VICTIM SUPPORT

POLICY STATEMENT

FRAUD

BACKGROUND

What is fraud?

Under the Fraud Act 2006[1], which came into force in 2007, a person is guilty of fraud if they:

- Falsely represent themselves in a way he/she knows to be misleading or untrue with the intention of making a gain or causing loss to another.
- Dishonestly fails to disclose information to another person which he/she is under a legal duty to disclose with the intention of making a gain or causing loss to another.
- Dishonestly abuses a position in which he/she is expected to safeguard, or not to act against, the financial interests of another person with the intention of making a gain or causing loss to another.

A person who is guilty of fraud is liable on conviction to a maximum prison sentence of 10 years and/or a fine.

There are different types of fraud including identity fraud, 'bank and credit account' fraud and dating fraud.[2]

How does it impact victims?

Victims of fraud describe experiencing a wide range of emotional and psychological responses. Button and colleagues (2014), for example, found that while the most common response to fraud victimisation was anger (68.4%) or stress (44.3%), victims also report feelings of shame, embarrassment, and upset.[3] Research conducted by Cross and colleagues (2016a) similarly found that common responses experienced by victims include shame, embarrassment, distress, sadness and anger.[4]

Research suggests that falling victim to fraud can result in people feeling suicidal (2.3%) or lead them to attempt suicide (1.7%).[5] Further, there is a small body evidence to show that victims of fraud can suffer from mental health problems, such as major depressive disorder (MDD) and generalised anxiety disorder (GAD), similar to those experienced by victims of serious violent crimes.[6,7] Ganzini and colleagues (1990), for example, found that

[1] http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf
[2] Dating fraud is when an online dating website or app is used by someone to gain your trust in order to ask for money or personal information to commit identify fraud.
[3] Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36-54.
[4] Cross, C., Richards, K., & Smith, R. G. (2016a). *The reporting experiences and support needs of victims of online fraud*. Australia: Australian Institute of Criminology.
[5] Button et al., 2014 (as n.2).
[6] Ganzini, L., McFarland, B. H., & Bloom, J. (1990). Victims of Fraud: Comparing Victims of White Collar and Violent Crime. *The Bulletin of the American Academy of Psychiatry and the Law, 18*(1), 55-63.
[7] Deem, D. L. (2000). Notes from the Field: Observations in Working with the Forgotten Victims of Personal Financial Crimes. *Journal of Elder Abuse & Neglect, 12*(2), 33-48.

25% of victims of fraud experienced a major depressive episode within 20 months of victimisation, whereas GAD was found in 45% of victims with further 5% developing suicidal ideation. Of those who suffered a major depressive episode, 48% continued to have depressive symptoms 6 months after victimisation (sample of 77 people).[8]

Studies suggest that the impact of fraud can vary depending on the type of act experienced. For example, Whitty and Buchanan (2015) found that victims of romance fraud experience feelings of embarrassment, shame, worry, stress, denial, fear, shock, anger and self-blame. While some reported a loss in confidence and sense of self-worth, others felt angry, violated, disgusted and likened their experience to sexual abuse.[9] In contrast, studies which focus on the impact of identity theft and identity fraud have shown that victims can feel betrayed, unprotected by the police, frustrated, annoyed and stressed. Cullina and colleagues (2014) found the most common emotional responses to this particular crime include frustration or annoyance (79%), rage or anger (62%), fear regarding personal financial security (66%), and sense of powerlessness or helplessness (54%).[10]

Research shows that fraud can have harmful physical consequences. Attempts to confront offenders and recover lost funds, for instance, can pose a significant threat to the victims' safety. Some report being kidnapped,[11] raped or sexually assaulted.[12] The emotional impact that this can have leads often to a decline in victims' physical health and the development of new health conditions, such as sleeplessness, nausea, weight loss,[13] skin conditions,[14] or even premature death.[15]

The financial loss resulting from fraud can vary considerably depending on a range of factors, such as the amount of money lost, the financial circumstances of the victim and the resources they can access to recoup losses. Often the impact of the loss is felt by the victim and their family and for some it is so severe that it leads to bankruptcy, homelessness, selling their home/businesses, postponing or giving up retirement or moving in with family members.[16]

What support does Victim Support provide to victims?

In 2016/17, VS offered support to 10,300 victims of fraud.[17] In the same period, VS provided at least one service to 3,900 fraud victims.

---

[8] Ganzini at el., 1990 (as n.5)
[9] Whitty, M. T., & Buchanan, T. (2015). The online dating romance scam: The psychological impact on victims-both financial and non-financial. *Criminology & Criminal Justice, 16*(2), 176-194
[10] Cullina, M., Velasquez, E., Bond, P., Grant, S., Cook, M., Fergerson, J., & Lee, J. (2014). *Identity Theft: The Aftermath 2014.* Identity Theft Resource Centre. Retrieved from http://www.idtheftcenter.org/images/surveys_studies/Aftermath2014FINAL.pdf
[11] Whitty, M. T., & Buchanan, T., 2015 (as n.8)
[12] National Crime Agency. (2016). *Emerging new threat in online dating: Initial trends in internet dating-initiated serious sexual assaults*. UK: National Crime Agency. Retrieved from http://www.nationalcrimeagency.gov.uk/publications/670-emerging-new-threat-in-online-dating-initial-trends-in-internet-dating-initiated-serious-sexual-assaults/file
[13] Cross, C., Richards, K., & Smith, R. (2016b). *Improving Responses to Online Fraud Victims: An Examination of Reporting and Support*. Final Report, Australian Institute of Criminology.
[14] Button, M., Lewis, C., Tapley, J. (2009). *A better deal for fraud victims.* London: Centre for Counter Fraud Studies.
[15] Spalek, B. (1999). Exploring the impact of financial crime: A study looking into the effect of the Maxwell scandal upon the Maxwell pensioners. *International Review of Victimology, 6*, 213-230.
[16] Deem, D. L. 2000 (as n. 6)
[17] VS data April 2016-March 2017. Data may be subject to human error.

Key statistics

Total number of fraud incidents and recorded fraud offences

- In 2016, there were 5.4 million fraud and computer misuse incidents[18]
- 3.5 million of these were fraud and 1.9 million computer misuse
- The number of fraud offences recorded by the police increased by 4% when compared with the previous year to 641,000

Types of fraud

- In 2016, there were 4.1 million victims of fraud and cyber misuse including: 2.8 million victims of fraud; 2 million bank and credit card account fraud victims; 1.5 million computer misuse victims; 1 million computer virus victims and 500,000 victims of unauthorised access to personal information (including hacking)[19]
- Figures from City of London Police show that between 2015 and 2016, victims of dating fraud lost a total of £40 million. Between January 2013 and December 2015, the number of reports of dating fraud to Action Fraud increased by 32%. On average, victims lost £10,000 each and almost half (45%) report that falling victim to dating fraud had a "significant impact on their health or financial wellbeing"[20]

Financial loss and reimbursement

- In 2015/16, £10.9 billion was lost to fraud and cybercrime in the UK. This amounts to around £210 per person[21]
- In the year ending September 2016, two-thirds of fraud incidents (66%) involved a loss of money or goods to the victim[22]
- In the year ending June 2016, victims receive full reimbursement in only 43% of fraud incidents. In 690,000 cases the victim received no or only partial reimbursement[23]

Demographics

- In the year ending September 2016, adults aged 25-34 were the most likely to be a victim of fraud (7.9%), followed by people aged 45-54 (7.5%)[24]
- 4.9% of people aged 65-74 and 3.3% of adults aged 75+ were victims of fraud[25]

---

[18] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdec2016

[19] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdec2016

[20] https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/nfib/nfib-news/Pages/One-victim-reports-dating-fraud-every-three-hours-according-to-the-latest-national-figures-from-City-of-London-Police.aspx

[21] http://www.actionfraud.police.uk/news/fraud-and-cybercrime-cost-UK-nearly-11bn-in-past-year-oct16

[22] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016#whats-happening-to-trends-in-fraud

[23] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016

[24] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016#whats-happening-to-trends-in-fraud

[25] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016#whats-happening-to-trends-in-fraud

- Individuals living in rural areas were more likely to be a victim of fraud (6.8%) than those living in urban areas (6.2%)[26]

Public awareness of fraud protection measures

- People are more likely to take steps to improve their home security than reduce their risk of falling victim to cyber-crime. While 82% of households have double locks or deadlocks, only 32% follow Government advice to use three random words to create a strong password[27]

Use of social media

- Social media is increasingly being used as a way to defraud young people. In 2015, there was a 64% increase on the previous year in the number of people approached on Instagram[28]

POLICY TOPICS IN FRAUD

- Reducing susceptibility to fraud amongst vulnerable people
- Increasing public awareness and understanding of fraud protection measures
- Enhancing the police response to victims of fraud
- Improving the service provided by banks to customers in cases of APP scams and relaxing SAR (serious activity report) rules on disclosure
- Improving the reporting rate of fraud offences

REDUCING SUSCEPTIBILITY TO FRAUD AMONGST VULNERABLE PEOPLE

Overview of the issue and how it affects victims

According to the National Trading Standards (2015) the average age of a person on a victim or 'sucker' list is 75. Sucker lists consist of personal details of individuals who have fallen victim to scams. They are sold between fraudsters and aim to target the most vulnerable and susceptible people to fraud. In 2015, Trading Standards identified more than 220,000 names of victims that had appeared on and been shared through one of these lists.[29] It is also estimated that around 85% of successful doorstep scams are committed against people aged 65 and over.[30]

Research carried out by the Financial Conduct Authority (FCA) suggests that of people over the age of 55, less than half (42%) know how to identify a fraudulent investment opportunity, yet they are an increasingly targeted demographic. Only 48% said it is likely that before making an investment they would seek independent advice.[31]

---

[26] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016#whats-happening-to-trends-in-fraud

[27] https://www.cyberaware.gov.uk/blog/britons-urged-take-cyber-security-seriously-home-security

[28] http://www.actionfraud.police.uk/news-sharp-rise-in-people-being-defrauded-via-adverts-on-social-media-nov16

[29] http://www.nationaltradingstandards.uk/site_assets/files/NTS%20Consumer%20Harm%20Report%202016.pdf

[30] http://www.ageuk.org.uk/home-and-care/home-safety-and-security/doorstep-scams/doorstep-scams/

[31] https://www.fca.org.uk/news/press-releases/inside-mind-scammer-tactics-investment-fraudsters

Victim Support's own data reflects these findings. Of the 27,900 fraud victims VS contacted in 2016/17 24.9% were 65 years and over, despite only making up 18% of the whole population. 14.4% of victims were aged 75 and over despite making up 8% of the population.[32]

Bournemouth University and the Chartered Trading Standards Institute expect that over the next 15 years, the percentage of people at risk of falling victim to financial scams will significantly increase as more people live to be over the aged of 65.[33] According to the Office of National Statistics (ONS), there were 11.6 million people aged 65 and over in 2015. By 2030, the department estimates that this figure will rise to 15.7 million.[34] Older people living alone and those with dementia are two demographics most at risk. Alzheimer's Society predicts that the number of people in the UK with dementia could reach 1,142,677 by 2025, with 40% of this growth occurring over the next 12 years,[35] and according to the ONS around a third of people over 80 report being lonely.[36]

As evidence suggests that vulnerable people are often deliberately targeted by fraudsters, the state has a responsibility to ensure efforts are made to protect them.

Overview of Government, government agency, parliamentary and other activity

In the Queens Speech on 18 May 2016 it was announced that measures would be brought forward to "strengthen protections for citizens in the digital world". Through introduction of the Digital Economy Bill 2016-17, customers will be required to give their consent for direct marketing to provide them with better protection from spam emails and nuisance calls. The Bill would also see the imposition of fines by the Information Commissioner on those who break the rules.[37]

In order to offer greater protection specifically to vulnerable people, the Chartered Trading Standards Institute and Bournemouth University launched a campaign in June 2016 calling on a 'duty of care' to be imposed upon banks and financial institutions for those with cognitive impairments. The campaign also makes the following asks of relevant organisations:

- Allow vulnerable people to put a 24hour delay on new or large transactions from leaving their bank accounts and send an email or text alerting a carer or loved one at the start of that period.
- Adopt a default that personal data is not shared without a clear opt in and that it is not held for longer than 12 months before permission is sought again, in order to prevent 'suckers' lists".[38]

The susceptibility of vulnerable people to fraud has been recognised by the Government. During a debate on financial scamming in the House of Commons on 8 September 2016, Parliamentary Under Secretary of State at the Home Office, Sarah Newton, confirmed that

[32] VS data April 2016-March 2017. Data may be subject to human error.
[33] https://www.tradingstandards.uk/media/documents/policy/research/scam-booklet-final-draft.pdf
[34] https://www.tradingstandards.uk/media/documents/policy/research/scam-booklet-final-draft.pdf
[35] https://www.alzheimers.org.uk/site/scripts/documents_info.php?documentID=412
[36] http://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/articles/measuringnationalwellbeing/2015-10-01
[37] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/524040/Queen_s_Speech_2016_background_notes_.pdf
[38] https://www.tradingstandards.uk/news-policy/financial-scamming-1

"tackling scams is a priority". She added: "scams have a devastating impact, particularly on the most vulnerable people in society". Ms Newton announced that National Trading Standards Scams Team is currently working on producing a new banking protocol for doorstep crime in partnership with the British Banking Association and the Building Society Association. In addition, in 2017 the FCA will launch a strategy on the ageing population. This will draw on the findings of an FCA programme of work into the use of financial services by older consumers, launched by the regulator in February 2016.[39]

Through the victims and susceptibility work stream, the Joint Fraud Taskforce is also undertaking work to improve the service that victims of fraud receive and the protections offered to those who may be more susceptible.

Victim Support's position

VS support's the Chartered Trading Standards Institute's proposal to introduce a mechanism for vulnerable banking customers that would enable a 24 hour delay on new or large transactions going out of their account to be set

In order to provide vulnerable banking customers with greater protection from fraud, we believe that an optional mechanism should be introduced, whereby large transactions from their accounts are delayed and a nominated person is notified. This would offer them time to review and cancel suspected fraud payments. In addition, to determine whether additional measures, such as tailored warning messages and caps on the amount payable to new payees, should be offered by financial institutions nationally to customers, VS would welcome further research into, and evaluation of, their effectiveness.

VS would support the introduction of new standards for financial institutions that aim to improve how cases of fraud, including those which involve vulnerable customers, are handled and how customers at risk are supported

VS supports the development and introduction of a Public Available Specification that sets out best practice in the provision of financial services, including to vulnerable customers, which institutions are encouraged to adopt. We believe this will help to ensure that those who are at risk of fraud are routinely provided with the necessary protection measures from their bank and those who fall victim are consistently treated with respect and made aware of victim support services. To take this forward, VS is working alongside the British Standards Institute to develop a new standard that aims to improve the customers' experience with financial institutions.

VS welcomes the national rollout of the Banking Protocol programme

Banking Protocol programme staff in local banks and other services, such as post offices, are trained by Trading Standards to help them identify and question large customer withdrawals where they suspect the individual is being defrauded. Early results of the programme have indicated that it is effective in helping to prevent people, including those who are vulnerable, from falling victim to certain types of fraud, such as rogue trader fraud.[40,41] We therefore welcome the roll out of the programme nationally.

[39] https://www.fca.org.uk/publications/discussion-papers/ageing-population-financial-services
[40] https://www3.havering.gov.uk/Pages/News/Haverings-banking-protocol-delivered-to-post-offices-across-the-borough.aspx

INCREASING PUBLIC AWARENESS AND UNDERSTANDING OF FRAUD PROTECTION MEASURES

Overview of the issue and how it affects victims

Research published by Financial Fraud Action UK (FFA UK) on 19 September 2016, revealed that 73% of people say they are aware of the methods fraudsters use yet 26% admit to still providing their details to people claiming to be from their bank even if they do not think they should. Get Safe Online report that 25% of the public say that have a limited understanding of the risks they face when going online. The organisation further found that 43% of adults use the same password across their personal accounts online and 12% fail to take action despite being advised to change them after a breach.[42] Similarly, VS caseworkers report that it is common for victims of fraud to have a low understanding of the practical steps that can be taken to prevent victimisation.

The lack of widespread public awareness and understanding of the importance of measures that can be taken to protect against fraud means that many people are at risk of falling victim to a crime which has been shown to cause significant financial[43], emotional[44] and physical harm[45,46,47].

Due to the increasing prevalence and sophistication of fraud, raising awareness of steps that can be taken to reduce risk is unlikely to be enough to prevent victimisation. As perpetrators find new ways to target people, the sector needs to increase its understanding of how to change people's behaviour to reduce risk and better target those who are most vulnerable. Research suggests that people are more likely to take steps to improve their home security than reduce their risk of falling victim to cyber-crime. While 82% of households have double locks or deadlocks, only 32% follow Government advice to use three random words to create a strong password[48].

Overview of Government plans or activity

The Government's approach has been to provide the public with the skills and knowledge needed to protect themselves. In January 2014, the Home Office launched the Cyber Streetwise campaign (now Cyber Aware) to encourage people to alter their behaviour and improve their cyber security, for example by using strong passwords and ensuring software is up to date.[49]

In February 2016, the Government launched the Joint Fraud Taskforce which includes representatives from VS, the City of London Police, FFA UK, the Bank of England and Cifas. Part of the remit of the taskforce is to examine why people fall victim to fraud and help

---

[41] http://content.met.police.uk/News/Currency-exchanges-help-combat-cash-cons/1400034674241/1257246745756
[42] https://www.getsafeonline.org/news/fraud-cybercrime-cost-uk-nearly-11bn-in-past-year/
[43] Deem, D. L. 2000 (as n. 6)
[44] Button, M., Lewis, C., & Tapley, J., 2014 (as n.2)
[45] Cross, C., Richards, K., & Smith, R. 2016b (as n.12)
[46] Button, M., Lewis, C., Tapley, J., 2009 (as n.13)
[47] Spalek, B., 1999 (as n.14)
[48] https://www.cyberaware.gov.uk/blog/britons-urged-take-cyber-security-seriously-home-security
[49] https://www.gov.uk/government/news/new-campaign-urges-people-to-be-cyber-streetwise

raise awareness of the steps that can help people protect themselves.[50] VS co-leads the susceptibility work stream with Trading Standards.

On 1 November 2016, the Government published the National Cyber-Security Strategy for 2016-21, setting out its policies across three areas: defence, deterrence and development. The strategy highlights the importance of the public having the ability to protect themselves against fraud. It commits to providing individuals and organisations in the UK with "access to the information, education, and tools they need". Success will be measured by whether "there is an improving cyber security culture across the UK because organisations and the public understand their cyber risk levels and understand the cyber hygiene steps they need to take to manage those risks". "Trusted voices" will be used to maximise the reach and effect of the messaging.[51]

Victim Support's position

Further research is needed to determine the most effective approaches to reducing the likelihood of falling victim to fraud to inform preventative strategies for the whole sector to adopt and target messages more effectively

While VS supports national and regional campaigns aimed at reducing the risk of fraud victimisation, the experience of our caseworkers suggests that they may not reach, or where they do, have an impact on, some members of the public. A number of VS caseworkers report that it is common for victims of fraud to have a low understanding of the practical steps that can be taken to prevent victimisation. In order to determine the most effective approach to reducing the likelihood of falling victim to this crime, we believe that further research is needed.

ENHANCING THE POLICE RESPONSE TO VICTIMS OF FRAUD

Overview of the issue and how it affects victims

VS has concerns that the police are not consistently providing victims of fraud with an appropriate response. Under the Victims' Code of Practice, all victims crime are entitled to a minimum level of support and information from organisations including all police forces in England and Wales. Despite this, our caseworkers who directly support victims of fraud report that the police often do not refer victims to victim support services, fail to offer the victim an opportunity to make Victim Personal Statement (VPS) and in some cases do not provide any entitlements under the Code. They also report that they often lack the knowledge and skills to investigate cyber-enabled fraud, provide an unsympathetic initial response to fraud victims, have a poor understanding of the impact of the crime and fail to conduct an adequate needs assessment.

Similar shortcomings were highlighted by HMIC's 2015 study of digital crime which found a "mixed picture about the extent to which the police provided good quality advice to victims". While examples were found to show that some victims of fraud are provided with adequate support and care, HMIC concluded that generally police officers struggle to empathise with them. It is suggested that this may be due to a lack of understanding and awareness of the context in which digital crime takes place. The study also identified a number of additional short-fallings in the police response to digital crime:

[50] https://www.gov.uk/government/news/home-secretary-launches-new-joint-fraud-taskforce
[51] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

- In some instances, police officers do not thoroughly collect evidence of digital crime, despite victims offering it having gathered it themselves.
- Where a report of fraud is made directly to a local police force, the call handler often directs the victim to Action Fraud without conducting a full assessment of their vulnerability which would determine whether an immediate police response was necessary.
- Some police forces set an arbitrary limit on the number of cases referred from the National Fraud Intelligence Bureau that they are willing to investigate (one force has set this at 20%). Others have a threshold of financial loss incurred by the victim which must be met for the NFIB to refer on.
- Recognition of the victims' vulnerability and the support that he or she needed tended to be based on the individual officers' personal judgement.
- Some police officers and staff are dismissive of complaints about the use of social media sites. For example, one individual who participated in the study said: "I do not use social media; how am I supposed to investigate it?".
- Victims are not always kept up to date by the police about the progress of the investigation and, where they are, the communication can be inappropriate and insensitive. The report recognises the harmful effect that this can have on victims. For example, it may result in a loss of confidence and trust in the police.

HMIC conclude that "there is some way to go before the victims of digital crime can be assured that they will receive the same response from the police as victims of more familiar crimes". As such, the following issues are identified in the report as requiring further work:

- The police service must show that it takes digital crime seriously.
- Better tailored support and advice to victims of digital crime is needed.
- Officers and staff should be more aware of the investigation process for digital crime.
- A more coordinated and consistent approach between and within police forces is required.
- Victims should be kept better informed of the progress of their case.[52]

Research suggests that in instances where a victim does report the incident to the police, it is highly important to them that their case is taken seriously and investigated. A study by Button and colleagues (2009) found that 94% of fraud victims see this as important.[53] Victims also report that a sympathetic response from the police, regular updates about their case[54] and to be treated with respect,[55] which HMICs study suggests is not guaranteed, are also valued by victims. Further, research by Cross and colleagues (2016) highlights the importance of victims receiving support from trained professionals who understand the complexities of fraud and the consequences of falling victim to this crime type.[56]

Overview of Government and agencies' activity to address this issue

[52] https://www.justiceinspectorates.gov.uk/hmic/news/news-feed/a-study-of-digital-crime-and-policing/
[53] Button, M., Lewis, C., & Tapley, J., 2009 (as n.13)
[54] Button, M., Lewis, C., & Tapley, J., 2009 (as n.13)
[55] Cross, C., Richards, K., & Smith, R. G., 2016 (as n.12)
[56] Cross, C., Richards, K., & Smith, R. G., 2016 (as n.3)

In September 2015, the College of Policing launched two new voluntary training courses, one for all police staff (Cyber-Awareness) and another for investigators (Cyber for Investigators). These are designed to improve the police response to cyber-enabled fraud and online crime by providing guidance on conducting an investigation and raising awareness of the available sources of support for victims, among other things.[57]

Through the Police Innovation Fund, the Government is seeking to "incentivise collaboration, support improved police ICT and digital working and enable PCCs to invest in innovative approaches to improve policing and deliver further efficiency in the future" with the aim of protecting vulnerable, among other things.[58] In addition, on 1 November 2016, the Chancellor, Philip Hammond announced that over the next year 50 new cyber-crime investigators and technical specialists will be recruited to work within the National Cyber Crime unit to enhance its capacity to respond to serious incidents of cyber-crime.

Victim Support's position

All police staff across England and Wales should undertake training on fraud, including cyber-enabled fraud, delivered by specialists to ensure it is of a high standard and victims get the respect and response they deserve

In order to improve the police response and ensure that victims of fraud are provided with their entitlements under the Code, VS believes it is vital that all police staff across England and Wales undertake training on fraud that is delivered by specialists.

Regional units staffed by fraud specialist should be set up to support police staff to ensure that victims get the respect and response they deserve

Regional units staffed by specialists should be set up to assist police staff in their investigation of fraud-related offences, particularly those that are cyber-enabled. This would help to ensure that all investigations of fraud are robustly pursued and adequately resourced.

IMPROVING THE SERVICE PROVIDED BY BANKS TO CUSTOMERS IN CASES OF APP SCAMS AND RELAXING SAR RULES ON DISCLOSURE

Overview of the issue and how it affects victims

There are two main issues regarding current responsibilities of banks about which VS has concerns with. First, according to the Consumer Association Which?, victims who are tricked into making bank transfers have no legal right to get their money back from their bank. However, if the payment is made via direct debit, credit card or debit card it is responsible for reimbursing customers (providing they did not act with gross negligence or fraudulently[59]). Research conducted by Which? showed that the majority of people (60%) are not aware that if they fall victim to this type of fraud, banks are not liable to reimburse them and that many people have either made a payment via bank transfer to a fraudulent account or know someone who has (9%).[60] Through a 'super-complaint'

[57] http://www.college.police.uk/News/archive/September_2015/Pages/Revised_cybercrime_training_for_police.aspx

[58] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/470122/HARD_LAUNCH_20151020_-_PIF_2016-17_on_a_Page.pdf

[59] http://www.which.co.uk/consumer-rights/advice/theres-a-transaction-on-my-credit-card-i-know-nothing-about

[60] https://press.which.co.uk/whichpressreleases/which-makes-super-complaint-on-scams/

submitted to the Payment System Regulator (PSR), Which? is calling for banks to offer better protection to customers who are tricked into transferring money to fraudsters.

Second, under current legislation, banks have a responsibility to inform the National Crime Agency (NCA) of suspicious activity taking place on customer accounts which might indicate money laundering or involvement in dealing with criminal property. However, they are not allowed to inform the client or their financial institution that a Suspicious Activity Report (SAR) has been made.[61] Consequently, information that could prevent a person falling victim to fraud is not shared with them or their bank.

Overview of government agency and other activity

In response to Which?, the PSR (which was required to respond within 90 days) agreed that "the ways in which payment service providers (PSPs), which includes banks, currently work together in responding to reports of APP [Authorised Push Payment] scams needs to improve". While the PSR did not find enough evidence to make banks liable in these cases or introduce risk management standards, it agreed a plan of action with the FFA UK that requires the "industry to develop a common approach or best practice standards that sending and receiving PSPs (payment service providers) should follow when responding to instances of reported APP scams".[62] The PSR is also working with the Joint Fraud Taskforce in response to the Super-complainant made by Which?[63]

Victim Support's position

VS would support the introduction of new standards for financial institutions that aim to improve how cases of fraud, including those which involve vulnerable customers, are handled and how customers at risk are supported

VS supports the development and introduction of a Public Available Specification that sets out best practice in the provision of financial services, including to vulnerable customers, which institutions are encouraged to adopt. We believe this will help to ensure that those who are at risk of fraud are routinely provided with the necessary protection measures from their bank and those who fall victim are consistently treated with respect and made aware of victim support services. To take this forward, VS is working alongside the British Standards Institute to develop a new standard that aims to improve the customers' experience with financial institutions.

VS would welcome a review into whether customers would benefit from the Suspicious Activity Reports (SAR) rules on disclosure being relaxed

By relaxing money laundering legislation to allow SARs to be shared outside of the reporting financial institution the National Crime Agency, VS believes that customers and their banks could be warned of suspicious activity on their accounts and the necessary protection measures put in place. However, we recognise that the information contained in such reports is sensitive and would therefore welcome a review into whether customers would benefit from the rules around disclosure being relaxed and the risks this change

[61] http://www.nationalcrimeagency.gov.uk/publications/suspicious-activity-reports-sars/550-introduction-to-suspicious-activity-reports-sars-1/file
[62] https://www.psr.org.uk/psr-focus/which-super-complaint-payment-scams
[63] http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-02-23/65350/

would pose to investigation. This might enable, for example, banks to delay transactions they suspect are destined for questionable accounts.

IMPROVING THE REPORTING RATE OF FRAUD OFFENCES

Overview of the issue and how it affects victims

Action Fraud is UK's national reporting centre for fraud and cyber-crime. People can report directly by using the online reporting tool or calling Action Fraud's specialist fraud advisers. In the year ending September 2016, Action Fraud recorded 232,832 fraud offences.[64] When a report is made directly to the local police it is the responsibility of the local call handler to determine whether an immediate police response or referral to Action Fraud is required. Action Fraud does not carry out investigations; reports are sent to the National Fraud Intelligence Bureau (NFIB) which uses the data to identify serial offenders and organised crime gangs. The NFIB then refers cases which have a chance of criminal investigation to police forces and other law enforcement agencies with information including on the victims' profile.[65]

According to experimental data from the Crime Survey for England and Wales, only one-fifth of victims of fraud report the incident to the police or Action Fraud. The ONS suggests that these victims are likely to have suffered greater financial and emotional harm which made them more inclined to report.[66] This means that some people affected by fraud may be choosing not to report the incident because they believe it to be too insignificant.

Other reasons that victims do not report fraud are included in the findings of HMICs 2015 study on the police response to digital crime. "Digital crime" encompasses cyber-enabled crimes such as fraud and child sexual exploitation, as well as cyber-dependent crimes[67] and internet-facilitated crimes.[68] As part of the study, HMIC spoke to eight victims, all of which reported that they did not contact the police immediately after the crime. The main reasons were embarrassment that they were somehow responsible, a belief that they could deal with the issue themselves and a lack of confidence in the skills and ability of the police to respond effectively. Consequently, the police were only contacted by some victims as a last resort for protection and reassurance.[69]

These findings are backed up by figures from Get Safe Online.[70] According to the results of their survey with 2,000 adults in the UK, published in October 2016, 38% felt the crime was too trivial to report and 37% believed that nothing could be done.[71]

---

[64] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016#whats-happening-to-trends-in-fraud

[65] http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

[66] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016

[67] "Cyber-dependent" crimes are acts that can only be committed using a computer or other form of IT.

[68] "Internet-facilitated" crimes are acts whereby the internet or smartphones have been used to commit an offence.

[69] http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

[70] Get Safe Online provides unbiased and practical advice on online safety.

[71] https://www.getsafeonline.org/news/fraud-cybercrime-cost-uk-nearly-11bn-in-past-year/

Similar to the findings of HMIC and Get Safe Online, VS caseworkers report that embarrassment is one of the main reasons that fraud victims do not come forward to the police. Other common reasons include that they feel somehow to blame, do not know how to report the crime, do not believe they will get their money back, do not think the police have the knowledge and skills to respond effectively, do not think the police will take the crime seriously or believe the money lost was not significant enough. Our experience has shown that fraud and cyber-crime can have a devastating impact on people's lives. VS is concerned that as a result of the many reasons that people choose not to report, victims of fraud are not seeking justice or support for the harm they have suffered. Not reporting the crime can also reduce the likelihood that they will have access to victim services.[72]

Steps therefore need to be taken to address victims' concerns around the crime being considered too insignificant or trivial, and feelings of self-blame and embarrassment to help encourage more people to report the crime. People also should be made aware of the role Action Fraud plays.

Overview of Government plans or activity

Included in the Government's National Cyber-Security Strategy for 2016-21 is a plan for a 24/7 reporting tool in Action Fraud "to improve support to victims of cybercrime" and "provide a faster response to reported crimes".

Victim Support's lines to take

The Government, criminal justice agencies, charities and the financial sector should promote clear messages for the public that fraud is a crime, how to report it and the available support

VS believes that people should not feel embarrassed or to blame if they fall victim to fraud. To help improve the rate of reporting and ensure that people do not feel alone in dealing with the crime, the Government, criminal justice agencies, charities and the financial sector should promote consistent and clear messages for the public that fraud is a crime, how to report it and the available support. Messages should be targeted at groups that are less likely to report the crime. We believe it would be beneficial for this to be accompanied by victim experiences which make clear that it is not unusual to feel embarrassed or to blame. It should also instil confidence that reporting all cases of fraud to the police is worthwhile.

For more information please contact policy.team2@victimsupport.org.uk

Date: 12 April 2017

[72] Bricknell, S., Boxall, H., & Andrevski, H. (2014). Male victims of non-sexual and non-domestic violence: Service needs and experiences in court. Research and Public Policy Series, 126, 1–50