FRAUD ADVISORY PANEL

FRAUD ADVISORY PANEL REPRESENTATION 03/18

RESPONSE TO ALL-PARTY PARLIAMENTARY 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.