Professor Michael Levi – Written evidence (FDF0042)

Introduction

Fraud is a very broad spectrum, encompassing serious or complex fraud within the remit of the SFO under the Criminal Justice Ac t 1987; high harm 'organised frauds' as understood by the NCA and ROCUs; tax and social security frauds (largely HMRC and DWP); and a vast spectrum of frauds against individuals, businesses and third sector bodies – digital, offline, and mixed . these are dealt with to varying degrees by police specialist units and divisional detectives, as well as by a range of regulatory bodies using both regulatory penalties and preventative efforts. There is no doubt that digital frauds have increased very substantially, in line with the digitisation of social life, and that this has presented major challenges for all of the Four 'P's: prevent, prepare, pursue and protect.

Working out what the optimal balance is between the four, and the optimal investment in each of them, as well as the appropriate organisational platform(s) and resources through to deliver them, is in the final analysis a political process, informed by limited evidence of impacts; the crude proportionalism of fraud numbers to policing numbers by the Social Market Foundation is an intellectually weak approach, though some of their other recommendations are sensible.[1] Institutional buy-in is a key component, and legislative frameworks as well as pressures from bodies such as this Committee clearly play a role in fixing liabilities or softer responsibilities.

Managing Responses

Designing *solutions* to 'fraud' is often an illusory goal: what we need to focus upon is the mitigation of a range of frauds. Without adequate monitoring and enforcement levels, the role of statutory – particularly criminal law - provisions in that mitigation process is largely hypothetical. It is not *wholly* hypothetical because some legitimate organisations take pains to stay within at least the letter of the law, while others are concerned about their reputational risk. A substantial part of reputational risk is mitigation of the chances and consequences of exposure, and this is a dynamic process, as those who formerly acted for wealthy Russian clients will be aware. Hence the salience of the comments by some who have given oral evidence to this Committee; these may be summarised as 'risks to offenders are low because there is little chance of investigation and prosecution'. It seems to be agreed by witnesses that reforms of the Fraud Act 2006 are not a sufficient condition for substantive fraud reduction; another question is whether they are necessary conditions, and that does not appear to be the case either.

The process of working out the adequacy of responses depends also on the moral messages that are intended and that are received, whether or not intended. As with the issue of whether the breaking of coronavirus laws are equivalent to speeding, levels of punishment are only a starting point. Frauds of all kinds evoke different social reactions, some based around almost Victorian

[1] https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/

conceptions of appropriate prudential behaviour by victims, while others treat blaming victims as a serious secondary harm in itself and seek to attribute blame instead to financial intermediaries for failure to prevent. Given limited resources, it might seem rational to focus intervention resources on 'vulnerable victims' but there is insufficient clarity about what that means. Does it mean anyone who is statistically likely to be a victim, or does this depend on the level of harm that single or repeat frauds generate, or on the ability to evoke a sympathetic response from media, public or police audiences?

Fraud Data Issues

England and Wales currently have the best data on fraud available in the world, but that data still has some major limitations, namely the *range* of frauds against individuals and businesses examined in the individual and in the business crime surveys. Sometimes design flaws get embedded in systems: in an earlier analysis of 2013-14 Action Fraud (AF) data, 'other' types of frauds accounted for over 30% of incidents,[2] and this applies to some clunky categories in Action Fraud's typologies so that the largest single category in those data are unclassified. That may soon change, with the reform of Action Fraud. Furthermore, surveys exclude those lacking mental capacity, persons in institutions, et cetera, as well as (by definition) those who are not aware that they have been scammed. This may not be a serious limitation, but these areas of vulnerability (e.g. fake Powers of Attorney, frauds against people under Court supervision) merit attention. What is counted, what is *not* counted, and what should be counted as 'risk indicators'? One of the things we might learn from the Covid-19 pandemic is how conventional methods of measuring harm and initial analyses of symptoms can be mistaken and generate sub-optimal outcomes, so in this spirit, we need to consider what components of fraud are omitted from existing counts, and whether our ways of identifying them earlier as well as of handling them might be improved.

Crime surveys measure particular sorts of frauds at a point in time, and usually include only completed frauds unless they specifically include attempts. Potential fraud victims may not know about third party efforts that have protected them, so surveys that ask them about what they have done to protect themselves may not be fully authoritative counts anyway. Police recorded frauds are more of a flow over time than are surveys, but even in those cases in which victims or third parties make reports and these are recorded 'for intelligence' or 'for investigation', there may be significant elapsed time from the event to the reporting and recording, even disregarding the issue of the proportion of frauds that are seriously investigated or the still smaller that have a criminal justice outcome.[3]

The 'balloon theory' in which fraud in one area that is squeezed merely reappears in another is commonly used, but it is little more than an assumption

[2] See Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2015). *The Implications of Economic Cybercrime for Policing: Research report, City of London Corporation*. City of London Corporation; Technical Annex.

[3] For a very useful study of this in relation to AF (but not other sources) in 2013, see A. Scholes (2018) *The scale and drivers of attrition in reported fraud and cyber crime*, Research Report 97, London: Home Office. The proportion of AF reports which had criminal justice outcomes then was 2 per cent. See also the recent reports on fraud policing by HMICFRS.

or 'folk theory' supported by some anecdotes and case histories. There is no logical reason why the total stock of fraud should be constant, within the public sector as a whole, within any part of the public sector, or jointly in public and private sectors.

Further, year-on-year comparisons are 'snapshots' of fraud, rather than an assessment of the dynamics of fraud. The unintended consequence is that the 'how much' figures do not add to some other important (and potentially difficult to answer) questions as *part* of a threat assessment to understand the extent to which individuals engage in a range of frauds or how far those committing fraud are sector specialists; how far the set of people and networks often labelled 'organised crime' will switch to fraud in general or particular types of fraud as a more lucrative and less risky activity than other forms of crime; how far changing attitudes in society expand or contract the potentiality for fraud among organisations' clients, customers and staff; and how far the changes in institutional cooperation and situational opportunity prevention cause fraudsters or potential fraudsters to look elsewhere to commit fraud. These all require good data on offenders, but with a low follow up to victim complaints, there will continue to be large gaps in our knowledge of offenders also.

Finally we have noted no mechanism that gears resourcing and strategic direction on the basis of available data. As a report for the Financial Services Authority (FSA) – the predecessor to the FCA - noted, using the apparent scale of fraud losses and focussing on specific groups of perpetrators, such as organised crime, may have little value unless it also maps where the greater harms lie and how roles, responsibilities and capabilities within the existing control environment map onto both losses and harms: 'the FSA needs to know which aspects of market failure leading to criminality it can effectively address (where it can make a difference). After all, knowing the scale or impact of various aspects of financial crime, but without knowing which of these the FSA can effectively address, would be unhelpful'.[4] Nevertheless, disregarding major SFO-type cases which typically mature over longer periods, the trends are clear that by volume, both frauds and concern about them are on the rise.

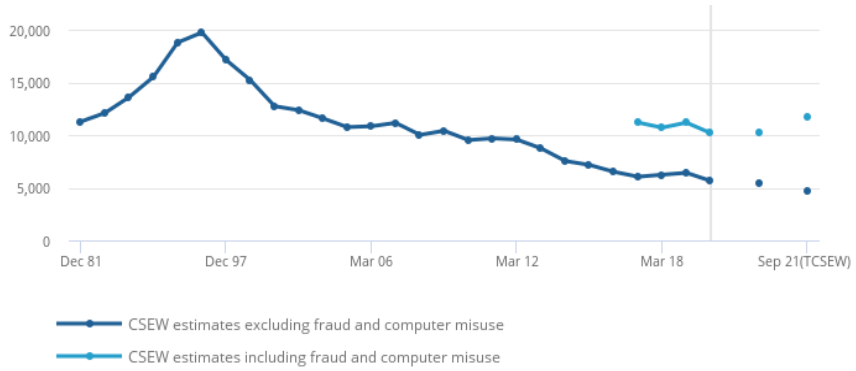
UK data on payment card fraud have always this century been illuminating and up to date (UK Finance, 2021): in recent years the largest fraud losses have been unauthorised frauds, mainly committed using payment cards. Online banking losses have more than doubled from 2010 to £159.7 million in 2020. In the first half of 2021, however, criminals focused their activity on authorised push payment (APP) fraud. This led to a 71 per cent increase in APP fraud during the first half of 2021 and, for the first time, the amount of money stolen through APP fraud overtook card fraud losses, reflecting better card fraud prevention and a rise in exploitation of social engineering opportunities and control weaknesses. So this is a combination of digital and some analog processes. According to the consumer group Which? (2022), more than 300,000 UK people lost £854 million to scams in the two years to the end of June 2021, but only 42 per cent of the

[4] Dorn, N., Levi, M., Artingstall, D. and Howell, J. (2009). *FSA Scale and Impact of Financial Crime Project – Impacts of Financial Crimes and Amenability to Control by the FSA: proposed framework for generating data in a comparative manner*. London: FSA. p5. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1458366

total was refunded to customers, despite the Banking Protocol which promises reimbursement. This plainly merits scrutiny, but also some reflection on what are the limits of acceptable customer deserts where they have been lulled into scams. It is not self-evident that bank shareholders or customers in general should pay for the foolishness of fraud victims, however difficult it may be for them to resist social engineering 'in the moment'.

Differently expressed, the risks of crime in the UK vary considerably by crime type, and both fraud and computer misuse offences outstrip all other property crime risks directly affected individuals. This was so before the pandemic, but the trend increased during it, as more people of all ages migrated their legal (and a little of their illegal) consumption online and spent far more time on it. This is shown graphically in Figures 1 and 2.

Figure 1: Trends in Survey Measured Crime in England and Wales, 1981-2021

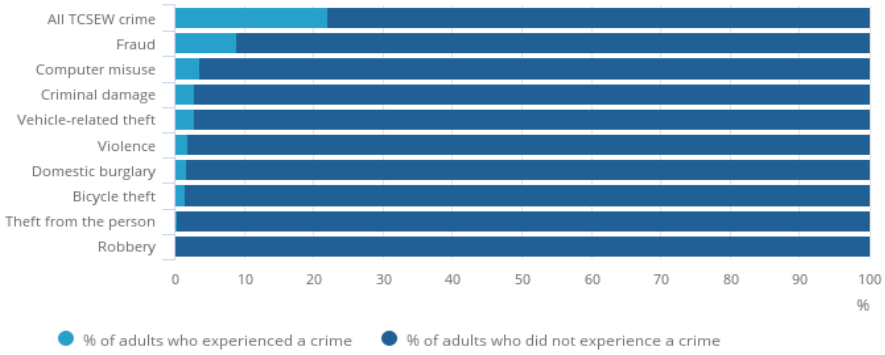


Source: Office for National Statistics - Crime Survey for England and Wales (CSEW) and the Telephone-operated Crime Survey for England and Wales (TCSEW)

Figure 2 below shows that fraud, followed by non-fraud computer misuse, are the two offences that are most likely to occur against individuals in England and Wales. It is a moot point whether the victimisation rate shown here is frighteningly high or reassuringly low: 1 in 12 people became victims, or 11 out of 12 people did *not* become victims of online or offline fraud in that calendar year, when so many fraud possibilities abound. There is no doubt that rises in online fraud are real, but the data do not reveal what proportion of the public were subjected to fraud attempts but successfully resisted them.

Figure 2: The likelihood of being a victim of crime varies by crime type

England and Wales, October 2020 to September 2021 interviews



Source: Office for National Statistics - Telephone-operated Crime Survey for England and Wales (TCSEW)

The Scale of Fraud

One key consideration when discussing responses is to understand what the data says about the scale of fraud, and those who are victims of what kinds of fraud. Estimates from the telephone-operated Crime Survey for England and Wales (TCSEW) showed that there were 5.1 million fraud offences against individuals in the year ending September 2021. The percentage of the population (8.9%) who were direct victims of fraud in that year alone was not far below the percentage who were victims of any other crime at all (12.3%) – if we add victims of computer misuse to the fraud data – the remit of this committee - it brings it up to 12%. Victims and repeat victims cover a full demographic spectrum. Of course, almost the whole population are indirect victims via frauds on business and public sector bodies including tax, social security, health and public procurement.

Fraud and Computer Misuse Data 2020-21

Offence group	Oct 2020 to Sep 2021 Incidence rate per 1,000 population	Oct 2020 to Sep 2021 Number of incidents (1,000s)	Oct 2020 to Sep 2021 Percentage, victims once or more	Oct 2020 to Sep 2021 Number of victims (1,000s)
ALL CSEW CRIME EXCLUDING FRAUD AND COMPUTER MISUSE	[x]	5,904	12.3	5,668

FRAUD AND COMPUTER MISUSE	151	6,982	12.0	5,517
Fraud	111	5,114	8.9	4,102
Bank and credit account fraud	61	2,838	5.0	2,294
Consumer and retail fraud	33	1,515	3.0	1,365
Advance fee fraud	10	480	1.0	441
Other fraud	6	281	0.5	214

Source: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables - Appendix Table A2.

This is a 36% increase compared with the year ending September 2019 and the number of fraud *victims* (as contrasted with the *incidents* figure above) showed a significant 27% increase compared with the year ending September 2019.

The estimates included large increases in "consumer and retail fraud", "advance fee fraud" (the highest *percentage* increase because from a low base rate) and "other fraud" and may indicate fraudsters taking advantage of behaviour changes related to the COVID-19 pandemic, such as increased online shopping and increased savings. For example, advance fee fraud offences included scams where victims transferred funds to fraudsters via postal/courier deliveries; 'other fraud' included investment opportunity scams. [5] A minority (26%) of these offences resulted in loss of money or property, with no or only partial reimbursement. Fraud and computer misuse offences do not follow the lockdown-related pattern of reduced victimisation, and their rises more than offset the reductions seen for other types of crime.F[6]

In the year ending December 2020, UK Finance reported 2.9 million cases of fraud involving UK-issued payment cards, remote banking, and cheques via their recording system, CAMIS. This shows a 4% increase compared with the previous year (2.8 million). There was a 68% increase in "remote banking" fraud (73,640 incidents). This increase reflects the greater number of people now regularly using internet, telephone and mobile banking, and the attempts by fraudsters to take advantage of this.

[5] For the most recent data, see *Crime in England and Wales: year ending September 2021* - https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2021#fraud

[6] For an excellent review of general behavioural changes from home working, see A. Felstead (2022) *Remote Working: A Research Overview*, London: Routledge.

Adults with what the FCA very broadly defined as 'characteristics of vulnerability'[7] are far more susceptible to these approaches: 12% paid out money, compared with just 1% of those with no such characteristics. Older people appear to be cagier than the young: 16% of 18-24 year olds paid out money, compared with 1% of those aged 55+. Of all who paid out some money, the average amount paid out was £6,160 and the median (half-way point) amount paid out was £240, so a small proportion of people lost considerably more than others. The FCA report does not state whether older people lost more, but this seems plausible because some of them have more money, and knowledge or beliefs about their assets could be a basis for targeting. Most of these frauds have a digital component at some stage in the money laundering process – including a rise in crypto laundering as well as crypto exchange exit scams - but it seems otiose for Fraud Act 2006 or analytical purposes whether we make a distinction between calls from landline phones and VOIP digital telecoms for the purpose of defining things as digital/analog. There may be practical differences, however, when organising prevention against number spoofing, et cetera.

It should recognised, however, that this scale does not always translate into a proportionate demand for a law enforcement response. Fraud offences reported to the police are recorded and collected by the National Fraud Intelligence Bureau (NFIB) from Action Fraud and two industry bodies, Cifas and UK Finance. Action Fraud (the public-facing national fraud and cybercrime reporting centre) reported a 27% rise in fraud offences (to 413,417 offences) compared with the year ending September 2020. The data showed a 42% increase in "financial investment fraud" offences in the last year (from 15,702 to 22,372 offences) and an 18% rise in "advance fee payments" (from 43,555 to 51,407 offences).

NFIB data showed referrals from Cifas (frauds against their member organisations) increased 5% (to 319,512 offences) compared with the year ending September 2020 while UK Finance reported a 49% increase (to 155,757 offences). Many cases recorded separately by UK Finance are not reported to the NFIB because they are of insufficient intelligence value. UK Finance reported a 5% increase in fraud incidents (to 3.2 million incidents) in CAMIS. There was a 53% increase in remote banking fraud (to 94,757 incidents), reflecting increases in numbers now regularly using internet, telephone and mobile banking, and the attempts by fraudsters to take advantage of this. It is not known whether there is a higher or a lower 'hit rate' but this may not matter to offenders so long as they obtain returns that satisfy them adequately. Between April 2019 and March 2020, the NFIB disseminated nearly 38,000 crimes to police forces in England, Wales and Northern Ireland.

The point here is both the complexity of frauds and the dynamics of what is investigated, or not investigated, by whom. Further, there are significant differences between sorts of frauds in the elapsed time from 'the fraud event(s)' (which sometimes may stretch over years) to awareness and to recognition as 'fraud' or even as 'a loss'. Most of the governmental and media attention is on

[7] The FCA (2021: 191) defines a vulnerable consumer as someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care. Characteristics associated with four key drivers of vulnerability (poor health, low capability, low resilience or the impact of a life event) may increase the risk of a consumer's being vulnerable to harm.

relatively short term scams against individuals and banks and social security (plus pandemic loans which have taken time to crystallise), and even some of those side-step questions about whether victims recognise them as fraud (e.g. some romance frauds; frauds by friends, families and lawyers against vulnerable individuals; pension fund and pension liberation abuses). In fields such as violence against women, policy and practice have been informed by an understanding of the special risks posed by repeat victimisation, but despite many discussions about 'vulnerability' in policing and social work circles, this has impacted responses to fraud unevenly. In short, even in England and Wales, where much effort has been spent on improving fraud data in the period since the 2006 government costs of fraud review,[8] it can be easy to forget that 'fraud' covers a range from the kinds of large, complex cases that are sometimes taken on by the SFO – only some dimensions of which are usually 'online' - to relatively small scale single victim interpersonal offline confidence tricks.

Responses and Interventions

Given the scale of fraud identified by surveys and, to a lesser extent, reports to Action Fraud, has and the levels of disseminated cases, what has been the strategic response by law enforcement in recent years and what have been the implications in practice for addressing fraud? It is recognised that there have been significant strategic, institutional and sector-specific responses to fraud, including a 2019 National Fraud Policing Strategy and a 2019 Economic Crime Plan, a 2020 Local Government Counter Fraud and Corruption Strategy, a central government functional fraud standard. Most major public agencies now have fraud units (as do banks and building societies, sometimes part of their Financial Crime Units, sometimes separate). The Economic Crime Plan is overseen by an Economic Crime Strategic Board which has 'agreed that a Fraud Action Plan will be developed by the government, private sector and law enforcement and will be published following the 2021 Spending Review'.[9] This is currently being developed, though the impact of sanctions against Russia and personal sanctions against Putin's associates, plus the rapidly evolving pressures over online financial abuse have made it a challenging exercise.

The Fraud Action Plan (FAP) gives a central role to the National Economic Crime Centre, located with the National Crime Agency, and 2021 also saw the relaunch of the Joint Fraud Taskforce, a partnership between the private sector, government and law enforcement to tackle fraud collectively and to focus on issues that have been considered too difficult for a single organisation to manage alone. It envisages roles for the NCA and the Serious Fraud Office, and it calls for a more coordinated response across law enforcement while enhancing

---

[8] Levi, M., Burrows, J., Fleming, M. and Hopkins, M. (with the assistance of Matthews, K.), 2007, *The Nature, Extent and Economic Impact of Fraud in the UK. London: Association of Chief Police Officers*. http://www.cardiff.ac.uk/socsi/resources/ACPO%20final%20nature%20extent%20and%20economic%20impact%20of%20fraud.pdf.

[9] HM Government and UK Finance. (2021). *Economic Crime Plan: Statement of Progress*. London: HM Government, p6. A useful summary of current trends and issues is found in Doig, A. and Levi, M. (eds.) (2021) *Frauds and Financial Crimes: Trends, Strategic Responses and Implementation Issues in England and Wales*, London: Routledge

the roles of regional organised units. It proposes the promotion of prevention as well as investigations.

Similarly, the National Fraud Policing strategy seeks to secure additional investment from government to establish nationally coordinated responses, work in partnership with the Joint Fraud Taskforce and with the finance sector to develop meaningful messaging. It also proposes that all victims who report to Action Fraud will be contacted and provided with protect advice, while local forces will embed fraud within their wider strategies and structures for identification and management of vulnerability and victim support. They will use victim data supplied by AF and Suspicious Activity Reports from regulated persons to safeguard those at risk from further harm and prevent repeat victimisation. The operational side of the policing response to fraud is shaped by the AF process, to the reports from individuals and organisations are added data from Cifas and UK Finance, and other sources, including telecommunications, government departments, and national and international police crime/intelligence systems. The NFIB assesses and data matches information and intelligence to identify serial offenders, organised crime groups and find emerging crime types, and then transmits these to police forces. (NFIB can also take down bank accounts, websites and phone numbers which are used by fraudsters.)

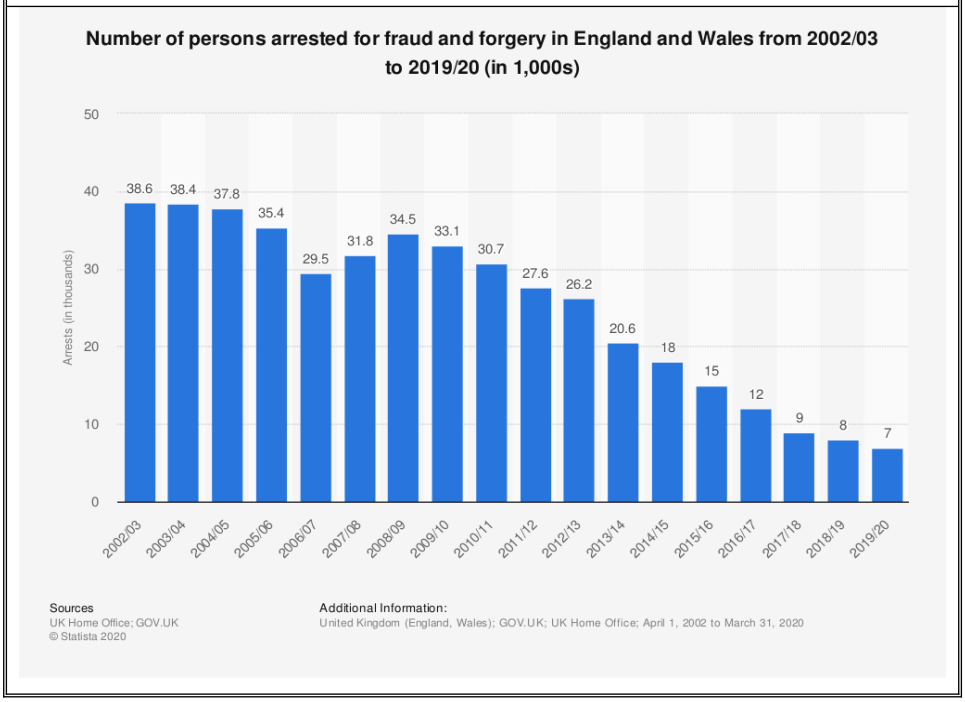
In practice, and away from the national strategic and policy statements, the reporting and investigation of fraud has been the subject of continuing concerns, none of which has been complimentary. A review commissioned following *The Times'* articles into the activities of AF and published in January 2020, succinctly noted that, 'for fraud to be investigated effectively, Action Fraud and the NFIB [National Fraud Intelligence Bureau] need to work seamlessly with the 43 police forces in an assured "end to end" process. However, the reality is that when cases are sent to forces for investigation, they frequently become lost among other priorities; there are disagreements about which force should take responsibility for investigations; and, most importantly of all, rarely are there sufficient detectives available to investigate them'.[10]

In terms of staffing, as of March 2021, the Home Office reported that there were 866 economic crime officers in English and Welsh forces (including regional asset recovery teams) from a total of 135,301 officers (although we note that dedicated economic crime officers are also allocated within other major crime units): this constituted 6.4% of total staff. However, our observations over decades to the present indicate that officers from economic crime units are regularly abstracted for homicide and other major enquiries, so the real proportion of fraud investigators would be lower. In 2018 the Police Foundation study noted that, 'judged by conventional criminal justice outcomes the police enforcement response to fraud is poor. Just three per cent of police recorded frauds result in a charge/summons, caution, or community resolution, compared

[10] Mackey, C and Savill, J. (2020). *Fraud: A Review of the National 'Lead Force' Responsibilities of the City of London Police and the Effectiveness of Investigations in the UK*. Accessible at: www.cityoflondon.gov.uk/about-the-city/about-us/Documents/action-fraud-report.pdf

to 13.5 per cent for crime generally. Fraud investigations also take much longer than most other criminal investigations'.[11] Historic data are unavailable for the specific case attrition, but fraud has always taken longer than other crimes for gain to investigate. In fact, the number of arrests has also been declining over the past two decades to less than a fifth of the number. This is not inherently a bad thing if the levels and cost of fraud were declining and/or if more meaningful rewards and sanctions were available to divert offenders, but rates and financial/social costs of fraud have not been falling.

Fraud and Forgery Arrest Numbers



Ministry of Justice data show that in the year ending June 2021, 4,406 people were sentenced for fraud, of whom a quarter (1,120) were imprisoned. Part of the issue here is that there has been a continuing shift in policing priorities and resources toward complex, sophisticated, and enduring patterns of criminal activity, which looked at fraud principally as a medium of exploitation by those already engaged in ongoing criminality.[12] This was in part because of government policy but also because organised crime offenders were seen as a bigger social threat than those who committed one-off or low-value frauds, or than managers, staff, customers, contractors or clients of public or private sector organisations who committed fraud. Between the 'high policing' of serious or complex fraud by the Serious Fraud Office (which even before the Bribery Act 2010 increasingly focused on bribery using its Deferred Prosecution Agreements, rather than on fraud) and the policing of fraud committed by organised crime groups (OCGs), there was a large hinterland of fraud. This ranges from non-trivial frauds committed by individuals (some of them organisational insiders),

[11] Police Foundation. (2018). *More Than Just a Number: Improving the Police Response to Victims of Fraud.* London: Police Foundation: p41. See also reports by the Victim's Commissioner and the Social Market Foundation.

[12] Apart from organised crime's increasing engagement in fraud, one developing aspect of the law enforcement approach to the investigation of OCGs was pursuit of their fraud schemes or money laundering-related activity not to combat fraud as such but because it presented a significant vulnerability to investigation and/or disruption and proceeds of crime confiscation under the relevant legislation and under the broadened definition of economic crime.

through frauds that clearly are 'organised' but not identified as committed by OCGs, to volume or lower-value fraud that might still cause serious distress, but which was not a high priority for police Economic Crime Units or others within the 'Pursue' function.

Attrition should be thought about in terms of processes (including elapsed time). Specifically:

- Awareness of victimization
- Decisions about what to do about the experience
- Reporting to (which?) enforcement/intelligence agency and/or civil litigation and/or trying to be wiser next time
- Investigation (or no investigation in most cases)
- Levels of domestic and international cooperation applied for and received
- Decision of authorities to aim for prosecution, disruption or other intervention (or No Further Action)
- Criminal trial
- Conviction and collateral impacts.

Thus in England, in the pre-pandemic year ending March 2020, out of 403,237 police-recorded frauds, of which 36,836 had been referred for investigation, there were 5,782 judicial outcomes. Without a better understanding of the specifics of criminal investigation, it is difficult to be 'realistic' about the potential for much better results within current resources or even for the 30,000 extra fraud staff suggested by the Social Market Foundation – the evidence base behind those numbers is absent, but if policing is removed from the constabularies, which sorts of fraud and victims would be prioritised by a new economic crime unit, how would capability be addressed and over what time frame? Though digital evidence sometimes leaves a better trace, it often requires assistance from private sector third parties – ISPs, card issuers and merchant acquirers, mobile phone companies, for whom such preventative and criminal justice work is loss-making – and sometimes from countries abroad.

International mutual legal assistance was designed for relatively rare cases, and with the exception of the powers and coordination available within the European Union- which the UK has left - it is a clunky and laborious process, especially for those lacking detailed knowledge and the imagination to frame letters of request in the language and legal format of other countries. There has been insufficient time to examine the inflows and outflows of requests in relation to digital and non-digital evidence: these need to be viewed interactively since international exchanges and trust-building are iterative over time. Some of these problems should be eroded by electronic translation, templates, and artificial intelligence, though evidential requirements may need to be adjusted which takes Parliamentary time and will, not just within Global Britain but elsewhere. However, though non-digital frauds did require elements of this cooperation, the sheer scale of cyber-enabled and cyber-dependent crimes make it harder, even

given the support of the requested law enforcement bodies and prosecutors, which has to take its place among other demands on them (just as incoming requests have to take their place and prioritisation among *our* scarce resources). One way of thinking about it is how much time does it take to process one case, and therefore given the amount of digital crime investigators available, how many such cases may be managed annually with a given set of resources. It is likely that the majority of mainly small cases currently reported by individuals to Action Fraud will remain untouched by any of the proposals made to the Committee to date.

Concluding remarks

'Fraud' should be broken down into sub-types and both reduction and justice strategies developed for each. Justice demands might require both substantive and evidential law changes, but these are neither necessary nor sufficient conditions for fraud reduction. This requires difficult social conversations about incentives and disincentives for action between different business sectors who might inhibit different parts of the social media-expanded fraud supply chain. Just as we now appreciate that more money will have to be spent on defence, it is inescapable that more money will have to be spent on fraud control if we are to make either a Justice or a Prevention impact, and preferably both. However, we must be clear about what we want from more expenditure on the police, on fraud victim care, et cetera, and on how we are going to judge improvement or that too binary term 'success'.

Within financial services, recent years have seen some serious efforts at dealing with money muling, whose existence and scale are a challenge to the effectiveness of anti-money laundering legislation as well as to fraud control. There has been some focus and expenditure on communicating warnings about fraud without much evidence of impact on victims, but within-app warnings do at least attempt to force customers to ignore them if they are in thrall to fraudsters' social engineering. If they do ignore those warnings, do they merit compensation? We need a stronger evidence base on impacts for the future, related to particular forms of scamming, as Alice Hutchings has suggested in her evidence to the Committee. Covid-19 was the first time that there was serious attention paid to persuading the public to avoid scams,[13] and the attention of the NCSC, banks and police to this is welcome, as is that of the FCA for warnings about high risk financial products, and organisations like Stop Scams UK are aiming at re-engineering fraud risks downwards. Designing out fraud and other cyber-security risks via evolving technologies[14] should be a serious goal, but there are limits to the plausible impact of technologies per se in eliminating all fraud. As with other areas of criminality, better risk management of fraud and cyber harms and enhancing our collective resilience remain more sensible goals.

---

[13] Levi, M. and Smith, R. (2021). *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19*. Research Report no. 19. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/rr/rr19; Buil-Gil, D., & Zeng, Y. (2021). Meeting you was a fake: investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime*.

[14] https://www.discribehub.org/ for a UKRI-funded initiative

22 April 2022