of 2017 – most commonly through acting as a money mule.[13]

22. When a young person lets their bank be used by a 'friend' or acquaintance without realising it was for criminal purposes – are they a victim or a perpetrator, or both? We believe that it is important not to lose sight of questions such as this.

23. Showing how a young person's future may be affected as a result of committing an offence (regardless of whether this was unwittingly or knowingly) – for example the risks of a criminal record, bad credit rating and problems securing financial products in future to rent a flat or buy a car etc. – could be powerful and stark reminder that there are negative consequences to an action they may only consider as a small risk.

24. Our earlier paragraphs highlight some of the ways that we can help young people avoid becoming victims however these methods can also be applied equally to prevent them becoming perpetrators.

25. Fraud Advisory Panel members are seasoned counter fraud professionals who work to advise on the prevention, detection, investigation and prosecution of fraud and financial crime. We subscribe to the joined up approach and believe that a clear, concise and consistent message which is tailored to the young person will be beneficial to this ongoing work.

[13] Cifas (16 February 2018) email communication about The All-Party Parliamentary Group on Financial Crime and Scamming.

JULIE LLOYD - HERTFORDSHIRE POLICE

1. What assessment have you made of the amount of young people:

a) Falling victims to fraud, scams and other financial crime?

We receive less reports from young people than adults. I think young people are less actively targeted probably because they are less likely to have large sums of money. Adults/older people tend to be wealthier.

2. What are the reasons why young people are falling for certain online frauds and scams?

Naivety, primarily. Also, they are familiar with always being online, so feel comfortable and possibly overly confident about interacting online with other people. When it comes to making a purchase, they are looking for a bargain but not asking for advice or considering why that item is being sold cheaply. They don't necessarily read the small print, so might go outside of terms and conditions or recommended procedures, and then find that they have been manipulated into sending money to someone they shouldn't.

3. What are the reasons why some young people are becoming perpetrators of fraud and economic crime? In particular money mules?

Less life experience, hence less empathy for victims or consideration of the impacts/consequences of their actions – attracted by "easy money" - more reckless! (and possibly some ignorance of the law, when it comes to money mule activity)

6. What further measures should be in place to prevent this type of crime amongst young people?

Inputs at schools (if it doesn't already happen) – standard lesson plans for different age groups. Also, maybe standard plans for activities for youth groups like scouts, explorer scouts, cadets, etc. Online advice through the banks via online banking for young peoples' online accounts.

7. What more should government and industry being doing to protect young people from predatory fraudsters and scammers?

Difficult, as the internet is hard to police. However, online sales/auction sites could maybe work to make some of the anti-fraud advice more obvious. Banks could maybe put clear anti-money mule advice when people log onto their online banking, with a "click to say you've read this".

10. How could the law enforcement response to these issues be improved?

Action Fraud could answer the phone rather than cut people off! Local officers and PCSOs have no idea of the levels of fraud in their areas because fraud is no longer on local police systems, all the fraud records are kept at Action Fraud, hence a PCSO can see all the crimes that happened in their area over the last few days, but cannot see any frauds, so they don't even know it has happened, hence the national response is a standard letter (probably the same standard letter an adult would get) and the local response is non-existent. Hardly any online frauds get investigated, so the proportion of frauds impacting on young people that get investigated is probably 2% or something, hence they could lose confidence in law enforcement.

Young People Inquiry | All Party Parliamentary Group on Financial Crime and Scamming | March 2018 | Keep Me Posted UK response

Keep Me Posted UK asks the All Party Parliamentary Group (APPG) on Financial Crime and Scamming to consider the role of paper bills and statements in the prevention of financial crime and scamming.

Keep Me Posted UK asks the APPG to recommend to the Government that they legislate to enshrine the consumer's right to choose, without penalty, paper bills and statements into UK law.

Keep Me Posted UK asks that the APPG recommend to the Government that, until relevant legislation protecting the consumer's right to choose, without penalty, paper bills and statements, government should work with industry and regulators to encourage access to such billing methods.

Background

Many service providers in the United Kingdom now require their customers to access important personal data online by imposing charges for paper bills and statements. Whilst government departments do not impose charges for accessing information online, often individuals are forced online without being given the choice. For some people online is not an option which leads to digital exclusion. The pursuit of digital innovation has led to a reduction in consumer choice.

About Keep Me Posted UK

Keep Me Posted is not an anti-digital campaign – it is pro-consumer choice.

Launched in July 2013, the Keep Me Posted campaign is a coalition of over 100 leading charities, consumer organisations, trade unions and businesses, fighting to ensure that service providers and government departments offer consumers the choice to receive paper bills and statements. The Money Charity, the Money Advice Service, The National Consumer Federation and the Trade Union Congress are but a few of the household names which form the campaign's broad coalition of supporters.

We are proud to be supported by the Credit Industry Fraud Avoidance System (CIFAS).

To date, 30 of the UK's service providers have been awarded a Keep Me Posted "Best Practice" Mark of Distinction[1] including the Royal Bank of Scotland, Barclays, HSBC and Natwest. Five local councils in the United Kingdom have been awarded the Mark including Edinburgh, City of Bradford Metropolitan District Council, Cornwall Council, Chester East Council and South Lanarkshire Council.

We continue to engage government, Members of the House of Commons and Lords, local government, the devolved bodies and regulators to encourage legislative reform.

[1] The Keep Me Posted Best Practice Mark of Distinction recognises service providers who offer all consumers the right to receive paper bills and statements without imposing charges or other penalties, without removing paper or altering frequency unless there is prior consent and without removing continued online access.

Independent research

Two pieces of research underpin this consultation response which were conducted independently of the Keep Me Posted campaign. The first piece which is summarised below is a study by London Economics from 2015 - Managing money online – working as well as we think*?* The second piece was conducted by Two Sides in 2017 titled Print and paper in a digital world; an international survey of consumer preferences, attitudes and trust.

London Economics and YouGov research summary

London Economics conducted a behavioural economics study to determine how the method by which people receive information, in this case financial information, influences their understanding of the information, the choices they make and the actions they take.

Data was collected by YouGov in October 2014 from 2, 399 consumers. Half of those invited to participate were sent a mock bank statement and a notice of changes to overdraft fees by post, while the other half were sent the same information electronically.

The study concluded that consumers were better able to understand information, make better choices and were more likely to take action when transactional information is received by post rather than electronically.

Consumers had a greater understanding of their finances when in receipt of a paper statement:

- 82% of the respondents in receipt of a paper bill correctly identified how much money was in their account at the end of the study in comparison to 32% in receipt of a digital bill.
- 75% of the respondents in receipt of a paper bill correctly assessed the financial health of their account in comparison to 48% in receipt of a digital bill.
- 71% of the respondents in receipt of a paper bill correctly identified the largest payment into the account during the statement period in comparison to 30% in receipt of a digital bill.

The research indicates that receiving correspondence may help people avoid detrimental situations such as falling victim to scams or fraud.

Two Sides research summary

In June 2017, a survey of over 1, 070 UK consumers was conducted on behalf of Two Sides by leading research company Toluna. The survey provides unique insight into how print and paper is viewed, preferred and trusted by consumers in today's digital world.

The data from Two Sides , within the 18-24 sample of 10, 763 consumers, will be referenced throughout this response. Young people, aged 18-24 made up 11% of the sample or 1, 315.

Consultation approach

Our response considers how paper bills and statements can be used to avoid fraud for victims *only* and will not take a view on ways to reduce the number of perpetrators. As such, we will respond to questions 2, 4, 6, 7 and 8. Questions 6 and 7 will be answered together.

Inquiry questions

Question 2: What are the reasons why young people are falling for certain online frauds and scams?

Young people are unable to access the tools, which allow them to effectively manage their finances. Keep Me Posted believes that one fundamental tool particularly lacking for younger consumers is access to paper bills and statements which, in turns, increases the chance of financial mismanagement, disengagement and a greater chance of being susceptible to fraud.

Young people, in particular, are at a greater risk of falling for online frauds and scams as a result of;

- attitudes to print and digital,
- the drive to digital and the specific targeting of young people,
- digital overload,
- digital exclusion and
- attitudes to safety and security.

Keep Me Posted advocates the use of paper bills and statements to allow a greater understanding, as demonstrated by the London Economics research, and to manage their financial affairs more effectively in order to decrease the number of young people falling for online fraud and scams.

Attitudes to print

The greater the importance attached to a document, the greater the likelihood of young people preferring to receive the document in paper format to a digital format. Interestingly, 47% of those young people surveyed by Two Sides in 2017 agreed that they find it easier to manage their finances when in receipt of a paper bill or statement.

However, for bank statements, only 27% of young people prefer print versus 73% who prefer digital whereas, for those surveyed who were over 55, 40% prefer print as opposed to 60% who prefer digital.

For council tax statements, 53% prefer paper as opposed to digital.

For personal information received from doctors and hospitals, 60% of those surveyed by Two Sides prefer to receive the document in paper format as opposed to 40% who prefer digital.

Consumer choice remains important to young people and there has indeed been an increase on how much emphasis is placed on the availability of paper bills and statements. 85% of young people surveyed

agree that they should have the right to choose how they receive communications from financial organisations and service providers; a 28% increase since 2013.

Evidently, there is a generational trend towards the amount of importance placed by young people towards their bank accounts and we are concerned to see that this is lower than other important documents. This generational trend increases the risk of young people falling victim to fraud and scams.

Keep Me Posted advocates for a targeted educational campaign to highlight the importance of paper statements and consumer choice in light of 47% of young people agreeing that they find it easier to manage their finances when in receipt of paper bills and statements.

The targeting of young people in the drive to digital

Young people are specifically targeted through the drive to digital as they enjoy higher levels of digital skills than older generations.

According a study conducted by Copenhagen Economics in December 2017, there has been a decrease of business and government mail from 100% of all communications in 2001 to roughly 38% in 2012 for those aged between 16 and 44 and 75% of over 45s.

According to PwC study in 2013, 16 to 24 year olds are sent 4% of transactional mail despite representing 15% of the population whereas those in the 55-64 age bracket are sent 27% of transactional mail and represent 14% of the population.

Many businesses assume that younger consumers, with higher levels of digital engagement, are able to manage their financial affairs when in receipt of e-billing. However, as our research evidences, young people, and consumers more broadly, are able to engage with their finances more effectively when in receipt of paper bills and statements which in turn will allow them to be less susceptible to fraud.

Digital overload

74% of younger people, surveyed by Two Sides in 2017, agreed that they spend too long on electronic devices as opposed to 29% of the over 55s. 42% agreed that they are suffering from digital overload.

Keep Me Posted advocates for a targeted educational campaign to highlight the importance of paper statements and digital overloading in light of 47% of young people agreeing that they find it easier to manage their finances when in receipt of paper bills and statements.

Keep Me Posted advocates that young people should be offered, without penalty, access to paper billing and statements.

Digital exclusion

Financial and digital exclusion are intrinsically linked. According to the House of Commons Library Briefing Paper Financial Inclusion (Exclusion) from 2017, 12 million people live in rural or remote areas of the UK which lack digital connectivity and 9.5 million people have a lack basic skills which limits their use of online financial services.

On the one hand, young people are digitally overloaded but on the other hand there are those with no access or a lack of digital skills to access e-billing and are therefore, as evidenced by the London Economics research, more susceptible to fraud and scams.

Keep Me Posted advocates that, in light of digital exclusion, young people should be offered, without penalty, access to paper billing and statements to increase their understanding of their finances and decrease the chances of falling victim to fraudulent activity.

Inaccessible digital devices

According to Bradford based debt charity, Christians Against Poverty (CAP), young people are three times more likely to have a smart phone than those aged 41-64. The same study found that 18% of young people who use CAP's services only have access to the internet through their smart phone.

The London Economics research evidences that consumers have greater difficulty managing their financial affairs through e-billing at a desktop computer. It is reasonable to suggest that the difficulty is only increased when accessing e-billing through a smartphone which is often smaller in size and less accessible as a digital device.

Keep Me Posted advocates that young people, and indeed all consumers, should be offered, without penalty, paper bills and statements as the tools used to access e-billing are often inadequate to manage financial affairs and increase the chance of a young person being susceptible to fraud.

Attitudes to safety and privacy

Attitudes towards online safety and privacy are also considerably more relaxed among younger people. A lack of vigilance towards safety and privacy increases the likelihood of becoming a victim of scams and fraud. 57% of those surveyed by Two Sides agreed that they are increasingly concerned with information held electronically being hacked, stolen, lost or damaged in comparison to 77% of those over 55.

Keep Me Posted advocates for a targeted educational campaign on the importance of online privacy and security.

Keep Me Posted advocates that young people, and indeed all consumers, should be offered, without penalty, paper bills and statements.

**

Question 4: What measures are already in place– across the public, private and third sectors – to help prevent young people from falling victim to financial crime and scams? How effective do you consider these to be?

Across business and government, we find that there is a lack of consistency with service providers offering paper bills and statements.

As mentioned in the introduction, the Keep Me Posted campaign has awarded the Keep Me Posted Best Practice Mark of Distinction to thirty service providers who have confirmed their commitment to offer, without penalty, paper bills and statements to consumers.

Recipients of the campaign's Mark include HSBC, Barclays, the Royal Bank of Scotland, Natwest, First Direct, Ulster Bank, the Scottish Building Society, Principality Building Society , the Progressive Building Society, M&S Bank, Northumbrian Living Water, Essex and Suffolk Water, Yorkshire Water, Welsh Water, Severn Trent Water, Bristol Water, Dee Valley Water, Wessex Water, Thames Water, OVO Energy, Grattan, Freemans, Damart, Post Office telephones, Edinburgh Council, Leeds City Council, City of Bradford Council, South Lanarkshire Council, Cornwall Council and Cheshire East Council.

Although a considerable proportion of industry agrees with the Keep Me Posted campaign, there are numerous industries underrepresented in the above list including telecommunication and energy firms.

The London Economics study demonstrated that consumers manage their financial affairs more effectively when in receipt of a paper bill or statement and have a greater understanding of their finances, which subsequently decreases their risk exposure to financial crime and scamming.

Keep Me Posted believes that organisations committing to offering their consumers, without penalty, paper bills and statements are an effective way to prevent young people from falling victim to financial crime.

Keep Me Posted advocates that young people, and indeed all consumers, should be offered, without penalty, paper bills and statements.

**

Question 6: What further measures should be in place to prevent this type of crime amongst younger people? Question 7: What more should government and industry be doing to protect young people from predatory fraudsters and scammers.

Keep Me Posted UK asks the All Party Parliamentary Group (APPG) on Financial Crime and Scamming to recommend to the Government that they legislate to enshrine the consumer's right to choose, without penalty, paper bills and statements into UK law.

Keep Me Posted UK asks that the APPG recommend to the Government that, until relevant legislation protecting the consumer's right to choose, without penalty, paper bills and statements, government should work with industry and regulators to encourage access to such billing methods.

**

Question 8: What methods in this space are considered good practice and should be replicated more widely.

As mentioned in the introduction and in response to question 4, the Keep Me Posted campaign awards the Keep Me Posted Best Practice Mark of Distinction to those service providers who affirm their commitment to offering, without penalty, paper bills and statements.

Consumers are at less risk of financial detriment, for example fraud and financial scamming, when in receipt of paper bills and statements and, as such, we advocate that service providers offer, without

penalty, paper bills and statements, which will, in turn, decrease the risk of becoming a victim of financial crime and scamming.

Keep Me Posted UK asks the All Party Parliamentary Group (APPG) on Financial Crime and Scamming to recommend to the Government that they legislate to enshrine the consumer's right to choose, without penalty, paper bills and statements into UK law.

Keep Me Posted UK asks that the APPG recommend to the Government that, until relevant legislation protecting the consumer's right to choose, without penalty, paper bills and statements, government should work with industry and regulators to encourage access to such billing methods.

Conclusion

Consumers manage their financial affairs more effectively when they are in receipt of paper bills and statements, which, in turn, decreases the risk of detrimental situations such as fraud. Young people are disproportionately affected by the switch to digital e-billing which increases the risk of falling victim to scams and fraud. Keep Me Posted unequivocally advocates for the use of paper billing to increase financial understanding and decrease the likelihood of young people falling victim to scams and fraud.

Thank you for encouraging the Keep Me Posted campaign to participate in this consultation. We hope you find the comments included above useful. The campaign would be happy to discuss any of these points in more detail with officials as your thinking develops.

***Further information** – If you require further information on the Keep Me Posted campaign, please contact Dominic Stewart on 020 7449 8259 or at Dominic@keepmeposteduk.com.*

Sources

Making money online – working as well as we think? A behavioural economics study for the Keep Me Posted campaign, London Economics (2015)

http://keepmeposteduk.com/sites/default/files/Final%20report%20%28190115%20REVISED%20EXECSUM%29%20126pp.pdf

Financial Inclusion (Exclusion) House of Commons Library Briefing Paper, House of Commons Library (2017)

http://researchbriefings.files.parliament.uk/documents/SN03197/SN03197.pdf

Print and Paper In A Digital World, Two Sides (2017)

http://twosides.info/includes/files/upload/files/UK/Research/Two_Sides_Print_and_Paper_In_A_Digital_World_UK-edition-websit.pdf

Offline and shut out, Christians Against Poverty (2017)

https://capuk.org/connect/keep-up-to-date/blog/offline-and-shut-out

The Future Of The European Mail Market, Copenhagen Economics (2017)

PSHE Association response to the APPG on Financial Crime and Scamming inquiry into young victims of financial crime

March 2018

Background and overview

1. The PSHE Association is the national body for personal, social, health and economic (PSHE) education in England, providing advice and support to a network of over 20,000 teachers and other professionals working in schools nationwide[1].

2. PSHE education is a non-statutory curriculum subject which covers the knowledge, skills and attributes all pupils need to develop in order to keep themselves healthy and safe and to prepare them for life and work in modern Britain. Evidence shows that well-delivered PSHE programmes have an impact on both academic attainment and non-academic outcomes for pupils, particularly the most vulnerable and disadvantaged[2].

3. PSHE explicitly covers aspects of personal financial education (such as saving and budgeting) as well as development of broader knowledge, skills and attributes which ensure young people understand risks and make informed decisions. This includes developing digital literacy skills to determine risks from genuine opportunities online.

4. To assist this we have worked with Cifas on a suite of PSHE lesson plans focussed on raising awareness and tackling fraud, scams and contributory factors. The lessons cover such aspects as keeping online information secure, money mules and social engineering. All lessons are intended to develop the skills of risk assessment, decision making and digital literacy to enable young people to protect themselves and others from fraud. These lessons have proven popular with schools.

5. To make this learning universal however PSHE education needs to be on a statutory (compulsory) footing like other subjects. Many schools teach high quality PSHE, but without statutory status curriculum time and consistency of provision suffers. The APPG on Financial Education for Young People recommend statutory PSHE[3] in order to deliver high quality financial education for all. The government are currently considering introduction of statutory PSHE to help consistency of provision across all schools and are expected to arrive at a decision over the coming months.

6. A recommendation from the APPG on Financial Crime and Scamming for statutory status for PSHE education would provide considerable additional weight to the argument for this area of the curriculum to be strengthened, and help ensure all young people learn about these vital topics at school.

What assessment have you made of the amount of young people:

a) Falling victims to fraud, scams and other financial crime?

b) Being involved as a perpetrator or willing accomplice to fraud, scams and financial crime?

7. Our knowledge regarding the high numbers of young people both falling victim to fraud and becoming perpetrators of fraud comes mainly from collaboration with Cifas on lesson plans to address the issue,

[1] *https://www.pshe-association.org.uk/*
[2] *Curriculum for Life: the case for statutory PSHE education https://www.pshe-association.org.uk/curriculum-and-resources/resources/curriculum-life-case-statutory-pshe-education*
[3] *https://www.young-money.org.uk/policy-campaigning/pfeg-and-parliament/appg-financial-education-young-people*

and the research they have produced (e.g. Fraudscape). This has identified, for example, that people are becoming victims of fraud at a younger age – with a 34% increase in the number of younger victims between 2014 and 2016.

What are the reasons why young people are falling for certain online frauds and scams?

8. Lack of digital literacy is a key concern. Despite young people being 'digital natives', they are not necessarily equipped with the critical thinking skills and digital literacy to recognise trustworthy and untrustworthy sources of information.

9. Young people are also still unclear about what information is suitable to share publicly online and which should be kept private. They can also be naïve to the ways in which social media profiles, for example, can be exploited by fraudsters using social engineering techniques such as phishing. Parents can often feel ill-equipped to deal with the complexities of the online world, so expect schools to play an important role. 92% of parents think all schools should teach PSHE education[4].

10. The importance of digital literacy is growing exponentially as digital technologies become the primary source of information and news, as well as significant sites of social interaction. Digital literacy should enable young people to critically engage with technology and develop an awareness of the factors which shape the ways in which technology conveys information and meaning[5].

11. As the National Literacy Trust have identified[6] , PSHE education provides an ideal place on the curriculum for covering content relevant to digital literacy – including learning about power, persuasion and influence.

12. The House of Lords Communications Select committee defined digital literacy as "the skills and knowledge to critically understand the internet."[7] The committee asserted that this should "…sit alongside reading, writing and mathematics as the fourth pillar of a child's education" and recommended that the Government makes PSHE education 'a statutory subject, inspected by Ofsted' to develop a holistic digital literacy that helps children and young people 'critically understand the internet' and ensure that online responsibilities, social norms and risks are covered on the curriculum in all schools.

13. The Computing curriculum is not the best place for educating young people about digital literacy. Much of what young people need to learn to stay safe and aware online is not about how to use technology, nor how technology works. It is learning about much broader knowledge and skills that are developed through PSHE – e.g. understanding risk, understanding peer influence, communication skills – which have little to do with technology.

What are the reasons why some young people are becoming perpetrators of fraud and economic crime? In particular money mules?

14. Young people need further education to develop skills related to risk assessment and decision making, and to understand the consequences of the financial decisions they make. This is increasingly important as

[4] *https://www.pshe-association.org.uk/sites/default/files/u18202/Results%20for%20PSHE%20Association%20%28Parents%29%20-%20England.pdf*
[5] *Hague, C., & Payton, S. (2010). Digital literacy across the curriculum*
[6] *National Literacy Trust, Fake News and Critical Literacy evidence review: https://literacytrust.org.uk/policy-and-campaigns/all-party-parliamentary-group-literacy/fakenews/*
[7] *House of Lords Communications Select Committee report - Growing Up with the Internet: https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm*

the environment becomes more complex and sophisticated. Young people may often engage in activities such as becoming a money mule without knowing that what they are doing is illegal. They are also potentially at risk of responding to peer influence / peer pressure from others who may persuade them to act in this way.

15. Research also suggests that young people do not consider many fraudulent actions as 'fraud', but instead think of them as a small 'white lie', for example using their parents' details to apply for car insurance or taking out insurance after breaking their mobile phone, so again, may unwittingly carry out these types of fraud without recognising the potential risk to themselves and others.

What measures are already in place – across the public, private and third sectors – to help prevent young people from falling victim to financial crime and scams? How effective do you consider these to be

16. We are privelaged to have worked with Cifas to design four lessons for secondary school students to be delivered within PSHE education lessons. Two lessons for key stage 3 explore what fraud is, and how to keep online information secure. Two lessons for key stage 4 explore money mules and social engineering techniques. All lessons are intended to develop the skills of risk assessment, decision making and digital literacy to enable young people to protect themselves and others from fraud.

17. These resources have proven popular, but to ensure all pupils have the opportunity to learn about such vital topics, high quality PSHE through regular, discrete lessons needs to be a fixture in all schools. Statutory status for PSHE education is a requirement in order to achieve universal, high quality provision.

What measures are already in place – across the public, private and third sectors – to help prevent young people from getting criminally involved in financial crime and scams? How effective do you consider these to be?

18. See above

What further measures should be in place to prevent this type of crime amongst young people?

19. Speaking specifically on education, if PSHE education were statutory, all pupils could benefit from lessons on vital topics such as fraud and scamming, and the underlying skills to avoid these issues. Taking a preventative and protective approach to an issue such as fraud, and teaching young people about both the risks and consequences of fraudulent actions, is likely to be far more effective than punishing those who become involved after the fact.

20. Relevant earning should begin in primary schools. For example the PSHE Association Programme of Study framework for PSHE suggests starting to explore and critique how the media present information at primary level so that there is a foundation on which to build when pupils make the transition to secondary. This is why we are and others - including organisations such as Young Enterprise (incorporating Young Money) are calling for statutory (compulsory) PSHE education from key stage 1.

21. In a recent letter to the Department for Education, Bank of England Chief Economist Andy Haldane urged statutory status for PSHE education, saying that "The role of PSHE is fundamental, the Bank believes to making progress in providing a strong educational foundation in economics and finance"[8]. The Church of England also recently urged government to place more emphasis on financial education through PSHE[9].

What more should government and industry being doing to protect young people from predatory fraudsters and scammers?

22. Our recommendations in this response concern education – and specifically the need for government to ensure PSHE lessons are compulsory in all schools – so that all pupils are prepared to recognise suspicious websites, know what sort of data is appropriate to publically share, understand the impact of their digital footprint and online reputation.

What methods in this space are considered good practice and should be replicated more widely?

23. Again, specifically regarding education, as with many other areas of life relevant to PSHE, (e.g. drug and alcohol education) teaching young people about issues such as fraud – and furnishing them with the skills to recognise and avoid it – before they come into contact with it is the most effective way to protect them if an issue arises.

24. PSHE education should begin in primary schools and carry on until pupils leave secondary education. PSHE should be delivered through regular, discrete lessons on the timetable and as with other school subjects it should be developmental in nature, building on prior learning as pupils progress through school. This is the case in many schools, but not all, due to PSHE education's non-statutory status.

25. The All Party Parliamentary Group on Financial Education for Young People agrees that PSHE education, on a statutory footing from key stage 1, is the best context for financial education. The Group made this point in its 2016 report 'Financial Education in Schools: Two Years On – Job Done?'[10] and it has been reiterated recently by APPG Chair Julian Knight MP.

[8] *https://www.bankofengland.co.uk/news/2018/february/department-of-education-consultation-response*
[9] *https://www.telegraph.co.uk/news/2018/03/03/learning-finance-important-sex-education-says-church-england/*

[10] *https://www.young-money.org.uk/policy-campaigning/pfeg-and-parliament/appg-financial-education-young-people*

FALCON

All Party Parliamentary Group - Inquiry into Young People Fraud and Scams

1. What assessment have you made of the amount of young people:

a) Falling victims to fraud, scams and other financial crime?

b) Being involved as a perpetrator or willing accomplice to fraud, scams and financial crime?

The National Fraud Intelligence Bureau (NFIB) would be best placed to provide figures relating to the volume of under 25 year old victims who have reported fraud against them and subsequently under 25 year old suspects involved in such crimes.

For the year end of 2017 The Metropolitan Police Service received 8,041 fraud related crimes into our system, of which 1,057 were victims under the age of 25 that equates to 22%. In addition 1,074 under 25 year olds were suspected of committing the crimes, therefore 23% of the total amount. It is worthy to note that the age range for the suspects maybe estimated by the victim therefore cannot be totally relied upon to be accurate. Secondly, owing to Home Office counting rules, the crimes are disseminated to the geographical area of the line of enquiry, which means that the victim could in effect be located anywhere in the UK or even outside of the UK.

2. What are the reasons why young people are falling for certain online frauds and scams?

Anecdotally, the reason why many young people are falling for certain online frauds is partly due to the vast acceptance and trust of social media communications like Facebook, Instagram, Snapchat and other online forums. Fraudsters use these forums and their fluid connectivity to post adverts offering the opportunity to make ‘easy money’. In some cases the enticement and visual representation can be appealing. Today’s generation who frequently use these types of social media platforms have a perceived large circle of ‘friends’. These are of course ‘online friends’ of which you could argue that in reality, are people who they have never physically associated with other than through an online existence.

In the English Oxford Dictionary the term ‘friend’ is defined as ‘a person with whom one has a bond of mutual affection’ it also goes onto to say ‘a person who is not an enemy or opponent; an ally’ thus engendering an element of trust. In the cyber world however the term friend has been over used and misconstrued. Historically, pre-computers when you met someone your natural ‘instinct’ would tell you how comfortable you are with them, how close you would like to stand next to them, how happy you were to talk to them, what amount of information you would be prepared to disclose to them etc. However, with online communication, these natural instincts do not always kick in and there is less opportunity for the benefit of ‘gut feeling’. With Social Engineering – the physiological manipulation of a person to perform a task or disclose personal or confidential information – we are left with individuals who openly provide private information without thinking about the consequences of who exactly they are communicating with. Fraudsters are not in a rush, they will take a ‘jigsaw’ approach to gaining your information and use it against you for their advantage at some point in the future.

Where technology has advanced with such rapid speed over the last 20 years, there is a distinct divide of lack of knowledge from parent to child learning. The young can be credited for the amount of technical information they know and this is where we see the tables turn with the child teaching the parent, however there is a lack of understanding by the young person of the risks associated with the online world and the tools and techniques the fraudsters use against them.

There appears to be limited coverage in respect of online safety specific to fraud and cyber crime within our Education system which, combined with a lack of personal desire to learn how to protect yourself, provides the fraudsters with an open ended supply of victims.

3. What are the reasons why some young people are becoming perpetrators of fraud and economic crime? In particular money mules?

We are experiencing the first generation where our education or even our everyday learning is online. For Fraud and other cyber enabled crime, the young are learning from peer groups, online forums or the dark web and combined with a general attitude that nobody has told them that it is wrong, individuals are lured, intrigued or encouraged into this type of criminality . Cyber related fraud hides behind a screen; you can achieve it with minimal assets, planning and with limited talent. With no perceived risk and a lack of taking personal responsibility for ones actions, it is seen as an easy way to make money.

With Money Mules, there is no direct link to the actual fraud that has taken place, its targeted victim or the repercussions of it, it is purely seen as transferring money from one account to another. There are a number of ways fraudsters use to get people to move money, from online advertisements to earn ‘easy money’ to genuine looking job adverts for payment assistants, or the recruitment of people where their main objective is to seek out and obtain mule accounts. They often lure people into allowing their account to be used by the offer of money, or making the account holder believe they are doing so as a favour.

4. What measures are already in place – across the public, private and third sectors – to help prevent young people from falling victim to financial crime and scams? How effective do you consider these to be?

5. What measures are already in place – across the public, private and third sectors – to help prevent young people from getting criminally involved in financial crime and scams? How effective do you consider these to be?

This answers both question 4 and 5 together.

Prior to August 2014 it would be fair to say that any ‘Protect’ work around Cyber related crime would have left to individual officers in charge of an investigation providing advice to the victims effected in that case. SC&O7 FALCON (Fraud and Linked Crime Online) was formed in 2014 as part of the MPS response to the evolving threat and increase of Cyber related Crime Offences. FALCON allows the MPS the capacity and capability to investigate cyber dependant and cyber enabled fraud and adapt to the emerging challenges of Cyber Crime.

FALCON takes responsibility for investigating fraud and cyber crime for financial gain referred by the National Fraud Intelligence Bureau (NFIB); secondary investigation of Territorial Policing calls to service and proactively targets Organised Crime Networks engaged in fraud and cyber crime.

Op FALCON bases its operational response to the 4 P’s principles;

Protect - Increase protection from cyber criminals

Prepare - Reduce the impact of Cyber Crime when it occurs

Prevent - Prevent people from engaging in Cyber Crime

(Pursue – Prosecute and disrupt criminal engaged in Cyber Crime)

Within Protect our aim is to identify crimes most affecting the citizens of London and through proactive prevention projects reverse engineer the methodologies, to identity the precursors and enablers. Devise

and deliver tailored and general fraud and cyber security advice, briefings, events, presentations and public campaigns. To target private, public and voluntary organisations, local communities and individuals in order to prevent crime and prevent repeat victimisation.

Through the Prepare strand, we provide advice to businesses and individuals to help them prepare for a Cyber attack, mitigate damage to them and increase their resilience in order to recover from the incident. This is achieved by working alongside businesses and industry experts to assist in delivering cyber-based exercises to test businesses response to a cyber-related attack. Debriefing will focus on capturing learning from these incidents which will, in turn be fed back to the company.

The aim of Prevent is to identify and deter individuals from becoming involved in cyber crime or re-offending. This will be delivery predominantly through two strands, general messaging and targeted interventions from individuals at risk. FALCON actively engage with schools, colleges, universities and other educational establishments to explain the importance of Prevent activities to teachers. Engage with pupils and students to educate them about the risks of cyber crime, to help them protect themselves and deter in the likelihood of becoming engaged in cyber crime.

The responsibility of the Pursue is to, through intelligence identify, group, gather evidence and locate Organised Crime Groups (OCG's) involved in cyber crime. Prepare criminal cases against them and pursue them through the Criminal Justice System.

FALCON has four reactive investigation hubs situated north, south, east and west of London consisting of approximately 20 detectives that deal with crimes reported to Action Fraud. The crimes are filtered through the National Fraud Intelligence Bureau (NFIB) who identify a geographical lead within the MPS. This usually consists of the location of the beneficiary account.

FALCON has produced printed/online resources consisting of Fraud advice with The Little Book of Big Scams and Little Book of Cyber Scams and leaflet Little Leaflet of Cyber Mistakes. These are distributed upon request within the Metropolitan Police area and can be adopted and re-branded by other Police Regional Organised Command Units (ROCU's).

As part of our strategy to help raise awareness, FALCON has produced five animation videos covering Online Identity, Passwords, Free Wi-Fi, Updates and Phishing. A further five animations are due to be released that concentrate on more specific crime types including Money Mules, Online Shopping, Payment Fraud, Computer Software Service Fraud and Romance Fraud.

FALCON Protect strand covers all Fraud, whether cyber dependant or cyber enabled. Current projects include; Payment/Mandate Fraud, Online Shopping, Romance Fraud, Computer Service Software Fraud (CSSF), Courier Fraud, Recruitment Fraud, Investment Fraud and Money Mules as an enabler to all frauds and Safer Neighbourhoods, which is piloting in two Boroughs (Redbridge & Kingston) upskilling Neighbourhood Watch Ward officers in relation to Fraud and Cyber advice. Each project, the officer and team will analyse the complexities of the crime and it's functionality to identify the enabler/s to that fraud type.

Each Project lead will engage with partners within the Public, Private, third Sector organisations and the Education system. A number of activates will include talks, presentations, local events and exhibitions. Partnerships that we work with are all other Police Regional Organised Command Units (ROCU's), National Crime Agency (NCA), National Cyber Security Centre (NCSC), City of London Police, Action Fraud, National Fraud Intelligence Bureau (NFIB), the major Banking institutions, Association Foreign Exchange Partners (AFEP), Cifas, UK Finance, Take five, HMRC, Get Safe Online, Age UK, Online Dating Association (ODA) and Royal Mail Scam Mail. NB. This is no means an exhaustive list.

In addition to the dedicated projects a number of fraud types are covered with advice within our resource books that include; Holiday Fraud, Ticketing Fraud, Online Banking & Card Fraud, Door to Door Fraud, Scam Mail, Wi-Fi Hotspots and Identity Fraud.

To support identity fraud enablers, Amberhill is a department that now comes under FALCON. It was formed in 2008 and its main focus is the disrupt Forgery Document factories. Amberhill Data obtained from the factories is shared with the public & private sector including financial and employment industries. Amberhill carries out document examinations for ongoing investigations for law enforcement, its partners and industry. Measures are in place to safeguard risks in industry of people attempting to use false identification documents.

Past Projects include;

The main enabler for Courier Fraud was the use of a telephone, where the fraudsters utilised the long disconnection facility on a landline to their advantage. Once a fraudster contacted their target with their con of choice, they encouraged the Victim to hang up and dial into a legitimate company/organisations. The fraudsters held the line open, answered the victim's call as if they were from the company/organisation they had dialled and they captured personal data including passwords, PINS and private details.

FALCON officers identified the scale of the crime, the effects of the victim and the financial loss made. With this information, a case was brought to OFCOM to have the phone line disconnection reduced to 2 seconds. This was supported by all the major landline telephone providers and in doing so prevented this type of fraud by 70% overnight.

Fraudsters historically have been tricking vulnerable people in to withdrawing large sums of money from their Bank accounts. FALCON officers looked into this as an enabler and developed an initiative to prevent fraudsters getting victims to make transactions or withdrawals against their own account in branch. The 'Banking Protocol' encourages Bank or Post Office staff suspicious of unusual transaction to ask a series of questions regarding the proposed transaction and if it still remains suspicious to call police, as well as advising the victim against proceeding with the request.

As at the end of February 2018, 44 police forces were live with the Banking Protocol. Through financial institutions and law enforcement working together, in February the Banking Protocol achieved £2.1million in prevented fraud with 16 arrests, bringing the total to date to £16,536,856 and 154 arrests. 2,064 emergency calls have now been placed and responded to, with the average prevention per call equating to £8,012.

With the launch of the Banking Protocol across Scotland on the 5th March this year, we have now achieved national coverage with all 45 Police forces. Initial results across Scotland are exceptionally promising with Police Scotland reporting £44,609 in prevented fraud and 1 arrest in the first 9 days alone.

6. What further measures should be in place to prevent this type of crime amongst young people?

7. What more should government and industry being doing to protect young people from predatory fraudsters and scammers?

This answers both 6 and 7 questions together.

Education from grass roots upwards, primary school through to further education. Cifas in conjunction with the PSHE Association has launched, as of January 2018 a series of Educational lesson plans targeted at 11-16 year olds, key Stage 3 and 4 pupils raising awareness of fraud, common scams, identity fraud and money mules. Whilst there has been to date a good number of downloads of the lessons, actual statistics of how many lessons and therefore how many pupils have been exposed to it is unknown at this stage. Collectively,

we are all playing catch up. Education around cyber security ethics, protecting young people online and the risks exposed together with an essential legal element covering the Computer Misuse Act and Proceeds of Crime offences are paramount in the current climate and the requirement should be mandated.

Financial institutions can play a part in deterring money mules and preventing money laundering by young people by having in place suitable policies for any new accounts for under 18 year old customers. The terms and conditions should be communicated in a way that can be easily understood by the young person, setting out their responsibility to look after the security of their account. In addition, if the banking industry cross-reference the payee details alongside the account number, this would prevent a significant proportionate of mandate/payment fraud being committed.

A Public awareness campaign lead from the Government to instil behavioural change. Delivered for the under 25's on social media/advertising space via pop up banners and You Tube influencers/bloggers etc.

8. What methods in this space are considered good practice and should be replicated more widely?

Exposure to education institutions around cyber knowledge and the risks associated with it is key. Presentations provide face to face opportunities with students, it allows for a personal touch, the opportunity for interaction and questions explored and answered. It is however labour and resource intensive and owing to the high number of establishments within London we respond on a referral basis. This is then supported with literature, posters and or a press release within the mediums of the establishment. Working on projects with partners is paramount, combining communication exposure and best practice. A good example of this is the latest 'Don't be fooled' campaign on Money Mules launched in November 2017 by UK Finance and Cifas.

9. How could the law enforcement response to these issues be improved?

Cyber fraud is fast pace crime, therefore from a reactive point of view, there is too long a delay from the date/time the fraud offence was committed to when it is in a position to be investigated by law enforcement. Action Fraud Reports are victim generated, therefore only completed once they have been made aware the fraud has taken place ie via a bank statement furthermore once the report has been completed by the victim.

The Action Fraud report is submitted to the National Fraud Intelligence Bureau (NFIB) for collation, this takes between 1-2 weeks, once received they are converted and provided with a unique NFRC reference number. A matrix filters out any cases that fall under vulnerability/high value/threats etc leaving the remainder for NFIB to assess if there is a viable line of enquiry to distribute to the relevant force area for investigation. These are received via email and would then need to be converted onto the relevant forces' crime reporting system. On average the reports received from the NFIB are anything from 4 weeks to 3-5 months old plus.

A common fraud investigation will start with the first beneficiary account and a request to the Bank concerned and depending on the account situation this will follow with either a Data Protection Act (DPA) or a Production Order request. This process would have to be repeated for any second beneficiary account identified and so on. In reality, once a person is identified they would be charged with an ancillary offence of Money Laundering, which means the NFIB Fraud crime will remain undetected. The NFIB do not have any system in place to record any victim outcome code that reflects the charge of facilitating the offence of fraud.

Action Fraud are in the process of re-designing the reporting system, it is not known at this stage however how this will affect the working process that are currently in place.

Public and Consumer Affairs

RBS

APPG Young People Inquiry on Fraud and Scams

Written evidence supplied by RBS

Submission Date: 16 March 2018 **Secretariat:** Cifas

Context

The All-Party Parliamentary Group on Financial Crime and Scamming is launching its first inquiry into fraud and scams against young people in the UK. Figures released by Cifas, revealed a 75% increase in the misuse of bank accounts involving 18-24 year olds during the first nine months of 2017, compared to same period last year. The inquiry is seeking views and best practice from law enforcement, industry, the education and voluntary sector, and government on the scale of the problem, how to prevent these crimes amongst young people and how current work can be improved.

NatWest position

Keeping our customers safe and secure and reducing harm from financial crime is a key priority for the Bank. We have invested in systems and controls to protect our customers' information and accounts and also invested in targeted communications to educate our customers and the wider community on how to better protect them against fraud. Research we commissioned last year[1] showed that younger people are less likely to be cautious online compared to older generations which can put them at increased risk of falling victim to online fraud. This trend is particularly notable among youth and student accounts where we are seeing an increase in Money Mule scams. In fact, 30% of our mules are a 'young person' (i.e. hold a youth account) which is disproportionately high when compared to our overall customer base. Given this trend, our response to the enquiry will heavily focus on this issue.

Questions

1. What assessment have you made of the amount of young people: a) Falling Victim to fraud, scams and other financial crime? b) Being involved as a perpetrator willing accomplice to fraud, scams and financial crime?

The increase in fraud and scams is strongly connected with the rise in internet usage - with 90 per cent of UK households increasingly using electronic payments. Research[2] we conducted in 2017 found that 16% of people had experienced online fraud in the past year, and 10% online bank fraud. It also showed that whilst older age groups (66+) are believed to be most vulnerable to online fraud, in reality it is younger people (18-24) who are most at risk as a result of taking fewer precautions to protect themselves.

Our internal analysis of fraud across different customer segments also supports this finding and we found that fraud is quite prevalent among 'Young Potentials' (18-34 yr. olds) with modest incomes and University/Graduates (18- 25 yr. old students). This is where we are seeing a growing trend of young people being persuaded and paid to give access to their bank accounts for fraud and money laundering. Analysis from a 3 month sample of money mule case data from 2017 shows that 33% of confirmed mule accounts are Youth accounts, 3% are student accounts and 63% are personal accounts.

[1] The Policy Network' *It could be you'* report commissioned by NatWest, November 2017
[2] YouGov online survey conducted in England and Wales, June 2017

2. What are the reasons why young people are falling for certain online frauds and scams?

One of reasons is simply a lack of awareness. Young people tend to 'live online' through social media channels and as such are less cautious about sharing personal information. The YouGov research showed that over 80 per cent of 18-24 year olds are willing to share their email address online with their friends, and as many as 29 per cent are willing to share their mother's maiden name (a commonly used security question). This contrasts with just 60 per cent of over-55s willing to share their email address, and only 12 per cent willing to share their mother's maiden name.

Another reason is young people tend not to take proactive steps regarding online security such as downloading the software and tools available to protect their smartphones, ipads or tablets. The YouGov research found that 86 per cent said they would install it on a laptop/PC, but only 57 per cent said they would on a tablet, and just 50 per cent on a mobile phone.

3. What are the reasons why some young people are becoming perpetrators of fraud and economic crime? In particular money mules?

- **New online platforms**

Social media and dating sites are particular targets for fraudsters to gather personal details and gain the trust of potential victims before recruiting 'money mules'. Schoolchildren and students are often targeted by fraudsters to set up and give access to their bank account details. These accounts are then used to transfer funds from money laundering, and also to hold money acquired through other scams. The majority of these cases are advertised on social media as 'cash flips' (see appendix A).

It is important to note that these customers start their relationship with the bank as genuine customers with no apparent intent to support any kind of financial crime. However, they are enticed by posts on social media forums which suggest they can earn money very quickly with no risk to themselves. We believe that they are heavily coached by the organised crime groups and told what to say in response to questions by banking staff.

Social Media Pages are commonly used by criminals to feedback on the success of transactions, or the actions taken by banks to deal with mules. If banks are seen to be a soft target for mule recruitment, this will be fedback to the forums and may lead to an increase in money mules at a particular bank (see Appendix B).

- **School Recruitment**

Social media is not the only way to recruit money mules. Recent developments show that a number of children in Essex and London have been targeted at the school gates and inside school grounds to allow use of their bank accounts and bank cards in return for a fee. As it can be other children asking, they do not see the harm and may allow this. Quite often children are being paid a fee but can also be threatened with violence if they refuse. Schools have begun to write letters to warn parents of the danger but much more needs to be done to prevent this from escalating.

We suspect many children are wilfully blind to the wider implications of their actions and are too focussed on the financial rewards that can be gained from participating in this activity.

Additionally, younger customers may feel as they have nothing to lose from participating in these schemes; they have lower account balances and can easily re-set their password after the transaction.

4. What measures are already in place – across the public, private and third sectors – to help prevent young people from falling victim to financial crime and scams? How effective do you consider these to be?

One of the most important measures is education and raising the awareness of the issue with young people and their families. We believe fraud education from a young age is vital which is why we developed **NatWest Money Sense** – a free financial education programme designed to support kids from 5 – 18yrs with financial capability and fraud education. https://www.natwest.mymoneysense.com. We recently launched a 'Fraud Scene Investigators' workshop, specifically focussed on protecting young school children from scams.

At an industry level, we are fully committed to supporting education initiatives such as Take Five and Friends Against Scams which work well to raise awareness of the issue among key segments.

- **Take Five Campaign:** Launched in 2016, Take Five is a national behaviour change campaign led by UK Finance designed to raise awareness and prevent fraud by asking the public to 'think before they act'. We have leveraged this campaign through our own customer channels since its launch and will continue to support the campaign on phases 3 and 4.

- **Friends against Scams**: We were the first bank to launch this financial education programme with the National Trading Standards Scams Team - a campaign to tackle the lack of scams awareness by providing information and training about scams and those who fall victim to scams. Since its launch in 2016, we trained over 20,000 colleagues to help educate customers and prevent them from falling victim to fraud. This year we pledged to recruit another 20,000 bank colleagues and we're also the official bank partner of the National Trading Standards 'One Million Friends' campaign, which has the support of the Security Minster and the Home Office.

In addition, we have a number of customer facing frontline roles to support community service and outreach. This type of intervention relies on local community intelligence and collaboration - something which is very effective.

- Our team of **Community Protection Managers** help protect customers from financial harm. Their role is to help safeguard customers and to liaise with external organisations like the police, where necessary, to help keep customers and their money safe.

- Our 109 **Community Bankers** provide face to face support for customers and local communities, running financial education events which include digital safety and fraud awareness seminars. Their presentations and drop-in clinics are held across communities in libraries, town halls and schools.

- Our **Business Growth Enablers** support small business customers by providing advice, events and training on how to keep businesses safe from cyber crime.

5. What measures are already in place – across the public, private and third sectors – to help prevent young people from getting criminally involved in financial crime and scams? How effective do you consider these to be?

External Campaigning

In November 2017, UK Finance and Cifas launched the 'Don't Be Fooled' campaign. The campaign deters students from becoming money mules, by educating them about what the term means, how criminals operate, why they are a target and the serious consequences of participating in such schemes. The campaign was launched on social media,

in the national news, through engagement with universities and with the support of social media influencers, including a hard hitting video entitled 'Sponsor a Child Trafficker' which aims to raise awareness of the issues behind money laundering and the implications of funding organised crime. The 'Don't be Fooled' campaign was funded by UK Finance members, including RBS.

Industry Collaboration

We chair the Industry Money Mule Working Group at UK Finance with the purpose of sharing best practice and developing an industry response to the problem. A strategic money mule solution is essential to managing this risk, and a work stream has been established to develop a Payment Data and Transactional Information Sharing solution. This should deliver short term tactical capability to identify suspect mule accounts and trace monies back to victims. However we need additional support from government to support a more strategic solution.

Where an account holder is found to have received and disseminated the proceeds of fraud, and we believe them to be complicit in this, we will raise as Suspicious Activity Report (SARS) in line with Money Laundering regulation and legislation. We will also exit the relationship and load the case to CIFAS. Our terms and conditions make it clear that we will exit the account if we reasonably suspect that the account is being used, or is planned to be used, for an illegal purpose. It is important that we take action against account holders that are involved in laundering money. This is to protect our genuine customers and in order to support the reduction in fraud and scams across the industry.

We are one of 11 banks that have signed up to participate in the delivery of a cross industry Money Mule insights solution with Vocalink and the Faster Payments Scheme that will track the proceeds of crime through the payments network, supporting the identification of mule accounts.

This will enable us to take swifter action against account holders that have been recruited as money mules and develop best practice standards for managing the risk of money mules at an industry level.

Process and Governance

There are also a number of process and governance interventions that we have proactively introduced to detect mule accounts and mule account networks:

- Strengthening controls at on-boarding stage for our most high risk money mule products. Suspicious behaviour is monitored and functionality is restricted
- Investigating mule intelligence received from customers, other banks and law enforcement which leads to account exit and recovery of funds (where appropriate)
- Blacklisting certain money mules within popular payment channels (to prevent payments being made)
- Analysing internal data to proactively identify other accounts linked to organised crime networks
- Introducing training programmes for account opening teams to detect mules and fake documentation
- Collaborating with the Financial Crime and Investigations Unit to increase knowledge and understanding of the nature and scale of the money mule threat to then cascade learnings to front line staff and control teams

6. What further measures should be in place to prevent this type of crime amongst young people?

See answer to question 7.

7. What more should government and industry be doing to protect young people from predatory fraudsters and scammers?

There are a number of areas that should be addressed, some of which have been recommended in the Policy Network 'It could be you' report:

- Ensure the next generation of digital natives know how to stay safe online, stepping up online safety education and ensuring all teenagers complete some form of educational training on scams before they leave school
- Continue to leverage the work of the Joint Fraud Task Force to share best practice across industry, public and private sector
- Invest more in victim-orientated approaches to disrupt scams through the use of financial intelligence
- Engage and have more open dialogue with social media, telecommunications and tech companies to encourage effective ways of preventing their platforms from being used to recruit money mules.

8. What methods in this space are considered good practice and should be replicated more widely?

We introduced a new social media 'takedown' process with an existing vendor, who monitor for brand infringement. Money mule recruiters often post pictures of online banking accounts and cards to evidence that they are legitimate and can make money. These posts often feature the banks brand / logo, which results in the ability for the bank to take action in order to shut down the page.

We also use the information gathered from these pages to investigate any accounts associated to the posts. Once identified, these accounts are investigated and closed down if confirmed mules. We would urge banks to replicate this process in order to target all pages posting different brands and ensure maximum impact. Social media companies and teams should be engaged and made aware of the problem and requested to review reporting guidelines to allow fraudulent activity to be reported and taken down.

9. How could the law enforcement response to these issues be improved?

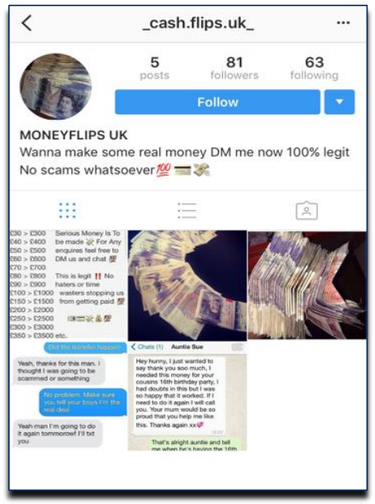
Given the scale of money mule accounts that have been identified across the industry it is not reasonable or practical to expect law enforcement to take action against every account holder. However, as per response to question 7, there are a couple of strategic solutions that could be explored:

- Explore the reallocation of resources and staff into economic crime and explore feasibility of introducing web constables
- Where appropriate, share data and intelligence from social network analysis in fraud investigations to pre-empt new and emerging scams

Law enforcement could use the intelligence gleaned from the network of money mules to help track down and take action against those who are involved in fraud and scams. Specialist law enforcement could also do more to target criminal markets in data and accounts and to identity and apprehend those people creating and profiting from mule accounts sold as a 'crime for service'.

Appendices

A



B

UK FINANCE

UK Finance response to All-Party Parliamentary Group on Financial Crime and Scamming inquiry on fraud and scams against young people in the UK.

16th March 2018

1. INTRODUCTION TO UK FINANCE

UK Finance welcome the opportunity to comment on the All-Party Parliamentary Group (APPG) on Financial Crime and Scamming inquiry on fraud and scams against young people in the UK.

UK Finance is a trade association representing nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association.

Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. Our members' customers are individuals, corporates, charities, clubs, associations and government bodies, based in the UK and overseas, served domestically and cross-border. These customers access a wide range of financial and advisory products and services, essential to their day-to-day activities, from our members. The interests of our members' customers are at the heart of our work.

2. OUR RESPONSE

Question 1: What assessment have you made of the amount of young people:

A) Falling victims to fraud, scams and other financial crime?

Research conducted on the YouGov omnibus in June 2017 found that 16% of people had experienced online fraud in the past year, and 10% online bank fraud. It also showed that whilst older age groups (66+) are believed to be most vulnerable to online fraud, evidence shows that it is, in fact, younger people (18-24) who are most at risk as a result of taking fewer precautions to protect themselves.

One of the reasons for this is younger customers sharing personal and sensitive details with friends in open forums for example and not understanding the repercussions of this, or purchasing goods online for a 'too good to be true' price then realising it was a scam. There are also a growing number of young people being targeted for impersonation fraud due to the amount of sensitive information they inadvertently make available to criminals.

One payment institution's internal analysis of fraud across different customer segments supports these findings and found that fraud is quite prevalent among 'Young Potentials' (18-34), with modest incomes and mortgages and University/Graduates (18- 25-year-old students and recent graduates).

There is also a growing trend amongst this segment of young people being persuaded and paid to give access to their bank accounts for fraud and money laundering, also known as 'money mules'.

Further analysis from a three-month sample of money mule case data from 2017 showed that 33% of confirmed money mule accounts were linked to youth accounts, 3% were student accounts and 63% were personal accounts.

Analysis undertaken over a similar period by another payment institution found that 41% of money mule accounts were linked to young people aged 0-25, 63% were male and 36% of these accounts were open for less than six months.

B) Being involved as a perpetrator or willing accomplice to fraud, scams and financial crime?

See response to question 1.

Question 2: What are the reasons why young people are falling for certain online frauds and scams?

One of reasons is simply a lack of awareness and compulsory education in schools and universities on financial crime and how to operate securely online. Young people tend to 'live online' through multiple social media channels and tend to be less cautious about sharing personal information. And therefore, they are more likely to encounter malicious activity. The YouGov research showed that over 80 per cent of 18-24-year olds are willing to share their email address online with their friends, and as many as 29 per cent are willing to share their mother's maiden name (a commonly used security question). This contrasts with just 60 per cent of over-55s willing to share their email address, and only 12 per cent willing to share their mother's maiden name.

Another reason is young people tend not to take proactive steps regarding online security such as downloading the software and tools available to protect their mobile devices. The YouGov research found that 86 per cent said they would install it on a laptop/PC, but only 57 per cent said they would on a tablet, and just 50 per cent on a mobile phone.

Young people also tend to have less experience of the 'real world' and therefore may be more naïve with regards to how typical frauds and scams operate. And criminals will exploit this, for example, perpetrating scams offering high value and fashionable/popular goods at low prices which unfortunately, attracts low income customer segments such as students.

Question 3: What are the reasons why some young people are becoming perpetrators of fraud and economic crime? In particular money mules?

The use of social media and online job platforms is a very common way for criminals to recruit money mules. There is also evidence to suggest that mule recruitment is prevalent in schools, colleges and universities as well as youth and junior football and rugby clubs; it is likely that there are individuals that are recruited as money mules who do not fully appreciate that they are committing a criminal offence. These mule accounts are used to transfer funds from money laundering, as well as from other scams.

It is important to note that these customers usually start their relationship with the bank as genuine customers with no apparent intent to support any kind of financial crime. However, they are enticed by posts on social media forums which suggest that they can earn money very quickly with no risk to themselves. We believe that they are heavily coached by the organised crime groups and told what to say in response to questions by banking staff. They will also share their experience with friends and fellow students.

However, as mentioned above, it is reasonable to assume that many individuals may be blind to the wider implications of their actions and more focussed on the financial rewards that can be gained from participating in this activity. Additionally, younger customers may feel as they have nothing to lose from participating in these schemes; they have lower account balances and can easily re-set their password after the transaction.

Question 4: What measures are already in place – across the public, private and third sectors – to help prevent young people from falling victim to financial crime and scams? How effective do you consider these to be?

One of the most important measures is on-going education and raising awareness of the issues with young people, their friends and families.

Individuals banking institutions and the banking industry collectively, with support from 3rd parties such as Trading Standards, have and continue to commit and invest in customer education and awareness and this includes targeted campaigns focusing on different customer segments such as university students.

The following are just some examples of this work and effort:

- Take Five to Stop Fraud Campaign: Launched in 2016, Take Five is a national behaviour change campaign led by UK Finance and supported by its members and the Home Office, designed to raise awareness and prevent fraud by asking the public to 'think before they act'. In 2017, Take Five led a campaign on money mule awareness targeted at 18-25 yr. old students. More information is available here https://takefive-stopfraud.org.uk/

- NatWest Money Sense – a free financial education programme designed to support kids from 5 – 18yrs with financial capability and fraud education. An example of this is the 'Fraud Scene Investigators' workshop, specifically aimed at young people protecting themselves from scams used by criminals to elicit personal information. More information is available here https://natwest.mymoneysense.com

- Friends Against Scams: National Trading Standards campaign to tackle the lack of scams awareness by providing information and training about scams and those who fall victim to scams. Since its launch in 2016, over 20,000 banks staff were trained to help educate customers and prevent them from falling victim to fraud. and in 2018, there is a pledge to recruit another 20,000 bank staff.

- Get Safe Online: is the UK's leading source of factual, easy-to-understand information on online safety. And multiple banking institutions and other stakeholders actively support this. https://www.getsafeonline.org/

Question 5: What measures are already in place – across the public, private and third sectors – to help prevent young people from getting criminally involved in financial crime and scams? How effective do you consider these to be?

See response to question 4

Question 6: What further measures should be in place to prevent this type of crime amongst young people?

- Education: the most effective way to prevent this type of crime amongst young people is to focus on mandatory financial education prior to becoming financially active. Education should focus on financial literacy more widely, but should ensure that young people fully understand the repercussions of financial crimes in terms of financial curtailment, criminal sanctions and outcomes for victims.

- Law Enforcement: Additional resource is required to improve the law enforcement response to these types of financial crimes. A greater focus needs to be given to prevention of these crimes and enforcement of criminal sanctions. The more action taken against perpetrators of this type of crime, the greater the deterrent will be for young people.

- Consistent Messages: There is a need to greater collaboration across industry, government and law enforcement to ensure that the messages delivered to young people are consistent. School and university societies, schools and universities need to raise awareness of these types of crime.

- Effectiveness: The effectiveness of these educational initiatives will be somewhat defined by the number of young people that the messages reach. Creative social media campaigns will have a wide reach across the younger generations due to their active online presence. The 'clickbait' style advertising used in the 'Don't Be Fooled' campaign is very effective as not many young people are proactively searching for information and websites on money mules.

Question 7: What more should government and industry being doing to protect young people from predatory fraudsters and scammers?

An ongoing campaign of education and awareness should be deployed to ensure that young people are aware of the risks of becoming a victim of fraud and also of becoming a money mule, including the types of crime and victims that this activity supports.

Additionally, social media corporations should be engaged to prevent their platforms from being used by people to recruit money mules. Previous mule recruitment campaigns focussed on the link between fake job advertisement and money mules. However, 'cashflips' now seem to be the term that is used when recruiting mules on social media. Industry wide communications should highlight how these are used. They should also clearly explain the link between criminality and the consequences of becoming a mule.

Improved collaboration across industry, government and law enforcement to increase the sharing of intelligence on mule networks and scams would also help better protect young people.

There also needs to be an alignment of the on-boarding and transaction monitoring controls that are used across the industry. Greater collaboration should be encouraged to exploit the various initiatives and technologic solutions which are being developed in the digital space to improve the identification of fraud and mule activities. Technical and strategic rules that are being built based on mule herder typologies and profiles should be shared across the industry to help improve the identification of mule rings and networks.

Question 8: What methods in this space are considered good practice and should be replicated more widely?

Some payment institutions use third party security vendors to monitor the internet, including social media platforms for brand infringement. Money mule recruiters often post pictures of online banking accounts and cards to evidence that they are legitimate and can make money. These posts often feature the banks brand / logo, which results in the ability for the bank to take action in order to shut down the page.

The information gathered from these pages can be used to investigate any accounts associated to the posts. Once identified, these accounts are investigated and closed down if confirmed to be money mules. We would encourage others to replicate this process. Unfortunately, current reporting and community guidelines set within the main social media networks don't allow scope to report fraud or money laundering recruitment. Therefore. social media companies should be engaged and made aware of the problem and requested to review reporting guidelines to allow fraudulent activity to be reported and taken down.

Question 9: How could the law enforcement response to these issues be improved?

Law enforcement agencies need increased resource and dedicated units to ensure that mule rings and networks are identified and shut down quickly. Criminal sanctions imposed against perpetrators need to be publicised more widely to act as a deterrent for young people.

Given the scale of money mule accounts that have been identified across the industry it is not reasonable or practical to expect law enforcement to take action against every account holder. However, law enforcement could use the intelligence gleaned from the network of money mules to help track down and take action against those who are involved in fraud and scams.

It is also important to note, however, that money mule accounts obtained or used by criminals may be used to move the proceeds of any type of crime, not just financial fraud scams. Criminals can make use of multiple methods to obtain a network of mule accounts, other than targeting and grooming young or vulnerable people. Methods include creating 'front' accounts in multiple identities or hijacking existing accounts without the knowledge of the person or account holder. Such methods are enabled by the flourishing criminal market in stolen personal data and the criminal use of malware. Some criminals are known to have been able to buy pre-existing 'ready-made' networks of mule accounts, without having to set them up themselves. Specialist law enforcement could do more to target those criminal markets in data and accounts, and to identity and apprehend those people creating and profiting from mule accounts sold as a 'crime for service'.

Written Evidence Submitted by Yoti -Inquiry Response: Young People and Fraud and Scams
June 2018

Introduction:

As a digital identity platform, Yoti shares the concern of the APPG on Financial Crime and Scamming about the impact of fraud and scams on young people and supports the efforts they are making to tackle them.

One of the ways that young people are being affected is by identity theft. CIFAS revealed that almost 175k cases of identity fraud were reported in 2017, a 125% increase compared with 10 years ago; in 95% of the cases the fraudsters used the victim's identity and in 4 out of 5 cases the victim's real address was used. It is likely that many low value frauds are not reported to CIFAS, Action Fraud or the Police.

There is strong potential for technology and innovation to assist those committed to combating economic crime and 12 areas we would like to discuss, where we believe that digital identity can support the fight against money laundering:

1. identity fraud fuelled by Lost & Stolen documents;
2. digital Age Verification - reduce documents lost in night-time economy;
3. low levels of Proof of Age Cards PASS Cards;
4. age verification the opportunity;
5. knowing who you are dealing with - online dating;
6. classified sites - verified seller profiles;
7. peer to Peer identity details swap;
8. electronic Customer Due Diligence for Know Your Customer ("KYC") and Anti-money Laundering ("AML") Checks;
9. digital identity for Right to Work, Right to Rent;
10. KYC for ICOs, Cryptocurrency exchanges and Crypto ATM machines;
11. lack of access to DVLA & HMPO data;
12. money Mules.

Background to Yoti:

Yoti is a UK founded and funded identity checking system that allows organisations to verify who people are, online and in person. It has a team of 250 based in London and Chelmsford, with offices in Mumbai and due to open offices in the US and Canada later in 2018. Yoti launched in November 2017 and so far over 1.3 million people have downloaded the app. Yoti has been announced as the eID provider for the States of Jersey and recently secured India's leading dating site as a verification partner. In addition, it is due to start working with the second largest peer to peer marketplace with 30m monthly users and one of India's biggest banks with 80m account holders.

For consumers, it's an app that helps them prove who they are and confirm the identities of others. The company distinguishes itself with its approach to privacy and security - earning money from businesses when users voluntarily share verified attributes e.g. for KYC (see FAQs for technical

detail). The app is available in the iOS and Google Play app stores and is free to download. The set-up involves a four-minute process, where the user links their facial biometrics to their phone and verify their identity by scanning in a verified photo ID document. Identities are verified using NIST approved facial recognition technology, which matches individuals with their government issued identity documents and where possible, biometric passport chips. As well as using facial recognition technology a trained security team review the integrity of the documents and check the faces match. Once the individual has completed set-up, their Yoti securely holds verified attributes of your identity, such as name, date of birth, gender, nationality. They can then use the app to scan QR codes to pass specific attributes to other people or organisations or websites. This might be for age verification in the offline or online world or to populate verified data on an online form.

Yoti have been part of the UK Digital Policy Alliance steering group creating the 1296 Age Checking PAS, which was made into a British Standard, chaired by Lord Erroll at Westminster ahead of the Digital Economy Act. Yoti serves as industry chair for the DPA Age Verification & Internet Safety Steering Group; is sponsor of the APPG Digital Identity and serves on the Home Office Identity Document Working Group and is a member of the newly formed Association of Document Validation Professionals. The Yoti team serve on several TechUK boards - for Justice & Emergency Services, Data Protection and Digital Identity. Yoti are a key partner of London Digital Security Centre, set up by City of London Police, Met Police and the London Mayor's Office to help businesses innovate, grow and prosper through operating in a secure digital environment and accredited by Met Police Secure by Design. Yoti are a registered BCorps member and have set up a Guardians Council to hold them to account; as well as working with Responsible 100, Doteveryone Sustainable Tech Trust Mark Prototyping, EU Compass Responsible Innovation to assist in developing an ethics framework.

Below are the twelve areas where digital identity can support the fight against fraud and scam.

1.Identity fraud fuelled by Lost & Stolen documents

One of the contributors to identity theft is lost and stolen identity documents. Almost a million driving licences were lost by British drivers in the last year, according to latest figures released today by the DVLA. British motorists applied for 931,527 driving licence replacements in 2017. Substitute licenses cost £20, meaning drivers spent £18.6m on new ones.

- The DVLA said that 8 in 10 drivers carry their licences with them every day.
- It said this is not a legal requirement and motorists should keep it safe at home.
- According to the most recent DVLA stats, there are around 37.5 million active licence holders in the UK. That means around 3 percent of all drivers in the country either lost or snapped theirs last year. The total bill for this amounts to £18.6million.
- Younger drivers are more likely to choose to carry their licence with them (87%) compared to older motorists who tend to keep their ID somewhere safe at home.
- 16 to 24 year olds apply for the most replacements - 82% of those surveyed.

A Freedom of Information request reveals that there were 303,881 lost or stolen passports (267,247 and 36,634, respectively) in 2010. So, between passports and driving licenses over 1.3 million identity documents risk getting in the wrong hands each year.

2. Digital Age Verification - could reduce documents lost in night-time economy

The night-time economy is another area where identity documents are frequently lost. Immigration Minister Robert Goodwill was quoted as saying, “Young people face a higher risk of losing their passport as they often use it as a form of age verification. A passport is a highly valuable document. If it gets lost or stolen, not only does it cost the holder money to replace it, but it can fall into the hands of criminals unless it is handed in and cancelled. We are working with a number of stakeholders including retailers, licensed premises, police, local authorities and students, to communicate that there are better ways to prove your age, such as the PASS card.”

3. Low levels of Proof of Age Cards (PASS Cards)

Many people do not have an alternative document to a Passport or Driving License. There is also a tranche of young people who have no identity document at all. Scotland issues PASS scheme documents to young people, via the Young Scot card, free of charge. However, there is a very low penetration of PASS scheme documents in the rest of the UK. There are an estimate of 0.7 million Young Scot cards in Scotland, versus circa just 0.6 million cards from other PASS providers across the rest of the UK.

Yoti has teamed with CitizenCard to create a co-branded Yoti-CitizenCard to begin to address this issue and will be actively seeking partners to enable more young people to access free or affordable documents to prove their age in person or online. Where Yoti can make a check via API to the relevant database, that document can serve as the anchor identity document to enable a young person to set up a digital identity in tandem. This will give these young people an alternative document, so not to need to take a physical document with them on a night out; it also allows them to data minimise and share less information, for instance just an over 18 or under 18 attribute and to provide data for KYC checks digitally, rather than filling in long forms online thereby reducing the risk of phishing fraud.

4. Age verification is an opportunity

From the standpoint of the Treasury and the FCA, the introduction of mandatory age checks via the Digital Economy Act to access adult content could lead to 20-25 million of the UK population voluntarily setting up a digital identity. Initially, they may use to anonymously share an 18 plus attribute for the purpose of accessing adult content but they can then use for KYC checks, or for use to verify themself as a seller on a classified site or set up a profile on an online dating site. If the digital identity could also be used in retail settings for age checks to purchase age restricted products and services such as alcohol, tobacco or lottery products, this would greatly assist in educating the public as to the wide utility of digital age and identity verification.

5. Knowing who you are dealing with - online dating

In today’s world there are many circumstances when it is hard to know if you are dealing with the person that you think you are dealing with online. This reduces trust in the counterparty. Online

dating, classified and social networking sites are three examples where verified digital identities could help to rebuild trust.

Romance fraud scams are a growing issue for policing. In 2016 there were an estimated of 7.8 million people using online dating in the UK. As stated by the BBC, a report by the National Fraud Intelligence Bureau revealed that the losses reported due to dating fraud reached £39 million in 2014.

Creating a fake social media account and then using that to create a dating profile is very easy. It requires just an email address which can be created in seconds. MP Ann Coffey commented: *"Catfishing is a modern day menace affecting the lives of many innocent people. It can cause years of heartache. We must do something to deter this and a change in the law is the most effective deterrent."* Hence, Ann Coffey is lobbying for a new law to classify catfishing as an offence.

Conscious of how false identities can be misused on online dating platforms, Yoti is keen to support a safer dating environment by verifying the identity of the people who join these sites. Yoti has partnered with a leading online dating site in India, Truly Madly. People can use their Yoti to share a limited number of verified attributes, for example their name or gender, enabling users to increase their trust score on the site. Linking their profile to a Government issued identity document is a strong deterrent to fraud and crime and builds trust in the dating platform.

For more information see:
https://www.yoti.com/blog/trulymadly-and-yoti-build-a-safer-community-of-online-daters/

6. Classified Sites - Verified seller profiles

Criminals are also targeting classified sites, using fake identities to offer goods and services and then blackmailing their victims to send money or sexual images. One such example was the Matthew Falder case, a paedophile who blackmailed at least 47 people to send humiliating pictures of themselves.

A way to prevent this is for the classified site to verify the identity of the users. Freeads for instance is a UK based site where sellers can be verified to their Yoti to achieve 'Trusted Seller Status' and government issued identity document.

Here is a short video of this.

Verified profiles could also enable a reviewer to be a verified reviewer linked to their Government issued identity document, to increase faith in online reviews.

7. Peer to Peer identity details swap

One of the Yoti app's earliest functionalities is the peer-to-peer swap. The Yoti app is free for users to install and peer to peer swaps are also free. The simple act of swapping checked and verified identity details like name, date of birth and say a verified photo, could help to reduce crime. Fraudsters typically do not like to reveal their identity, which is linked to a Government issued identity document and leaves an audit receipt trail behind them. For instance, when buying something secondhand from someone, you may choose to swap just a photo and over 18 status to help to recognise the person when you meet up and to ensure that you are dealing with an adult. Ahead of a date, you may wish to exchange gender, photo and over 18 status.

8. Electronic Customer Due Diligence for KYC and AML Checks

Yoti is working with the FCA RegTech sandbox to enable insurers such as Marsh and Worry & Peace to fulfill KYC checks. Yoti lets people prove their identity in seconds, without showing or photocopying paper documents. They can share specific identity attributes, such as their name and date of birth, rather than disclosing their full identity; helping to protect them from the ever-growing risk of identity theft. In turn, companies can benefit from fast and accurate KYC, as well as save time and money when verifying the identities of their customers. In addition to traditional insurers Yoti is also working with a number of ICOs (Initial Coin Offerings) to provide them KYC Solutions (including Coinfinity, NCloud, Vertpig, Chainstarter, Blockchain reserve) and is keen to support regulators developing regulation in this space. Yoti is also working with leading Bitcoin ATM providers to provide KYC solutions.

9. Digital identity for Right to Work, Right to Rent

The legislation and code of conduct surrounding right to work and right to rent checks are still mandating that physical checks be made of documents and copied made and stored. These traditional methods have fuelled the proliferation of copies of sensitive documents. In the light of GDPR; it would seem more sensible to enable a recruiter or a letting agent to make a check to a digital identity and record that a check has been made, in the same way that an electoral roll check is made.

10. KYC for ICOs, Cryptocurrency exchanges and Crypto ATM machines

The lack of KYC and AML checks undertaken by cryptocurrency exchanges and ICOs have made cryptocurrencies and ICOs investments an attractive means in which to launder, semi anonymously, small or large sums of capital. As regulation has become more and more common and exchanges/ICOs and Crypto ATMs wish to become compliant, Yoti is gaining traction in the virtual currencies market with clients and active leads all over the world.

The ability for consumers or would be investors to share they verified identity attributes using via their Yoti app, securely and with ease, has led to Yoti being integrated as a KYC provider by multiple ICOs (Initial Coin Offerings) and cryptocurrency exchanges.

Yoti is currently working with a number of ICOs and ICO incubators to provide them KYC solutions (including NCloudSwiss, Globcoin, Chainstarter, Blockchain Reserve) and is keen to support regulators developing regulation in this space. Yoti is also working with leading Bitcoin ATM providers; Trilliant.io (Germany), Chain Bytes (USA) and Cryptocurrency exchanges including Vertpig (UK), Digax (UK), Coinfinity (Austria), BTCX (Sweden/India) to provide KYC solutions and is in advanced discussion with some of the largest cryptocurrency exchanges globally.

11. Lack of access to DVLA & HMPO data

Despite the high volumes of lost and stolen passports and driving licenses, an identity company such as Yoti does not have a simple route to check via API to the HMPO or DVLA database. This could quite simply enable us to block stolen or fraudulently obtained genuine passports from entering the Yoti platform and then being used for criminal activities. In the past the DVLA Data Sharing team, have responded to information requests from non travel companies with the statement, "...we do not provide data for identity purposes." However recent DVLA data sharing strategy document indicates an awareness of growing demand, however no clear route as yet for private sector companies outside of Gov.UK Verify to access it.

Other government departments want driver data either to support their own enforcement functions or as part of initiatives that are looking for the public benefits that sharing data across government can bring. Demand for driver data is often linked to its use for identification and verification. It can be a valuable tool in helping to establish identity alongside other validation. It is already being used in this way for the GOV.UK Verify service which assures the identity of digital public service users. However, the Verify service is built on the idea of government-set standards for identity assurance with users choosing between certified companies who can meet these standards. In this way, the service has created a growing market that can assure identity not only for central but for wider government and private sector services. This could lead to wider demand for DVLA data. With an increasing focus on the potential value of government data to the wider economy, DVLA could also face future demands for driver data for research other than that related to road safety.

D. Identity verification 5.14 There are risks in extending too far the concept of using DVLA data for confirming identity. Our databases were never intended to provide the basis for a national identity register. 5.15 We know that the driving licence is often used as a means to prove identity. We accept that services which allow individuals to share their own data can be used as part of this. However, the driving licence is not an identity document in itself and we will not develop services specifically to support it being used in this way. 5.16 We recognise though that where it is not used in isolation, the data we hold can be used to support identity assurance services, which can deliver public benefits.

Source:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/592987/dvla-data-sharing-strategy.pdf

https://www.gov.uk/government/publications/dvla-business-plan-2017-to-2018/business-plan-2017-to-2018

The UK DVLA approach is in direct contrast to the US market, where Yoti, a 4 year old UK private sector company, after four months of application, review, due diligence and contract signing, is able to make an API call to the AAMVA database to check US Driver Licenses across 30 states. Hopefully this is an area which the DVLA will progress over the coming months. Similarly, the HMPO is gearing up to enable private sector companies to be able to check the HMPO database; however this is not as yet available.

12. Money Mules

The 'money mule' threat is still growing. Young people, between the ages of 14 and 24, are often targeted by criminals so that their bank accounts can be used to move money proceeding from criminal activities. According to a report by CIFAS, last year 32,018 mule accounts were detected, 11% more than in 2016. People caught acting as 'money mules' will face prison and subsequently it will be harder for them to get a student loan or a mobile contract.

Having a digital identity linked to device and a need of digital identity linked to biometrics to set an account and to login will make it more difficult to mule networks to operate victims accounts.

Summary & Recommendations

In summary, it is clear that identity is at the heart of fraud. Current knowledge-based self assertion of personal details, entered into web registration forms, is a deeply flawed approach. The BBFC has shared its regulatory guidance for electronic age verification stating that entry of name, DoB and address will not alone be acceptable for proof of age when age verification is required by adult content sites later in 2018. Hence it is important to be open to and understand innovations in digital identity.

Identity fraud is partly being fuelled by the requirement for people, especially young ones, to carry around physical passport and driving license documents to prove their age in the night time economy, retail settings, for recruitment and rental checks. The updating of legislation to allow wider access to proof of age cards and digital age checks to be performed across a greater range of sectors could reduce the loss passports and driving licenses. Data sharing by UK Government departments such as HMPO and DVLA could greatly reduce the misuse of fraudulently obtained genuine documents, or lost and stolen documents and so enable private sector identity providers to assist in fighting money laundering, fraud and crime.

2018 is a landmark year due to the enactment of the Digital Economy Act. As a result of the legislation, approximately 25 million individuals are due to be required to verify their age to access adult content. There is an opportunity to broaden the appeal of digital identity to a wider sector of the population by allowing digital age checks across a range of age restricted goods and services (e.g. tobacco, alcohol, lottery, pharmacy products). We support the work of the FCA Regtech Sandbox in terms of encouraging innovation in terms of electronic customer due diligence for KYC Checks. We would encourage HMT to support similar regtech innovation in retail tech in order to encourage more people to adopt a digital identity to prove their age in retail and travel settings.

Once consumers have set up a digital identity for age checks, they can then use the same digital identity to perform KYC or AML checks for a range of financial services transactions, to check who they are interacting with at a company or via a classified site, or to reduce the romance scams.

Contact details
Julie Dawson
Director of Regulatory & Policy, Yoti
Email: julie.dawson@yoti.com

appg financial crime and scamming

www.appgfinancialcrime.org