Article

Hiding behind the Veil of Action Fraud: The Police Response to Economic Crime in England and Wales and Evaluating the Case for Regionalization or a National Economic Crime Agency

Mark Button

Abstract This article explores the policing structures that emerged in the noughties in England and Wales to tackle economic crime, such as Action Fraud and the National Fraud Intelligence Bureau. This article reviews some of the growing literature on these structures, in-particular, two reports by Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services and a major investigation by the Police Foundation which provides a critical review of the police response to economic crime. This article argues the central problem is the lack of investigative capacity, among others. It also argues Action Fraud, which has become commonly derided, has become a useful veil from which the police to hide their inadequate response. This article argues radical change is required to address the investigative gap through either regionalization or a national solution, through a National Economic Crime Agency. This article considers some of the arguments for against such approaches and calls for a debate to commence on the future structures for policing economic crime.

Introduction

Action Fraud has become the focus of media, public, and professional vitriol for non-existent or ineffective response to fraud and related cybercrimes. This was exemplified by the 2019 expose of Action Fraud by The Times, where staff were shown by an undercover reporter to be mocking and misleading victims (The Times, 2019a,b). One report even featured a retired leading criminal psychologist, Professor David Canter, who had fallen victim to a fraud who had reported it to Action Fraud, a body he had not heard of until the police referred him, and had been shocked to discover his case was not investigated, opining, 'It is outrageous that cases are not taken more seriously. By not even taking fraudsters'

Director of the Centre for Counter Fraud Studies, University of Portsmouth, Portsmouth, UK
Email mark.button@port.ac.uk

Advance Access publication: 10 May 2021
Policing, Volume 15, Number 3, pp. 1758–1772
doi:10.1093/police/paab022

bank account details they cannot possibly find the networks behind these crimes.'

Fraud and related economic crimes have risen substantially over the last 30 years largely fuelled by the technological revolution associated with the internet and associated forms of communication (Ibrahim, 2016; Button and Cross, 2017). In England and Wales, the odds of being a victim of fraud/computer misuse were four times more than the burglary (ONS, 2020). The technological changes that have fuelled immense benefits in commerce, banking, friendships, etc., have also facilitated even more ways to become a victim of crime. Many countries' law enforcement structures are only slowly (it at all) adapting to this move from 'traditional' crimes, such as theft, burglary, robbery, etc., to the crimes of fraud, hacking, ransomware, etc. (Button and Cross, 2017; HMICFRS, 2019a,b). In the UK, in the early noughties, policymakers began to grapple with these changes and facilitated a variety of initiatives, such as Action Fraud, to try to better equip the limited capacity that existed to deal with fraud and the increasingly cross-border nature of it (both force boundaries within the UK and international borders).

This article evaluates some of the reforms that have been implemented to better tackle fraud in England and Wales, such as the introduction of Action Fraud and the National Fraud Intelligence Bureau (NFIB) along with the wider policing structures. The article draws upon a growing body of work that has evaluated these structures, in particular two reports by Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS) (Her Majesty's Inspectorate of Constabulary, 2019a,b), a significant investigation of the policing of fraud by the Police Foundation (2018), a report on Action Fraud commissioned by the City of London Police (COLP) (Mackey and Savill, 2020) and several other articles and reports (e.g. The Times, 2019a, b; Which, 2019). Some of these have been deep and intensive investigations. For example, Her Majesty's Inspectorate of Constabulary (2019a) involved 750 interviews, the inspection of 11 forces, 9 ROCUs, the National Crime Agency, Action Fraud among others, and the review of 250 calls from the public and 250 investigations, among extensive data analysis. HMICFRS (2019b) involved over 600 interviews and inspection of 10 forces, Action Fraud and NFIB, the analysis of 232 calls from the public and 129 investigations, among extensive data collection and analysis. The Police Foundation report was based upon 107 interviews, a survey of strategic leads in policing, a workforce survey, trading standards survey, case file analysis, and extensive analysis of data and other literature. This body of work has produced extensive data on the operation of the policing structures dealing with fraud and cyber-dependent crime. All have made relatively conservative recommendations around the existing structures to improve the response to fraud, with the exception of the Police Foundation, which advocates a move towards a regional response towards fraud. This article considers this argument and also evaluates an even more radical solution of the creation of a national response through a National Economic Crime Agency (NECA), which has also been advocated in the past in Conservative manifestos and by an influential think tank among others (Fisher, 2010; Brooks and Button, 2011; Ryder, 2011).

The purpose of this article is not to set out a blueprint for a new national or regional bodies, it is to look at the arguments for and against such changes and to stimulate a debate. The deep reviews of the policing of fraud and computer misuse expose serious gaps which are unlikely to be seriously addressed within the confines of current structures and with ever increasing volumes of these types of crime, starting a debate about more radical solutions seems timely and appropriate.

The tsunami of fraud and cyber-dependent crime

Economic crime is an increasingly used term without a rigorous definition, which is generally

assumed to cover fraud, corruption, money laundering, intellectual property crime, and certain cyber-crimes, which facilitate these. This article is largely focused around fraud and cyber-dependent crime, but use will be made of the term economic crime too when a broader view is required. Fraud, is a term that covers a wide range of criminal behaviours (as well as civil wrongs), perhaps best summarized by Section 2 of the Fraud Act 2006, where a person, 'dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss'. The essence is deception that is used to cause a gain to the perpetrator and/or a loss to the victim. There are a wide range of different types of fraud, some of which also have their own special legislation (such as benefits fraud), of which some of the most common are advanced fee frauds, investment frauds, romance frauds, consumer frauds, credit card frauds, and insurance frauds to name some. Cyber-dependent or computer misuse crime covers crimes under the 1990 Computer Misuse Act which can only be perpetrated via information technology such as hacking, computer viruses, distributed denial of service attacks, and ransomware. Many of these offences often overlap with fraud (although not all), such as hacking of customer databases to secure personal data that enable the criminal to either directly use it to perpetrate fraud (such as using credit card details to purchase goods and services) or to sell on the darkweb for others to do so.

There is nothing new about fraud, but the catalyst of technological advances of the last three decades has increased the volume of these offences substantially. Combined with the addition of the cyber-dependent crimes (computer misuse offences, such as hacking, malware attacks, ransomware, etc.) to the Crime Survey for England and Wales (CSEW) these have served to almost double crime. In the first publication of the experimental statistics these offences added 5.2 million crimes (3.4 million fraud and 1.8 million computer misuse) to the 5.9 traditional crimes experienced by individuals in year ending March 2017 (ONS, 2017). Figure 1 illustrates more recent statistics from the CSEW with, in the year ending December 2019 there were 5.8 million crimes (non-fraud and computer misuse), 3.8 million frauds, and just under 1 million computer misuse.

The National Fraud Authority (NFA) had also commissioned research on the impact of fraud on victims which had highlighted consequences comparable to other traditional volume crimes for

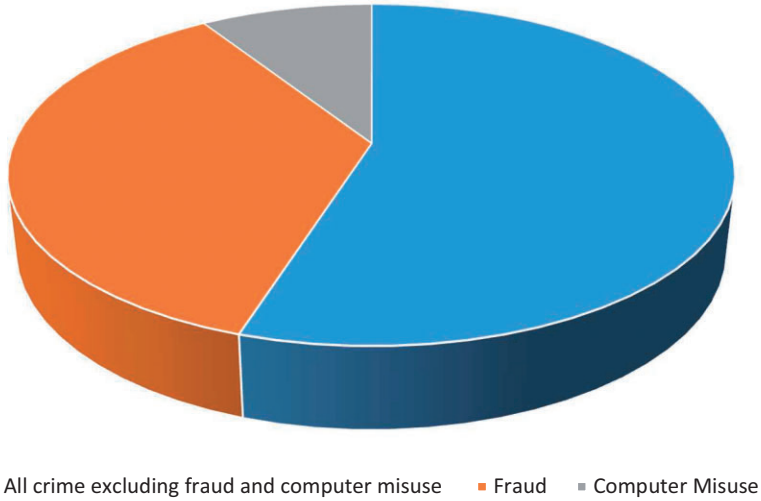

Figure 1: CSEW crime for year ending December 2019

many (Button *et al.*, 2009) as did the Sentencing Council (Kerr *et al.*, 2013).

It is also important to note that fraud and cyber-dependent crime have always posed unique challenges to the police. First, they are covered by specialist legislation that most police officers are not trained deeply in and which the nature of these offences requires such training. Secondly, with most other volume crimes there is often clear evidence of a crime and forensic evidence to harvest (a burglary might involve a broken window, possible fingerprints and DNA evidence, witnesses, and lost property). With many frauds and computer misuse offences this is not the case. Some frauds—and this is common with consumer frauds—there might also be a question over whether it is a criminal or civil matter, bringing into doubt whether the police should actually be involved. There might also be very limited evidence and leads to pursue or specialist knowledge and skills is needed to pursue. For example, a website that has lured victims to pay money for something false requires special training for an investigator to try and identify who is behind it and where the money has gone. Thirdly, with fraud and computer misuse there are many other states (e.g. Serious Fraud Office (SFO), Financial Conduct Authority) and private bodies (private investigators, insurance companies, banks, etc.) who investigate such crimes creating confusion and excuses not to become involved for some agencies (Levi, 1987; Button, 2019). Finally, many of these crimes cross both force and national borders causing additional challenges. All of these combined and make fraud and cyber-dependent a challenge for the police to deal with.

The noughties and the road to change

Policing before the noughties

During the 1980s the most significant development in the policing of fraud was the Roskill Committee on Frauds Trials, established in 1983 and reporting in 1986, it made a series of recommendations relating to the policing, prosecution, and trials related to serious fraud (Levi, 1986a). One of the most significant was for a unified body to investigate and prosecute serious frauds, which paved the way for the establishment of the SFO in 1987.

Research on the police and fraud was rare in the 1980s, 1990s, and noughties, but the small body of knowledge illustrated a number of common themes. First, a diversity of state and private bodies 'regulating fraud' (Levi, 1987). Secondly, a fragmented police capacity with some forces with specialist fraud squads, some with none, but most with limited resources (Levi, 1986b, 1987; Gannon and Doig, 2010). Thirdly, that fraud was generally a low priority for the police and policy-makers with Doig *et al.* (2001, p. 108) noting at the start of the noughties:

> . . .fraud is invariably not seen as core priority; it is not a Home Office objective and, apart from one force, not a force performance measure.

By the mid-noughties, however, two reports were published which triggered policy changes that laid the foundations for the current structures of policing. Commissioned by the Attorney General, these two 'Fraud Review' report conducted a very deep investigation into the extent, prevention, investigation, and prosecution of fraud in the UK. The review culminated in a hefty interim report and even larger final report published in 2006 with 62 recommendations (Fraud Review Team, 2006a,b). The final report was to lay the groundwork for developing structures in countering fraud that still exists today. It is not the purpose of this article to explore the findings of the Fraud Review in any depth, but they were damning, exposing a crime that was estimated to be a major cost to society, limited capacity in investigation in law enforcement, few prosecutions for fraud, limited co-operation, and poor support for victims to name some. The 62 recommendations included the following suggestions:

- The creation of a Nation Fraud Reporting Centre;
- the formation of a Nation Fraud Strategic Authority;
- for the COLP to become the 'lead force' nationally for fraud; and
- for better measurement of fraud.

The report had impact and in 2008 the National Fraud Strategic Authority (NFSA) was created with a remit to better gauge the size of the problem and facilitate across the public, private, and voluntary sectors of the economy more effective action to deal with fraud. It was also given responsibility for implementing the recommendation on developing a national fraud reporting centre, which was later named Action Fraud. The NFSA soon shortened its name to the NFA and published some significant estimates of the size of the problem of fraud (National Fraud Authority, 2012).

In 2010, however, a new Conservative Government was elected with an aim to cut quangos and the NFA was culled in 2014 with most of its functions redistributed. For many who had welcomed the focus of a national government agency directed at fraud at a time of rising rates, this seemed a negative step. Nevertheless, Action Fraud was moved to the COLP, which had already been given lead national status in response to the Fraud Review and which also hosts the NFIB and Fraud Academy. Other functions undertaken by the NFA were transferred to the National Crime Agency and the Home Office. The annual fraud indicator was one function that was dropped and not taken on by any of the other public organizations. Figure 2 provides a detailed description of the fraud policing structures in the UK.

Assessing the fraud policing structure of England and Wales

In this section the fraud policing structures in England and Wales will be evaluated using the growing number of depth investigations that have been published in recent years using a variety of themes.

Better reporting, intelligence, and analysis

National reporting for crimes that regularly cross both force and national borders is clearly beneficial in the fragmented policing system in the UK. As Which (2019) was to note in its largely critical report on Action Fraud:

> Before Action Fraud, local police forces often failed to share fraud reports with each other, so scam outfits could target victims around the UK without anyone spotting the bigger picture. The introduction of Action Fraud had at least one major benefit. Expert crime reviewers and analysts at NFIB receive fraud reports from all over the UK and form a broad intelligence picture. They can spot groups of scams linked by bank account details, names or other data (known as 'networks') and act quickly to allocate them to forces, or disrupt them (Which, 2019).

The advent of Action Fraud has brought with it increased reporting of fraud and data collection. This can better help victims and potential victims by quicker disruption of schemes targeting multiple victims and understanding the impact and needs of the victims (Correia, 2019). As will be shown shortly there has been criticism of the recognition of Action Fraud. But the reality is in the years preceding it there had been a marked decline in reports, which since formation has markedly picked up. Indeed, there was substantial evidence of fraud victims sent on merry-go-rounds of different agencies trying to report prior to Action Fraud (Button *et al.*, 2009). Now there is much greater clarity: Action Fraud or the police, the latter of which should refer on to Action Fraud unless it is a 'crime in progress'.

City of London Police

The City of London Police is the National lead force on fraud covering this crime on the National Police Chiefs Council (NPCC). This role entails a range of functions, but the most important of which it undertakes are responsibility for Action Fraud and National Fraud Intelligence Bureau and running the Fraud Academy. The force is also important because it also has one of the largest group of fraud and economic crime related officers largely due to its location in the City of London.

Action Fraud

The City of London Police contract out Action Fraud to a private provider, who run a call centre to receive telephone reports and a website for reporting and providing advice and support for victims. It is the:

- The single reporting centre for all fraud and cyber-crime reports from members of the public in England and Wales and Northern Ireland (Scotland recently withdrew and returned to receiving reports via the police). It receives these:
    - Directly from members of the public over the telephone (8 am–8 pm Monday to Friday for fraud).
    - Directly from members of the public via the online reporting tool on the Action Fraud website.
    - Directly from police forces or other law enforcement agencies on behalf of victims through the online reporting tool on the Action Fraud website.
    - Directly from businesses using the online bulk reporting tool on the Action Fraud website (HMIC, 2019a).

National Fraud Intelligence Bureau

The National Fraud Intelligence Bureau (NFIB) processes the information received by Action Fraud, along with information supplied by other agencies, such as Cifas and UK Finance on their database called the Know Fraud system. The bureau is staffed by police officers and other police staff and is not contracted out. In theory when an investigation appears viable, it is allocated to a police force or other law enforcement agency for investigation by the NFIB. It also provides forces and agencies with intelligence products. These include:

- Victim care packages, which provide details of vulnerable victims who need additional support;
- monthly victim lists, of all the fraud and cybercrime victims in a force area;
- six-monthly force profiles, of fraud and cybercrime in the force area; and
- threat updates of emerging types of fraud/cybercrime.

The NFIB also hosts the Know Fraud Database. This contains all fraud-related crime reports. It uses numerous tools to analyse data related to crimes solvability factors. Those that meet these criteria are allocated to staff within the bureau to review, analyse and develop. When there are viable lines of enquiry to pursue the offender, the matter is referred to the relevant police force or other law enforcement agency to pursue. This could be a police force, but also another relevant enforcement body, such as Trading Standards for consumer frauds and the Financial Conduct Authority for financial services related frauds. Victims who report to Action Fraud receive two potential outcomes: a follow-up letter stating no further action or lines of enquiry have been identified and it will be forwarded to relevant enforcement body for potential investigation.

Other key state actors

The *National Crime Agency* took on some of the functions of the old NFA related to developing a national strategy. The NCA hosts a National Economic Crime Centre as well as a small capacity for fraud investigation and it generally focuses upon serious organized crime. The *Home Office* is also important in funding many initiatives and holding a significant research capacity in this area. In the UK the police are divided into territorial separate *police forces* (and some national specialist police such as the British Transport Police) which include *43 in England and Wales, 1 in Scotland, and 1 in Northern Ireland*. It is important to note the priorities and division of resources, including how much is dedicated to fraud, are largely decided by each of them (influenced by the political structures that oversee them—Police and Crime Commissioners/Mayors in England and Wales and regional governments in Scotland and Northern Ireland and the Home Office).

There are also some other important investigative bodies dedicated to fraud, some of which are noted here:

- *Serious Fraud Office*: which has responsibility for the investigation and prosecution serious fraud and corruption;
- *Financial Conduct Authority*: which regulates the financial services sector and conducts enforcement action related to fraud in this area; and
- *Trading Standards*: the local government staff who enforce trading and consumer law and conduct some fraud investigations.

Figure 2: The Fraud Policing Structures in United Kingdom

The distribution of intelligence and cases with potential leads to pursue should also have in theory led law enforcement to save resources and better target cases with potential to pursue and there is an evidence that this has been occurring albeit on a small scale (Her Majesty's Inspectorate of Constabulary, 2019a,b). The Fraud Investigation Model, advocated by the COLP (which builds in alternatives to criminal prosecution when this is not possible, such as disruption by closing bank accounts, websites, etc.) also provides the basis for more realistic responses to frauds. Many reported cases which have not led to criminal justice outcomes have led to websites being taken down, bank accounts closed, cease, and desist action among others. Indeed, in the 2014–15 period the City of London Police (2016, p. 15) sent over 150,000 requests to partners in the UK and abroad to suspend websites, telephone numbers, and bank accounts linked to criminal activity, and closed down 3,889 websites in the UK alone. These actions would have prevented many further crimes, although how many is difficult to determine and has not been estimated.

Recognition and reputation of Action Fraud

Action Fraud is the centre of the web of new structures created and has not gathered the high visibility hoped for. It has also developed a negative brand among many that do recognize it. Research by Couture and Pardoe (2017, p. 22) found:

> The findings suggest that awareness of the official bodies established to tackle fraud is low. Asked who they would be most likely to report a scam to, nearly half (48%) of people said the police, with very small numbers naming Action Fraud (5%).

Many victims (and some professionals) do not understand what Action Fraud is (HMIC, 2015; Which, 2019). Indeed, HMICFRS (2015, p. 70) secured evidence from one senior officer who considered Chief Constables had, 'given [fraud] in its entirety to Action Fraud.' Some victims think it is a specialist police agency, which will conduct an investigation, leading to expectations of such a response (Button *et al.*, 2020). As evidence to the Home Affairs Committee submitted by the COLP noted:

> an expectation by some members of the public that most, if not all, frauds should be investigated. Operationally this is not feasible (House of Commons Home Affairs Committee, 2018, p. 23).

Action Fraud is in reality a call centre provided by a private company under contract to the COLP. The staffs, it employs, are largely low skilled and paid at around the minimum wage. It has no capacity to investigate. However, even in the area it does have responsibility for there is an evidence of areas in need of improvement.

The Her Majesty's Inspectorate of Constabulary (2019a) in their assessment found the growing volumes of fraud had led to an increase in an average call length from 12 min in 2012 to 19 min in 2018, between April 2016 and March 2018, call waiting times had increased from 8 to 16 min on average and HMIC noted abandoned calls were at 37% for the year to March 2018. These increases both stretch the limited resources of Action Fraud and frustrate victims who wish to report their incident as quickly as possible. Some victims struggled with the online reporting system too, which had subsequently changed by Action Fraud (Her Majesty's Inspectorate of Constabulary, 2019a; Button *et al.*, 2020).

The standing of Action Fraud, however, was damaged even further by an investigation by The Times newspaper published in 2019 which placed an under-cover reporter in the organization. The newspaper ran a series of front-page exposes with titles, such as 'Action Fraud Investigation: Victims Misled and Mocked as Police Fail to Investigate', 'Action Fraud: Thousands of Cybercrime Cases Ignored due to a Computer Glitch', and 'Action

Fraud: Victims Tell their Stories of Despair'. One of the Times reports highlighted how:

> managers at Action Fraud mocked those who have lost money as 'morons', 'screwballs' and 'psychos' (The Times, 2019a).

The reports exposed many other negatives beyond the mocking of victims. There were cases of victims with an evidence that could help in an investigation being ignored and led to believe their cases would be investigated. The reports also highlighted young workers with limited training have been thrown into handling discussions with highly distressed victims. Such was the concern that arose from the reports the City of London commissioned a detailed report into Action Fraud which identified numerous areas for improvement (Mackey and Savill, 2020).

The performance of the NFIB

The NFIB has a much lower profile than the Action Fraud, but undertakes some of the most significant work in identifying cases which could be investigated. The assessment of cases submitted to Action Fraud with the computer algorithm and case handler's appraisal determines whether the case has at least the chance of an investigation. HMIC noted that despite the increase in volume of fraud there had not been a corresponding increase in staff. The Police Foundation noted that it takes on average 54 days from report to dissemination. A long period of time when it comes to fraud, by which time many of leads (if they were to be pursued) may well have disappeared. HMIC found the packages that were sent to forces for potential investigation were mixed in quality, with some:

> . . .not easy to read or interpret and we considered they would be difficult to use for investigators who were either, not trained to deal with fraud or who were not regularly investigating it (Her Majesty's Inspectorate of Constabulary, 2019a, p16).

A report by Which (2019) also questioned the quality of some cases, noting some police forces, 'being given "appallingly" low numbers of detailed fraud cases to investigate'.

Once reported victims should be kept informed on the progress of their case, be provided with advice and support. Several investigations have also found an evidence of delays in response to this provision and in some cases not provided at all (see Police Foundation, 2018; Her Majesty's Inspectorate of Constabulary, 2019a; The Times, 2019a,b; Which, 2019; Button *et al.*, 2020).

Level of police resources and priority

Action Fraud might be the focus of much negative attention, but the reality is the most significant problem is the lack of resources and priority given to investigation by police forces. Several studies over the years have sought to gauge the level of investigative capacity in the police directed at fraud (Fraud Review Team, 2006a,b; Button *et al.*, 2015; Gannon and Doig, 2010). The most recent assessment conducted by the Police Foundation (2018) noted that there were 1,455 FTE police personnel working in economic crime in England and Wales, nearly half of which were civilian staffs ($n = 667$) and it must be noted, economic crime covers in addition to fraud, money laundering, corruption, etc. In 2017, the total number of police officers in England and Wales was 123,143 (House of Commons Library, 2020, p. 24), which would mean the 788 police officers amounted to 0.6% of police officers dedicated to fraud. Considering fraud (and computer misuse crime) amounts to a third to half of all crime against individuals this is a huge mismatch. Many senior police officers would argue that general police officers and detectives also have capability for many fraud and computer misuse investigations, but the reality is that such crimes are generally not a priority for such officers and the specialist nature of many of these

offences requires special skills, which many officers do not feel they possess (Bossler *et al.*, 2020). Indeed the Police Foundation (2018) noted from a survey of police officers in three forces that 86% thought fraud should be investigated by specialists and 74% felt that they did not have enough time to deal with a fraud case or victim.

Resources illustrate the low priority given by most police forces towards crime, although this does vary across forces. For example, the House of Commons Home Affairs Committee (2018, p. 26) found:

> In the year ending March 2017, for example, Devon & Cornwall received 1,055 referrals from the NFIB but recorded just one judicial outcome, along with 33 non-judicial outcomes. In contrast, West Mercia police received 388 referrals but recorded 288 judicial outcomes and 274 non-judicial outcomes. In theory, any investigation should result in an outcome, suggesting that in many forces, a substantial proportion of fraud offences are not being investigated (or they are not recording outcomes accurately).

Her Majesty's Inspectorate of Constabulary (2019a, p. 50) in their inspection found fraud was generally given a low priority and one interviewee even told them:

> Everything is against fraud. It is not a priority, not sexy, people don't report it and it is difficult to prove, which takes time, resources and money.

The low priority and resources available for fraud are the most significant problems, because this ultimately undermines any of the benefits that arise from Action Fraud and the NFIB. The police simply do not have the resources to process a significant number of the cases referred to them. Indeed, Her Majesty's Inspectorate of Constabulary (2019a, p. 5) even found:

> some forces seeking reasons not to investigate allegations of fraud – one force filed, with no further action, 96 percent of the cases it received from the National Fraud Intelligence Bureau; some of these cases had a good degree of evidence, including identified suspects. Staff performing this role were clear that their function was to 'reduce demand'.

Even in forces with capacity they were unable to cope. The Her Majesty's Inspectorate of Constabulary (2019a) found two forces they inspected accounted for 46% of NFIB disseminations, but these forces filed 37% of these cases without further investigation. These were cases which had been identified as having viable lines of enquiry.

The consequence of the low resources and priority is significant attrition. Both Her Majesty's Inspectorate of Constabulary (2019a,b) and the Police Foundation have noted this and the latter argued:

> While 3.2 million frauds were estimated to have taken place in 2017–18, just 638,882 frauds were recorded by the police and industry bodies. For every crime reported just one in 13 was allocated for investigation and in that same period only 8,313 cases resulted in a charge/summons, caution, or community resolution, representing just three per cent of the number reported to the police (Police Foundation, 2018, p. 4).

As the House of Commons Home Affairs Committee (2018, p. 27), noted, 'The proportion of fraud cases being investigated is shockingly low. . .'.

Level of specialist training

The COLP Academy, which leads on fraud training and is the biggest provider in this area in policing, although some forces do their own. Her Majesty's Inspectorate of Constabulary (2019a) found it only trains about 130 officers per year—another very small number given the scale of the problem. Consequently, not only are many police officers who investigate untrained in the speciality of fraud, they also lack knowledge of important tools, such as the Fraud Investigation Model and the products disseminated by the NFIB. The Police Foundation (2018, p. 75) also found strategic leads in policing, 'believed insufficient training was provided to practitioners in their local investigation (61%), neighbourhood (62.5%), or response teams (71%).'

Proposals to fill the gap

Some of the negative issues identified above relate to organizational structures, the ways things are done, quality of staff, training, etc., which could be implemented relatively easily. Indeed, many of the Her Majesty's Inspectorate of Constabulary (2019a,b) fall into this category. However, the problems of resources and priority, linked to some of the others can only be tackled by more radical reform. The Police Foundation has set out proposals for a regional solution and national solutions have also been advocated in the past. This article will now consider these two ideas illustrating the advantages and disadvantages.

Regional solutions

The Police Foundation (2018) and subsequent articles published by its authors (Skidmore *et al.*, 2020) have pushed for a more radical solution recommending:

> Fraud investigations should no longer be the responsibility of local police forces and all investigations should be handled by regional fraud investigation units that would exist alongside the Regional Organised Crime Units. This network of regional units should be coordinated and tasked by the City of London Police as the lead force accountable to the Home Office (Police Foundation, 2018, p. 72).

The desire for more local and regional based approaches is something Doig and Levi (2020) have advocated who are also critical of top-down London centric approaches. Mackey and Savill (2020) also argued for greater investigative resources located at a regional level.

a) Advantages. The main advantage of the regional approach is that it would create greater organizational capacity to deal with economic crime in both resources and expertise. The very small economic crime capacity that exists in many police forces could be better utilized at a regional level with bigger teams able to better learn from one another, target resources more effectively, and undertake larger investigations.

Regional bodies would be much closer to their communities than a national solution and with some regions having very strong identities, such as the North East, policing could become more tailored to those needs. Although there still might be a risk in large regions that certain areas receive disproportionate interest.

b) Disadvantages. There are already regional structures in policing, such as the Regional Organized Crime Units (ROCUs) and outside of policing circles these are not widely recognized. One of the challenges of a regional response is that existing and past regional police structures have suffered from a number of problems. They have lacked clear leadership and direction and accountability mechanisms have been less effective (Harfield, 2008). Such bodies are often low in profile and have lacked the strength and status to

withstand the organizational politics and turbulence of policing. For example, the National Crime Agency's antecedents stretch back through the Serious Organized Crime Agency, formed in part from the National Crime Squad, which emerged from the merger of Regional Crime Squads, illustrating the longevity of some regional bodies.

They would also add a further dimension of complexity, as organizations and overseas bodies seeking to deal with the fraud police in the UK would still face multiple bodies, albeit less than the present. There are therefore weaknesses in the regional solutions offered.

As with the national solution about to be discussed there would also be a risk as a consequence of regionalization local police forces abandoned economic crime completely and if such bodies were not adequately funded the impact on economic crime could be compromised.

National solutions

Button *et al.* (2008) argued that the Fraud Review could be laying the foundations for a national fraud police or national counter fraud executive. In both scenarios one based upon a national COLP force bringing in more resources and potentially encompassing the SFO too. The other was a more radical proposal of more preventative orientated regulatory body rooted in a Health and Safety Executive model. Brooks and Button (2011) also argued for a more national led solution to fraud investigation. Fisher (2010) wrote a report for the influential think tank Policy Exchange arguing for a new national 'Financial Crime Enforcement Agency' either built upon the SFO or a new body incorporating the functions of the SFO, Financial Services Authority (now financial Conduct Authority), what was then the Office of Fair Trading (2006) as well as some parts of HM Revenue and Customs and the relevant prosecution arms. Ryder (2011, p. 261) came to a similar conclusion arguing:

> The effectiveness of these anti-fraud agencies must be questioned. There is a considerable degree of overlap among the SFO and FSA; both have extensive investigative and prosecutorial powers that seek to achieve the same objective. The failures of the SFO are well documented; however, the FSA's effectiveness must be questioned because of its obsession with combating money laundering. It is recommended that a single financial crime agency should be established to coordinate the UKs fraud policy with extensive investigative and prosecutorial powers.

The 2010 Conservative Party manifesto was to argue for such a Fisher/Ryder structure (Ryder, 2011). This was never implemented and was missing from the 2015 manifesto, returning in 2017 with a less ambitious plan to merge the SFO with the NCA:

> We will strengthen Britain's response to white collar crime by incorporating the Serious Fraud Office into the National Crime Agency, improving intelligence sharing and bolstering the investigation of serious fraud, money laundering and financial crime (Conservative and Unionist Party, 2017, p. 44).

By the 2019 manifesto there was only reference to the creation of a 'new national cyber crime force' (Conservative and Unionist Party, 2019, p. 19) with a very little detail to its composition.

The NECA considered here goes much further than the regional solution by not only considering the merger on police capacity into a national body, but also some of the other existing national and local bodies discussed above. If a national body was to be considered another important aspect of the debate would be the extent to which some existing national and police bodies were part of it.

a) Advantages. One of the most significant advantages would be bringing together the expertise of relevant economic crime policing capacity creating an organization with extensive expertise, substantial resources, and economies of scale. There is a debate over the extent to which different bodies it should cover different policing bodies, but for the basis of this article the debate will be started with the most radical configuration. Figure 3 outlines what a NECA might be formed from. At its slimmest it could be the police capacity alone merged at its widest (Figure 3).

The creation of a 'NECA' could bring together the capacity of the COLP (Action Fraud, NFIB, Fraud Academy, Investigative capacity, including specialist units), the SFO and the small capacity of the National Crime Agency dedicated towards economic crime. It could also swallow the current constabulary capacity in economic crime teams at force and regional level. There are other bodies with a significant role in tackling different forms of economic crime where there might be a case for their inclusion too, such as the enforcement arms of the Financial Conduct Authority, Competition and Markets Authority, and trading standards officers currently within local government.

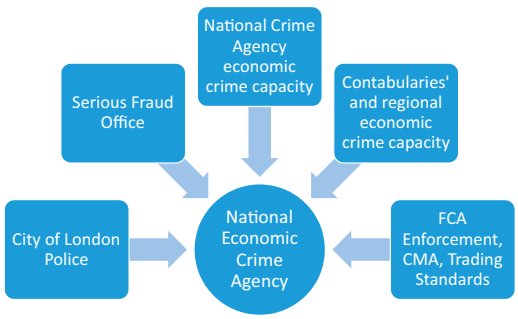

Figure 3: The potential components of the NECA

Some economic crime enforcement bodies have already developed more wide ranging and innovative approaches to counter economic crime, such as the COLP fraud investigation model, the SFOs use of alternatives to criminal prosecution, and trading standards use of the civil law and orders such as the Anti-Social Behaviour Order (Levi, 1987; Button *et al.*, 2015; Her Majesty's Inspectorate of Constabulary, 2019a; Hock, 2020). Bringing together a wide range of organizations could lead to such innovative approaches spreading across the whole organization. Figure 4 provides an example of the wide range of approaches which could be used. The expertise and training for many of these tools require a critical mass in an organization and such a 'heterogeneous'

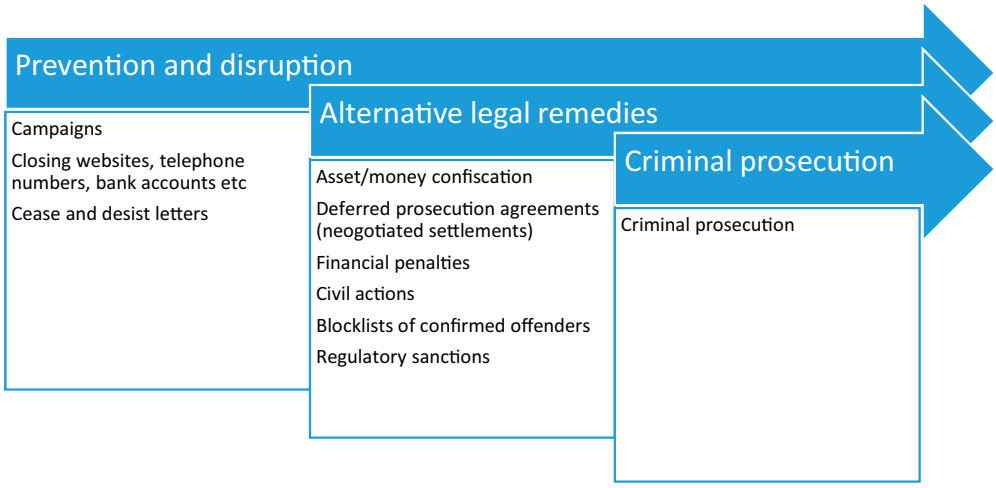

Figure 4: A hypothetical 'heterogeneous' prevention, disruption and enforcement strategy

approach, which might be more difficult to achieve in regional bodies.

A strong central body could also be much better at developing partnerships with other policing and enforcement bodies, the private sector, and relevant bodies in other countries. COLP is already involved in some partnerships, but there are so many more where a single coherent police voice would be much more effective from the regional and specialist fraud forums to international networks. There are a large number of bodies where one central police body, such as the NECA, could be more effective in negotiating and setting structures for regional and local partnerships too. It would also enable clearer, better, and more relationships with overseas law enforcement, something the current structures do not facilitate (Cross, 2020).

b) Disadvantages. There would be risks to a national organization too. The experience of Action Fraud has shown how this has given some forces the justification to further reduce their commitment to fraud. A strong argument could be that any national body (even if narrower than the much wider structure considered here) would lead to the complete abandonment of fraud and economic crime by the police.

If the new NECA did have the capacity to fill the gap this would not be a problem, but a serious risk would be the NECA in times of austerity is formed with inadequate resources. This could create a body that is still born if there are not enough resources. However, for some force areas with a very little fraud activity and the many victims that already do not experience an investigation this would be a low risk.

Another potential problem already alluded to is such a body would be London centric and out of touch. This risk could be addressed and it would be imperative on the creators to ensure structures were in place to avoid this with regional offices and engagement with communities and stakeholders.

Another concern is that the NECA might gravitate towards only the serious economic crimes, neglecting low-level frauds. Again it would be imperative for the creators to ensure structures such that this does not take place.

Conclusion

Economic crime is the most common type of crime and costs society billions of pounds. In the current policing structures economic crime will always be the 'Cinderella' crime falling behind other policing priorities and lacking the resources required for agencies to effectively tackle it. Much of economic crime requires specialist knowledge and skills (Bossler *et al.*, 2020; Skidmore et al., 2020). This article has explored two radical solutions to address some of these problems: a move towards regional investigation of economic crime or the even more radical solution of the creation of a new NECA, which could be based upon only the existing police capacity at the 'thin' end, through to a much more radical composition incorporating other existing national bodies too. This article has explored some of the advantages and disadvantages of these approaches. The evidence strongly suggests one of these alternatives is necessary, the status quo even implementing some of the less radical reforms advocated by HMICFRS, the Police Foundation and others still ultimately face the challenge of resources and priority in the existing local structures. This article has not sought to identify the clear solution, but rather to provide two options and most importantly start a debate long overdue on the future structures for policing economic crime in the UK.

References

Bossler, A. M., Holt, T. J., Cross, C., and Burruss, G. W. (2020). 'Policing Fraud in England and Wales: Examining Constables' and Sergeants' Online Fraud Preparedness.' *Security Journal* **33**(2): 311–318.

Brooks, G., and Button, M. (2011). 'The Police and Fraud Investigation and the Case for a Nationalised Solution

in the United Kingdom.' *The Police Journal* **84**(4): 305–319.

Button, M. (2019). *Private Policing*. Abingdon: Routledge.

Button, M., Blackbourn, D., and Tunley, M. (2015). 'The Not so Thin Blue Line after All?'Investigative Resources Dedicated to Fighting Fraud/Economic Crime in the United Kingdom.' *Policing: A Journal of Policy and Practice* **9**(2): 129–142.

Button, M. and Cross, C. (2017). *Cyber Frauds, Scams and Their Victims*. Abingdon: Routledge.

Button, M., Lewis, C., and Tapley, J. (2009). A Better Deal for Fraud Victims: Research into victims' Needs and Experiences. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118468/better-deal-for-fraud-victims.pdf

Button, M., Sugiura, L., Blackbourn, D. et al., (2019). Victims of Computer Misuse. https://researchportal.port.ac.uk/portal/en/publications/victims-of-computer-misuse(5e1984a5-974e-490a-984b-777691286e51).html

Button, M., Wakefield, A., Brooks, G., Lewis, C., and Shepherd, D. (2015). 'Confronting the "Fraud Bottleneck": Private Sanctions for Fraud and Their Implications for Justice.' *Journal of Criminological Research, Policy and Practice* **1**(3): 159–174.

Button, M., Johnston, L., and Frimpong, K. (2008). 'The Fraud Review and the Policing of Fraud: Laying the Foundations for a Centralized Fraud Police or Counter Fraud Executive?' *Policing: A Journal of Policy and Practice* **2**(2): 241–250.

Button, M., Sugiura, L., Blackbourn, D., Kapend, R., Shepherd, D., and Wang, V. (2020). Victims of Computer Misuse. Portsmouth: University of Portsmouth. Available at https://researchportal.port.ac.uk/portal/files/20818559/Victims_of_Computer_Misuse_Main_Findings.pdf

City of London Police (2016). National Policing Lead for Economic Crime Annual Review 2015–16. City of London Police.

Correia, S. G. (2019). 'Responding to Victimisation in a Digital World: A Case Study of Fraud and Computer Misuse Reported in Wales.' *Crime Science* **8**(1): 4.

Couture, X. and Pardoe, A. (2017). *Changing the Story on Scams: Protecting Consumers and Increasing Reporting*. London: Citizens Advice.

Conservative and Unionist Party (2019). Get Brexit Done Unleash Britain's Potential. https://assets-global.website-files.com/5da42e2cae7ebd3f8bde353c/5dda924905da587992a064ba_Conservative%202019%20Manifesto.pdf

———. (2017) Forward Together. http://ucrel.lancs.ac.uk/wmatrix/ukmanifestos2017/localpdf/Conservatives.pdf

Cross, C. (2020). 'Oh we Can't Actually Do Anything about That': The Problematic Nature of Jurisdiction for Online Fraud Victims.' *Criminology & Criminal Justice* **20**(3): 358–375.

Doig, A. and Levi, M. (2020). 'The Dynamics of the Fight against Fraud and Bribery—Reflections on Core Issues in This PMM Theme.' *Public Money and Management* **40**(5): 343–348.

Doig, A., Johnson, S., and Levi, M. (2001). 'New Public Management, Old Populism and the Policing of Fraud.' *Public Policy and Administration* **16**(1): 91–113.

Fisher, J. D. (2010). Fighting fraud and financial crime: a new architecture for the investigation and prosecution of serious fraud, corruption and financial market crimes. Policy Exchange.

Fraud Review Team. (2006a). Interim Report. http://www.lslo.gov.uk/pdf/Interim Fraud Report 03 06.

———. (2006b). Final Report. http://www.lslo.gov.uk/pdf/FraudReview.pdf

Gannon, R. and Doig, A. (2010). 'Ducking the Answer?. Fraud Strategies Police Resources.' *Policing and Society* **20**: 39–60.

Harfield, C. (2008). 'Paradigms, Pathologies, and Practicalities–Policing Organized Crime in England and Wales.' *Policing: A Journal of Policy and Practice* **2**(1): 63–73.

HMICFRS (2015). Real lives, real crimes: A study of digital crime and policing. Retrieved from https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services HMICFRS (2019a). Fraud: Time to Choose. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf

HMICFRS (2019b). Cyber: Keep the Light on. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/cyber-keep-the-light-on-an-inspection-of-the-police-response-to-cyber-dependent-crime.pdf

HMIC (2015). Real Lives, Real Crimes: A Study of Digital Crime and Policing. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

Hock, B. (2020). 'Policing Corporate Bribery: Negotiated Settlements and Bundling.' *Policing and Society* 1–17.

House of Commons Home Affairs Committee (2018). Policing for the Future. https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/515.pdf

House of Commons Library (2020). Police Service Strength. https://commonslibrary.parliament.uk/research-briefings/sn00634/

Ibrahim, S. (2016). 'Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian

Cybercriminals'. *International Journal of Law, Crime and Justice* **47**: 44–57.

Kerr, J., Owen, R., Nicholls, C. M., and Button, M. (2013). *Research on Sentencing Online Fraud Offences*. London: Sentencing Council.

Levi, M. (1987) Regulating Fraud: White-collar Crime and the Criminal Process. Tavistock.

Levi, M. (1986a). 'Reforming the Criminal Fraud Trial: An Overview of the Roskill Proposals.' *Journal of Law and Society* **13**(1): 117–130.

Levi, M. (1986b). 'Investigating Fraud.' *Policing* **2**: 196–211.

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. City of London Corporation.

National Fraud Authority (2012). Annual Fraud indicator. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118530/annual-fraud-indicator-2012.pdf

Office of Fair Trading. (2006). *Research on Impact of Mass Marketed Scams*. London, England: Author.

ONS (2020) Crime in England and Wales: Appendix Tables. Year ending March 2020 version of this dataset. Table A3. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

Police Foundation (2018) More than just a number: improving the police response to victims of Fraud. http://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/more_than_just_a_number_exec_summary.pdf

Ryder, N. (2011). 'The Fight against Illicit Finance: A Critical Review of the Labour Government's Policy.' *Journal of Banking Regulation* **12**(3): 252–275.

Skidmore, M., Goldstraw-White, J., and Gill, M. (2020). 'Understanding the Police Response to Fraud: The Challenges in Configuring a Response to a Low-Priority Crime on the Rise.' *Public Money & Management* **40**(5): 369–379.

The Times (2019a). Action Fraud Investigation: Victims Misled and Mocked as Police Fail to Investigate. https://www.thetimes.co.uk/article/action-fraud-investigation-victims-misled-and-mocked-as-police-fail-to-investigate-wlh8c6rs6

——— (2019b). Action Fraud Company Faces Sack as Police Scotland Pulls Out. August 16, 2019.

Which (2019). Exclusive: Scam Victims Ignored by Police Fraud Reporting System. https://www.which.co.uk/news/2019/09/exclusive-scam-victims-ignored-by-police-fraud-reporting-system/