

Devon and Cornwall Police – Written evidence (FDF0009)

This Paper has been recently submitted to the Commons Justice Committee as well and with their knowledge is now shared with House of Lords Committee. It specifically offers recommendation regarding legislation which I believe is relevant to the HoL review.

Thank you for giving fraud SPOCs from the policing sector an opportunity to respond to the Commons Justice Committee review into the Justice System's ability to effectively prosecute fraud cases.

I am Chief Inspector John Shuttleworth from Devon and Cornwall Police. I worked for ten years as a Detective Inspector involved in managing the force response to serious and organised crime and more recently took the lead for delivering a local fraud 4 P strategy.

In my submission I wish to cover the following areas of the review:

- The prosecution of frauds that are not of sufficient scale to be investigated by the SFO.
- Problems with evidence and disclosure in the prosecution of fraud cases, and

1) Prosecution of frauds not sufficient in scale for SFO.

Following a four year investigation in Devon and Cornwall, into a number of nationally based fraud OCGs, I can make the following observations.

In our cases the stolen money was filtered through multiple layers of bank accounts. The account holders were predominantly from Asian communities and most were not UK citizens, having arrived here as foreign students. Our work with Immigration Enforcement identified that high numbers of suspects had long since left the UK and travelled home; their bank accounts available for other money launderers to use. One case involved an account which was in use two years after the account holder had returned home. These individuals are being recruited at a very early stage on entering the UK and current efforts to target education establishments and educate naive foreign students are clearly only partly successful.

Elsewhere we found the response to these crimes varied across the forces and victims we spoke to. Whilst some forces embarked on investigations (although we found them to be in the minority), some referred the problem to their Regional Organised Crime Units (ROCU), some forces referred victims to Action Fraud, in line with national protocol. The majority of crimes were closed with no viable lines of enquiry seemingly because the suspects were indicated as living outside of the force's geographical boundaries.

The initial police response to fraud needs to improve.

The piecemeal response left victims without a consistent service. Victim F reported the theft of £100k, being advised to report direct to Action Fraud. She didn't see or have any contact from a police officer until we arrived on her doorstep over a year later to take a statement. It was a crime we discovered deep within the banking disclosures of one of our suspects. Mrs F lived many miles from Devon and Cornwall and the suspect had never stepped foot within our Force area. No-one was investigating her fraud. It remained one of the many cases reported to Action Fraud that are not subject to any further dissemination or investigation; crimes and victims that were and still are falling between the gaps.

Within the Home Affairs Committee Inquiry, published in October 2018 – Policing for the Future, Yvette Cooper MP, highlights the problem: 'it appears highly unlikely that more than one in 200 victims of online fraud would ever see the perpetrator convicted.'

Paragraph 50 of the paper states: 'It is sensible to have a centralised reporting facility for fraud, but this must not simply become a way to divert and fob off victims of crime. Most importantly, it must

be accompanied by a proper system to investigate crimes and respond to victims, or it will become irrelevant.'

The report goes on to state:

- Lack of clarity regarding inter force cooperation when cases cross force boundaries.
- Of 260,000 cases recorded by Action Fraud each year, 27% are disseminated to Force and 3% end with a judicial outcome

If Mrs F reports a fraud of this nature where money has been siphoned from her account into another, the information she has available to her is limited as to where the money has gone. If she is lucky enough to see a police officer at the initial reporting of her crime, the officer may establish the receiving criminal bank account and may identify a phone number linked to the suspect. Many forces would end their investigation at this stage, identifying a bank account registered to another part of the country and a mobile telephone that is 'pay as you go'. Their expectation being that Action Fraud would progress the information gathered.

So in the majority of cases Action Fraud will capture the 'first layer' of the banking trail. In all the I managed as SIO, the first layer account was a 'mule account', which paved the way to multiple other money laundering accounts. Each one designed to hide the money, launder at each part of the process, with small amounts being passed to account holders before it is dissipated beyond trace. A money trail that would take investigators months to track across multiple bank accounts; money that would be long gone by the time investigators obtained banking orders and waded through pages of financial data.

Unless a police force or specialist crime unit is invested to follow the money trail expeditiously, Action Fraud will only ever get the mule accounts from victims such as Mrs F. When you multiply this across thousands of victims, the intelligence picture available to NFIB is piecemeal, identifying single accounts with no consistent pattern where the money is ending up. This reduces their ability to see a true picture of crime, resulting in less cases being disseminated for forces to investigate and leaving victims without justice.

Conversely, if the initial police response and gathering of evidence is more comprehensive then the information available to Action Fraud is 'richer' and enables far more insightful links to be made. The disseminations to police forces therefore become more convincing and compelling in identifying the organised crime gangs that sit behind these large scale frauds.

The Home Office Affairs Committee paper on policing for the future goes on to quote Security Minister, Ben Wallace MP: "[it is] very clear that capabilities need to be aligned more intelligently between national, regional and local" structures.

Policing still functions in geographical boundaries and organised crime involving cyber enabled fraud will never fit nicely into geography; it transcends borders and is part of a global web of criminality.

The SOCS 2018 strategy states: 'Police force responsibilities focus on: local policing across the '4Ps' in response to national priorities; identification and management of local threat; and local safeguarding of children and adults'. I am unconvinced that such delineation between local, regional and national boundaries can be maintained in an age where crime has evolved, especially cyber based.

The strategy commits to 'establishing a single, whole-system approach - At the local, regional, national and international levels, we will align our collective efforts to respond as a single system.'

Whilst I have observed tasking and coordination processes and partnerships across agencies improve significantly in the last ten years, it has to be remembered there is always a limit to the capacity of ROCUs, NCA and other specialist serious and organised crime resources – I would contest they are not established to tackle all cross border organised crime and police forces need to re-think their

model of policing based purely on geography in all scenarios. Both ROCUs and NCA have thresholds for harm and have finite resources to match and currently this leaves a void for crimes such as this. Fraud is now a volume crime and has to be business as usual for all law enforcement.

So what does this mean when Mrs F reports her fraud? At first glance it won't have any appearance of organised crime, neither will the other hundreds of reports received across the country with the same MO with different bank accounts used by the money launderers. It will never appear as organised crime until someone is able to join the dots; and when they do, it may still not reach thresholds for regional or national squads and by this stage, the investigation team have already invested many hours of their time building the picture of criminality and the evidence.

The ethical dilemma for forces is whether to embark on pursuing criminals linked to these offences or whether to simply ensure safeguarding around the victim and hope that Action Fraud are able to see the hidden organised crime that sits behind these individual reports of fraud. Currently if the force isn't careful it will quickly assume responsibility for the investigation due to the transfer principles with the Home Office.

Recommendation: All forces need to agree a minimum level of investigation for all reports of fraud over an agreed threshold of seriousness/harm.

Recommendation: Forces that undertake national scale investigations into OCGs should be able to access central funding, administered through the ROCU's

Operation Fardel cost an estimated £500k to run over the four years, with less than 5% of the victims from Devon and Cornwall. Yet the outcome has resulted in the dismantling of two organised crime gangs with links to over £7million in fraud. The ROCU should be able to flex its resources or access funding to assist Forces that lead on investigations of this nature.

According to SOCS 2018, "currently there is no dedicated serious and organised crime funding stream; funds are allocated from a range of sources, spread across the many different agencies involved, and often bid for on an annual basis from specific programme budgets. This restricts our ability to ensure investment is focused on those areas of highest priority. To remedy this, investment needs to be placed on a sustainable footing and consideration given to how and where capabilities are built across the system and resources best directed and allocated. Therefore, we will explore a new funding model that is able to commit investment over multiple years, including for ROCUs to cement their position and support the development of the whole system."

This development could see cases adopted by individual forces tackling national OCGs, funded by central government and facilitated by regional ROCUs. This would help ensure parameters for investigation are around harm and not be unduly influenced by local budgets or geography.

2) Problems with evidence and disclosure in the prosecution of fraud cases.

Let's explore briefly some of the investigative challenges for a force when they do embark on an investigation of this nature. We start with one, two, maybe a handful of crimes within the force area. We quickly identify the mobile phone is no longer in use and has no attribution linked to it. Without intelligence or evidence from other sources, investigations of this type very quickly turn into financial investigations: the fraudsters contact the victim by phone using an unsubscribed mobile which they dispose of within a week; the money is transferred to a mule account of a foreign student that has since left the country and the challenge is on to find those responsible. A challenge that results in months of work.

These crimes typically involve as many as twenty, thirty different bank accounts and each account leads to another potential suspect account, where new victims and offences are discovered.

Very often decisions around the scope of investigations are based on the harm evident from the criminality. Remember that the footprint associated to this crime may only be a handful of crimes within a force area and tomorrow the fraudsters turn their attention to a telephone directory in

another part of the country. This makes it difficult for Forces to justify significant investment in tackling these crimes pursuing offenders.

Police Forces are under increasing fiscal pressures and the investment needed in these cases is significant not just due to the complexities of the criminality but also dictated by the burden of proof within the legislation for money laundering.

Those that played a small part in the overall crime, allowing their accounts to be used, turning a blind eye would still involve a great deal of work to investigate. The law under the Proceeds of Crime Act 2002 states that a person is guilty of money laundering if they 'knew or suspect' the property is criminal proceeds. So whilst sentencing guidelines allow for more punitive outcomes for those with a greater involvement it is still necessary to prove the mens rea (guilty knowledge) for everyone involved.

Every suspect I encountered denied guilty knowledge. The burden is therefore on the Crown to prove, requiring a substantial investigative outlay even for 'mule account' offenders. To reach the threshold of a realistic prospect of conviction, in the absence of an admission or other damning evidence, it was necessary to go to great lengths to prove the mens rea when the outcome in these lesser cases would often result in a suspended prison sentence.

With fraud being borderless and often international it provides huge challenges to law enforcement to hold any non UK suspect in the country long enough to bring them to justice. The main offenders in a number of investigations we undertook, were foreign nationals in the UK on student visas. All suspects denied having any 'guilty' knowledge that the stolen money in their UK bank accounts (provided to them by the banks, as visiting students) was derived from criminal acts. Without their admission it was incumbent on the police to spend significant efforts tracing money entries in and out of their individual accounts, tracing all accounts under their control to show a pattern of criminal behaviour, interrogate their electronic devices-, their lifestyles, identify further victims and gather evidence on a national scale. It took months and months to piece together all the evidence only to eventually bring the suspects to Crown Court. The Police, the defence and prosecution barristers, the court clerks, the judge, all waiting for the suspects to arrive and face trial. Unbeknown to us the suspects had acquired duplicate passports to the ones we had seized upon their initial arrest. They had subsequently returned home, evading justice and safe to spend the thousands of pounds they had sent overseas from their criminal activity.

In my experience, the law needs to change its burden of proof to enable a speedier prosecution where it is proportionate and appropriate to do so. In many cases it is appropriate to prosecute a 'mule' (someone who is not extensively involved in a criminal operation, other than to allow their bank account to be used for the transfer or laundering of stolen money), with an offence of 'causing or permitting a bank account to be used for holding or transferring criminal property'. This offence would remove the need to prove the account holder (or mule), 'knew or suspected' the money to be stolen. It is merely enough to show that the money was stolen and the account holder allowed someone else to use it. That the account holder willingly, in the absence of due diligence and reasonable excuse, permitted their account to be used by another and stolen property entered said account.

In removing the burden on the police and crown to prove a person had guilty knowledge in some cases, prevents a lengthy and costly prosecution to prove beyond all reasonable doubt to a jury that the defendant must have known the money was stolen. All of this can often result in a non-custodial sentence which is disproportionate to the amount of investment made by the police and CPS to get a case as far as the Court room, particularly when swift justice may actually prevent a foreign offender from remaining in the UK. Therefore, a speedier disposal of a case via a less burdensome piece of legislation may actually be the most appropriate and proportionate action to take and allow law enforcement to focus on the more significant criminals involved in the frauds and money laundering.

Absolute offences such as this apply in other areas of law and provide a further option for investigators and prosecutors around proportionality and the application of justice.

Recommendation: new legislation to assist police forces issue swifter justice.

The banking sector needs better ways of tracking and stopping stolen money laundered across the banking sector.

Finally, the one consistent feature in all these crimes is the criminal use of bank accounts. The work being undertaken on a national level is most encouraging. Undoubtedly the banking sector need to be doing more to rigorously administer their bank accounts to ensure legitimate use and whilst current provisions are inadequate the creation of law enforcement partnerships such as the Joint Fraud Taskforce and Joint Money Laundering Intelligence Taskforce are certainly welcome partnerships between NCA, City of London and the banking sector. But whilst small banks in rural locations are now closing and more and more personal contact between banks and their customers is diminishing, the need for the highest technology and software to identify unusual activity and compute algorithms becomes even more critical.

For example, I spent some hours with Mrs S who lost £45k to a vishing scam. She lost her husband a year later and two years on, she is still incredibly upset by the crime and her perceived treatment by the bank. The bank have refused to refund her money and this has left her devastated and without her life savings. Whilst this example is not intended to highlight a failing of the bank it nevertheless raises an important point; the suspects opened internet banking in the name of the victims and accessed their bank account, stripping it of its contents. The suspicious activity was not detected by the bank at the time, no call was made to the police alerting them of a crime in action and 24 hours later the money has disappeared. The fact that the elderly couple had never used internet banking before and the IP data for the banking was many miles from the location of our victims, failed to raise a question by the bank. No checks were made with the actual customers at the time and the money was stolen.

Whilst this doesn't directly refer to the two questions posed in this report for the committee, it is worthy of mention in my view.

12 April 2022