Written evidence submitted by Dr Emily Cooper, Dr Nicola Harding, Prof Sarah Kingston, Dr Nathan Birdsall, Dr Rebecca Fish, Alice Mills, Georgina Bahri, Deborah Powney, Dr Clare Scollay and Tony Sales

1. Introduction

Our research with UK and international police forces and those with lived experience of fraud perpetration has demonstrated the prevalence and complexity of fraud and the need for more evidence-based policing responses on a local, national and international level. Collaborations between police, corporations and those with lived experience of fraud perpetration are invaluable for understanding and responding to contemporary societal challenges (such as the recent COVID19 pandemic) and the dynamism of fraud perpetration. We offer this evidence as a collection of academics and those with lived experience of fraud perpetration and of fraud investigation.

2. The value of innovation and co-production in prevention strategies

In 2021, a Rapid Response Taskforce, comprised of academics (Harding and Cooper), lived experience colleagues from We Fight Fraud, and those with investigative expertise (McDonald), was directed by network members in the Fraud and Financial Crime Clinic (UK) to assess the vulnerabilities potentially posed by 'returning to the workplace' after the COVID-19 pandemic (Harding et al., 2021). The taskforce identified five distinct attack vectors within the threat landscape, including building entrances (front and rear), obtaining staff data, gaining network access (at home and in-office), and residual/opportunistic threats. The taskforce identified that there had been more focus placed on COVID-19 compliance within organisations than on security breaches. The now more prominent hybrid model of working needs to account for vulnerabilities that are evident in *both* face-to-face and online working environments and the transitions between these (for example, ensuring that team members all know what staff changes have occurred before allowing entrance to buildings).

The results of this, and other similar studies conducted by Harding et al. found the need for greater and more meaningful levels of awareness within employees and the general population, but that offering information is not enough. The team devised the fraud and money mule prevention film Crooks on Campus (www.crooksoncampus.co.uk) that is being rolled out in universities nationwide. The purpose was to make students more aware of money mule recruitment, money laundering and fraud to reduce criminals' ability to 'clean' criminal funds through the UK student population. Working with the National Crime Agency, the City of London Police, WPM Education, and Lloyds Bank, We Fight Fraud produced this 45-minute film and rolled it out in two pilot studies in the Northwest of England and London. Under evaluation, we found that students *perceived* themselves to be more fraud aware than they are, with 66% of students sharing their private details and showing interest in money mule recruitment within a mock recruitment exercise. After watching the film, just 6% of students submitted their data. This shows the power of creative forms of prevention that utilise lived experience to really help people understand the tactics used by fraudsters and the impact that becoming engaged in fraud as a money mule can have on them and others.

3. The cross-cutting nature of fraud

Preliminary findings from studies conducted by both Cooper et al. (2020) and Harding et al. (forthcoming) suggest that policy-makers and police must develop their understanding of the cross-cutting nature of fraud, both between different types of fraud and between fraud and other crimes. For example, methods of digital-sexual exploitation such as sextortion occur during romance fraud

interactions to target individuals, but businesses may also be targeted in this regard whereby perpetrators conduct romance fraud interactions to blackmail individual staff into providing access to sensitive data. There needs to be greater connection between fraud awareness, both at work and in wider society, and fraud reporting. Currently, it is difficult for police forces to capture both repeat victimisation and offences or offenders who cross over different fraud or crime types, or where fraudsters utilise others within organisations to commit fraud. This means the connection between fraud and serious organised crime is not as well understood as it should be. Factors such as the underreporting of incidents by victims (either from embarrassment or unawareness), the vast and dynamic methods employed by fraudsters making detection complex, and the sheer volume of digital data (which can overwhelm traditional investigative process) exacerbate the difficulties in adequate data capture.

4. How offenders are committing fraud:

The following information in this section is drawn from the findings of a systematic literature review conducted for the Scottish Sentencing Council by Fish et al. (2022):

A systematic literature review on fraud sentencing, conducted for the Scottish Sentencing Council (Fish et al., 2022) identified that there has been a rapid transition from offline to online methods according to police recorded crime in Scotland. Reports of cybercrime increased by 40% during the COVID-19 outbreak in 2020 (Buil-Gil et al., 2021; Kemp et al., 2021b). Figures of police recorded cyber-crime in Scotland (2020-2021) show that 57% of all recorded fraud in 2020-21 was cyber-crime. An estimated 8,580 frauds recorded by the police were cybercrimes, increasing by 149% from the estimated 3,450 recorded in 2019-20 (Scottish Government, 2021a). Reports were amplified during April and May of 2020, the months with the strictest lockdown policies and measures (Buil-Gil et al., 2021). The increase was most evident in the number of frauds associated with online shopping and auctions, as well as the hacking of social media and email, the two most common cybercrime categories in the UK (Buil-Gil et al., 2021). This increase in cyber-dependent fraud has mainly been experienced by individuals rather than organisations; these organisations include private companies, public limited companies, and charities (Buil-Gil et al., 2021).

For the recorded figures in the financial year 2018-19, a study was conducted by the Scottish government into the specific characteristics of fraud cases (Scottish Government, 2019). This study, led by Scottish Government statisticians, reviewed a random sample of 500 fraud cases, therefore the percentages given below are a proportional of *all* fraud offences in 2018-19 (ibid). The research examined the methods used to commit fraud offences and found the following:

- **Bank card fraud** (estimated 30%) was the most frequently recorded type of Scottish fraud in 2018-19. This offence relates to a victim's bank card being used to make a purchase without their knowledge or consent.
- **Failure to pay fraud** (estimated 20%) was the second most frequently recorded type of fraud in Scotland. This offence relates to the refusal to pay for a product or service by the perpetrator; most of these cases relate to the evasion of taxi fares.
- **Fraudulent selling** accounted for approximately 12% of fraud cases in Scotland in 2018-19. This generally relates to a purchase being made by the victim, where the perpetrator has no intention of providing the product or service. 55% of these offences were cyber-enabled, that is traditional crimes which can be increased in scale or reach through the use of Information and Communication Technology (ICT) (CPS, 2019).
- **Phishing** frauds accounted for approximately 10% of fraud cases in Scotland in 2018-19. In this type of fraud, the perpetrator has obtained sensitive information from the victim, through claiming to be a reputable organisation, such as a bank. 90% of these cases were cyber-enabled, with the median loss to the victim of £900. This is the highest recorded media of the four types of fraud discussed here.

5. **Impact on victims:**

The following information in this section is drawn from the findings of a systematic literature review conducted for the Scottish Sentencing Council by Fish et al. (2022):

- Fraud can lead to devastating consequences not limited to only financial losses. Victims often feel a sense of shame and blame, as well as financial loss (Cross, 2015). Additional impact can include mental and physical health implications: anger, stress, reduced self-esteem, relationship breakdown and in extreme cases, suicide (Button et al, 2014; Cross, 2013). The 'fear of crime' can also be a limitation, for example some internet users who are knowledgeable about the presence of online fraud adopt an avoidance technique, thus limiting their potential opportunities of positive online use (Brands and Van Wilsem, 2021).
- Despite greater awareness of fraud, particularly where online fraud is common, past research has shown that victims are only likely to report their crimes if they have suffered a significant financial loss, resulting in a self-blaming culture. Within the realms of romance fraud, scammers use techniques such as isolation, monopolisation, degradation, and psychological destabilisation to wear their victim down. Emotional or interpersonal withdrawal interaction pattern is a known destructive behaviour tactic used by fraudsters seeking access to vulnerable individuals online, under the guise of a romantic relationship with their victim by using 'contingent expressions of love' (Whittle et al, 2013; Carter, 2021). Victims who have the perception of a developing relationship, often refrain from reporting. Officers have been known to describe such victims as unwilling to help themselves (Millman et al, 2017). Shame and embarrassment from negative perceptions of cyberstalking may therefore act as a barrier to reporting these crimes (Woodlock, 2013; Carter, 2021). Notably, these types of crimes usually have a time span of at least six months as part of the grooming process, whereby the perpetrator gains the trust of the victim over that period, so there is sense of victim compliance and distortion that has been cultivated by the fraudster. Carter's study reports victim responses of romance fraud to be psychological, a key component of techniques used in domestic abuse of coercion and control (Stark, 2013; Cross et al, 2018). Viewing fraud from a domestic abuse lens may be beneficial in terms of raising awareness of decision-making of online romance. This would therefore increase the frequency of reporting these crimes, prevention, and protection of future victims.
- Correia's (2019) review of 17,049 reports from victims, found that only 19% had been 'actioned' - in terms of being referred to a police force or partner agency.
- Cryptocurrency has become a global phenomenon over the last decade with the rise in cryptocurrencies scams. Merryweather, (2022), reports an estimated 9 million people have been targeted by social media platforms, with many losing thousands in life savings in stark comparison to mass-marketing scams for an individual. Many victims lose their home, isolate themselves from family and friends, turn to substance misuse or even suicide.

6. **Effectiveness of the current system for reporting fraud**

Our projects with police forces in the UK and USA (Florida) and colleagues with lived experience of perpetration (We Fight Fraud) outline several issues in reporting and recording fraud which can result from the reliance on victim-led reporting systems. For example, regarding demographic details of victims, missing data makes it difficult to identify patterns of victimisation and levels of risk for appropriate prevention strategies to be targeted. However, our research does suggest that particular communities and age brackets may be more at risk of specific types of fraud and thus

more comprehensive data capture is needed for a more robust evidence base, particularly around repeat victimisation and the nature of the offence itself.

Furthermore, reporting systems do not record victim impacts beyond financial loss (reinforced by Correia, 2019); therefore, other impacts such as the psychological, emotional and social effects are not adequately captured. This, coupled with difficulties in data capture regarding victim and offender demographics and characteristics of the fraud offence, make it difficult to identify useful patterns of victimisation and social engineering tactics which may assist in creating effective preventative strategies. A focus on financial loss may also mean that higher cost fraud such as investment fraud is being prioritised as highest harm, thus de-prioritising those with lower cost (such as the more person-centred frauds) which may be having more varied and significant impacts on victims. Forces also face difficulties, due to resourcing, they have in appropriately signposting victims to support agencies and in their lack of capacity or sometimes capability (e.g. across international borders/difficulties in tracing cryptocurrency quickly) to investigate.

We are currently conducting a comparative analysis of US and UK fraud data from two police agencies with a particular focus on victim demographic characteristics to help inform reporting and law enforcement investigative practices.

7. Fraud Sentencing

The following information in this section is drawn from the findings of a systematic literature review conducted for the Scottish Sentencing Council by Fish et al. (2022):

- Those who have more power and status, i.e., white-collar offenders, are often perceived and sentenced differently to blue-collar offenders, such as those who commit welfare fraud (Gustafson, 2009; Marriott and Sim, 2017). So called blue-collar offenders may be expected to receive harsher treatment during various stages of the criminal justice process than white-collar offenders (Gustafson, 2009). In Australia, Marston and Walsh (2008) comment that, when looking at case law, a sentence of imprisonment is generally considered as the starting point for cases of social security fraud by the courts. Although the court is not obliged to impose a sentence of imprisonment, courts in Australia emphasise the importance of deterrence for this offence, and the imperative of protection for the integrity of the social security system (ibid). Therefore, the firm approach of imprisonment is deemed as justified for these reasons. When looking at cases of tax evasion however, this is not the case with tax evasion, aside from the most serious cases. This disparity is also reflected in numbers of investigations. Whereas the tax authority in New Zealand investigated around 0.01% of taxpayers per annum, the welfare agency investigates 5% of welfare recipients (Marriott, 2013).
- Austin found that welfare offenders generally received harsher punishments than those convicted of tax offending. On average welfare offending was 'punished more harshly dollar-for-dollar than tax offending' (Austin, 2016:2). This finding, gained from cases of welfare and tax fraud between 1989-2016, concludes that the length of prison term relative to the money obtained was much greater for welfare offending (Austin, 2016).
- Results from the case analysis of Villum (2018) found a correlation between gender and the type of punishment granted for benefit fraud. In a sample of 141 cases, females had a proportionately higher frequency of probation and community sentences than that of males.
- In a Scottish context, Crowe (2021) comments on the outcome of the appeal in RA v HM Advocate, within which a mother of six children had the sentence of 12-month imprisonment affirmed in respect of a £55,000 benefit fraud that spanned six years. For added clarity, this sentence was discounted from 18 months for an early plea. This type of case arises when a single woman claims benefits and then does not change her claim when her partner returns. Prior to the appeal, the accused was making repayments of £100 a

month to the Department of Work & Pensions. Crowe then asks a key question in this debate; with RA being granted imprisonment, is this not surely her payment for her offence? Has she not already paid her debt to society? Will she have to continue these payments of £100 a month to the DWP after her release? With the victim in benefit fraud being the public purse, perhaps then it is counterproductive for more public resources to be driven into incarceration and court processes, in a way further harming the 'public purse' that is trying to be punished.

- Although the court in Australia is not obliged to impose a sentence of imprisonment for this branch of fraud, various case law reviewed by Marston and Walsh (2008) shows that imprisonment is generally regarded as the starting point. Emphasised consistently by the courts was the importance of deterrence and upholding of the social security system. Epstein (2013) studied sentencing remarks made by magistrates, Crown Court judges, and the Court of Appeal in 50 cases of the imprisonment of mothers with a dependent child in the U.K. In a particular case of benefit fraud were the mother had three children, the judge made no mention of the children during sentencing. Epstein continues to say that after looking at several sentencing remarks in cases of benefit fraud, courts often stress that the imposition of custody is used as a deterrent to other potential defrauders of the benefits system. This is despite research demonstrating the negative impact of maternal imprisonment on children (Minson, 2019). Although deterrence as a purpose of punishment is acknowledged, it has to be considered alongside the weight of mitigating factors when sentencing decisions are ultimately made. More effective punishment, for example the use of community justice as mentioned earlier in this section, would have less of a devastating effect not only on mothers who have committed fraud, but their dependents.
- An example of community forms of punishment is electronic monitoring (EM). Holdsworth and Hucklesbury (2014) interviewed 31 women, the vast majority of whom were first-time offenders charged with benefit fraud and sentenced to EM. EM-curfews allow women to continue their caregiving duties as well as continue working. EM was a favourable option amongst the women as it disrupted their lives the least. All of the women participants stated that the EM curfew made little difference to their family routines. This choice of sentence therefore effectively imposes a punishment, whilst simultaneously considering factors which may disproportionately affect particular groups of offenders.
- Research from Marston and Walsh (2008;285) in Australia suggests that most cases of welfare fraud involve relatively small debts, with explanations that are far more complex than the stereotyped media representation of the 'welfare cheat' suggests. Their small-scale empirical study of sentencing outcomes for social security fraudsters in Brisbane, Queensland found just this. They also discovered that, in most cases, the defendant had repaid some or all of the debt before the court appearance took place (ibid).

8. Government response to fraud

Our research shows law enforcement faces significant challenges in securing executive buy-in from leadership that fraud should be and remain a top priority. Combatting fraud effectively necessitates specialised strategies that emphasise cyber intelligence, inter-agency collaboration, public awareness campaigns, technological solutions and continuous training and education for policing and multi-agencies that support victims. These require appropriate funding and recognition of the multi-faceted and severe harms that fraud causes.

Authors and Affiliations

Dr Emily Cooper (Senior Lecturer, UCLan)

Dr Nicola Harding (Lecturer, Lancaster University; Director of Research, We Fight Fraud

Prof. Sarah Kingston (UCLan)

Dr Nathan Birdsall (Research Fellow, UCLan)

Dr Rebecca Fish (Research Associate, UCLan)

Alice Mills (Research Associate, UCLan)

Georgina Bahri (Lecturer, UCLan)

Dr Deborah Powney (Lecturer, UCLan)

Dr Clare Scollay (Research Fellow, UCLan)

Tony Sales (We Fight Fraud)

Adam Boome (We Fight Fraud)

Solomon Gilbert (We Fight Fraud)

Andy McDonald (We Fight Fraud)

Larry Kraus (Pasco Sheriff's Office)

October 2023