Crime script for mandate fraud

Michael Donegan

University of Derby, Derby, UK and Cyber Crime Investigation Unit,
Derbyshire Constabulary, Ripley, UK

Abstract

Purpose – The purpose of this paper is to critically analyse research surrounding mandate fraud and to
device a crime script identifying the crime commission process. It is hoped this will assist in standardising
investigation of mandate fraud by law enforcement.

Design/methodology/approach – The design of this paper follows on from the approach taken by van
Hardeveld et al. (2017) in identifying a cybercrime script for carding activity. The current environment
surrounding the investigation of digital fraud in the UK is examined through a review of the existing
literature. Analysis of the crime commission process for mandate fraud is then outlined in a potential crime
script identifying possible intervention points for law enforcement.

Findings – UK law enforcement’s current response to digital fraud is struggling to provide positive
outcomes for victims. There is inconsistency in the investigative approach and practical issues surrounding
how the digital fraud problem is tackled. Changing the emphasis of digital fraud investigation to focus on the
money laundering networks based in the UK also needs to be considered. Standardising investigation into
digital fraud by mapping out digital criminality using crime scripts and routine activity theory could be
beneficial for law enforcement. The results of this process could also assist in effectively identifying where
law enforcement resources may be best deployed to solve some of the practical issues highlighted.

Originality/value – There is little literature directly focused on a crime script for mandate fraud. This is
despite it being a significant contributor to fraud losses in the UK. For law enforcement, both digital and
financial investigation skill sets are required to investigate such offences. Therefore, mapping the crime
commission process has significant value for clearly identifying investigative intervention points.

Keywords Mandate fraud, Money laundering, Organized crime, Financial investigation,
Investigation, Criminal event

Paper type Viewpoint

Introduction

Fraud in the UK is estimated to have cost the economy £190bn in 2017 (NCA, 2017, p. 11). The third biggest contributing offence to this figure is called mandate fraud (MF). This involves an offender convincing a customer to change a payment process, by purporting to be a company that receives regular payments from them (NCA, 2018, p. 20). This is most commonly done through compromising and gaining access to a victim email account (Commonwealth Bank, 2018, p. 8). Despite preventative literature being published by the UK’s central fraud agency (Action Fraud, 2018) aimed at countering this issue, the number of victims has not reduced. Data obtained from Action Fraud have actually shown that between 2017 and 2018 the number of victim reports increased by 123 per cent to 3,451 (RSM, 2018). This corroborates a recent study, which concluded that UK law enforcement (LE) is failing to deal with fraud effectively (Police Foundation, 2018).

The prevalence of MF makes it important to consider how LE could effectively tackle the issue. Unfortunately, the researcher could find very little academic research, which directly covered MF. To address this gap in the literature this piece will provide a concise analysis of the investigation of MF in the UK. Existing literature will then be used to inform a potential crime script for MF. Due to the complex nature of this crime type, it will not be possible to
cover every aspect of the issue. This would require primary research with individuals involved in the investigation or commission of the offence, which is beyond the scope of this study. As a result, the aspects considered most poignant by the author will be the focus.

Frameworks
The concepts of crime scripts (Cornish, 1994) and routine activity theory (RAT) (Cohen and Felson, 1979) will be used in this research. These are prominent concepts within criminology and have been used effectively in studies on various crime types (van Hardeveld et al., 2017; Adamson, 2005). RAT outlines that the prerequisites for crime occurrences are motivated offenders converging in space and time with suitable targets in the absence of capable guardians. The implication being that the absence of either of the first two elements (offender and target) or the presence of the third (capable guardians) would be sufficient to prevent a potential criminal event (Miro, 2014, p. 1).

Crime scripts focus on identifying the process of crime commission, examining the procedural aspects and requirements put in place when committing a certain crime type. This allows for a method of organizing and systematizing knowledge about the commission of crime. The aim is to identify the fullest possible range of intervention points to enhance crime prevention opportunities (Cornish, 1994, p. 151). The potential drawbacks with crime scripting are that little research has been done on the action scripting process. This has led to the procedural aspects of physical and cybercrimes being predominantly modelled using intuitive rather than structured methods (Dehghanniri and Borrion, 2016, p. 1).

Current environment
Numerous sources argue that victims of fraud in the UK are being “let down” by LE (Police Foundation, 2018; House of Commons, 2018). They state that the challenge presented by those committing fraud offences is not understood by LE and mishandled as a result (HMIC, 2015; House of Commons, 2018). This argument of not understanding is corroborated by the apparent lack of research on prevalent offences such as MF. Improving this understanding is a real challenge for LE as they are dealing with a huge volume of offences, which present real difficulties in terms of effective investigation (Police Foundation, 2018).

One such difficulty is the cross over in policing disciplines, which frauds often represent. Many are committed online due to the high number of internet users presenting offenders with a plethora of potential victims (House of Commons, 2018, p. 22). As a result, digital frauds often involve offences under the Computer Misuse Act (1990) (CMA), the Fraud Act 2006 (FA) and the Proceeds of Crime Act (2002) (POCA). This is an issue for policing as specialist units are often in place for each of these pieces of legislation. Economic crime units for frauds, cybercrime units for computer misuse act offences and financial investigation units for money laundering (WMP, 2016). This often means that identifying who has responsibility for investigating a fraud is more complex than it should be (Police Foundation, 2018, p. 6).

Though no direct literature on this matter could be identified there are studies, which indirectly highlight the issue. Research findings have outlined that specialist units in LE believe they have a narrow remit directly linked to their skill set (Gale and Kelly, 2018, p. 20; Schreuders et al., 2018, p. 15.20). This makes for rigid operational structures, something, which literature has identified as potentially restricting problem-solving capabilities (Brown and Sutton, 1997, p. 22). MF is a prime example of a cross-discipline fraud, a recent study identified 94 per cent involved CMA, FA and POCA offences (Police Foundation, 2018, p. 21). With no one specialist unit covering all three offence areas it is possible to argue that rigid operational structures prevent cross-discipline offences from being effectively investigated.
Issues around who is responsible for investigating fraud could also be impacting the number of investigations and positive outcomes achieved. It has been reported that in 2017-2018 from the 277,561 frauds reported to the police, only 8,313 cases resulted in a charge/summons, caution or community resolution. This represents just three per cent of police recorded fraud (Police Foundation, 2018, p. 5). Some forces are not even investigating many of the frauds reported, according to recent evidence Greater Manchester Police only investigate 4 per cent of the Action Fraud disseminations they receive (House of Commons, 2018, paper 26). To cover every challenge fraud investigation presents is beyond the scope of this essay, a deeper examination is offered by the Police Foundation (2018). What is clear is that the issues are long-standing with HMIC (2015) highlighting an “absence of strategic leadership and direction” on digital crime including digital fraud. This is potentially a poignant point as it could be impacting LEs ability to effectively counter the issues. It has been argued that reducing crime requires a targeted approach, based on detailed knowledge of the crime in question (Dehghanniri and Borrion, 2016, p. 1). With a lack of leadership and direction it is possible that LE does not have the capacity to deliver a targeted approach for digital fraud offences.

RAT highlights how LEs approach is negatively affecting opportunities to reduce fraud. When considering the motivated offender element there is clear evidence to argue that offenders are maintaining high levels of motivation. In the current environment committing fraud is a very lucrative business, in 2017-2018 MF accounted for £77m worth of business losses in the UK alone (RSM, 2018). Corresponding with this only 3 per cent of frauds currently result in a positive policing outcome (Police Foundation, 2018, p. 5). As such offenders are able to operate with a level of impunity. With an estimated 86 per cent of people in the UK using the internet on a daily basis (House of Commons, 2018, p. 22) it is possible to contend that offenders are converging in time and space (all be it digital) with potential victims on a regular basis. In terms of the third component of RAT there appears to be a distinct absence of capable guardians. The volume of offences reported is one potential corroboration for this with the number of reported MFs rising by 123 per cent in 2017-2018 (RSM, 2018).

**Crime script for mandate fraud**

Crime scripting could be a valuable starting point for improving LEs role as a capable guardian. It would provide a way of identifying significant steps, which remain routine in the commission of the crime (van Hardeveld et al., 2017, p. 3.2). Breaking MF down into different steps could help improve LEs knowledge (Chiu et al., 2011), potentially making intervention points clearer and more accessible. It is important to note crime scripting will not show all the possible decisions and processes offenders could take. For example, in digital crime technological innovation offers offenders multiple, new and ever-changing choices in how they commit crime (Europol, 2017a, 2017b, p. 1). In this study, MF will be deconstructed into five potentially significant steps and an explanation provided for each.

To identify the significant steps the researcher has used crime scripts from other crime types and their own expert knowledge. It is acknowledged that this last element would not ordinarily be a significant source of detail in an academic study. The reason for inclusion here is that very little direct literature on MF exists, this is an issue for fraud in general with other studies highlighting this (Levi, 2008, p. 390). As such the researcher’s experience as a serving detective constable investigating digital crime has been a significant influence on the script outlined. To corroborate this influence wherever possible points outlined will be backed up with literature references. Where it is not possible detail will be provided highlighting this. The first significant step to be examined will be “preparation”.

There are
numerous pieces of crime script literature, which use this as the first significant step. These include traditional non-fraud based crimes (Light et al., 1993; Leddo and Abelson, 1986) and digital fraud crimes (van Hardeveld et al., 2017). Research findings highlight that digital fraud offences are largely committed by “financially motivated, organised global criminal enterprises.” (Bryant, 2008, p. 87). Considering this it is possible to argue that preparation is an important part of the process.

The next significant step will be “target selection”. For fraud to take place there has to be a target who will become the victim (Levi, 2008, p. 392). This step is present in the majority of crime scripts found in the literature (Light et al., 1993; Leddo and Abelson, 1986; Clarke, 1992). Following this will be “compromise”, some scripts reference actualisation as the stage at which a target has become accessible. For example, in a crime script for vehicle theft the actualisation stage is defined as removing the ignition barrel (Light et al., 1993). In this study compromise is seen a more accessible term for actualisation, it will, however, have the same meaning for the purpose of the script. “Doing” is a term used by some scripts to detail the point at which a crime occurs (Cornish, 1994, p. 162). In MF, communication is ordinarily used to engage the victim. As such the doing phase will be termed “engage” in this study. The final step will be “laundering”, given the international nature of digital fraud (Bryant, 2008, p. 87; McGuire, 2018), laundering the proceeds of the crime are an important aspect of successful fraud.

This is an effort at an initial macro-level crime script for MF. It is acknowledged that crime scripts have an inherently dynamic quality (Cornish, 1994, p. 175) and the aim in this study is to stimulate thinking on the subject as opposed to providing a definitive account on the matter.

Preparation
To carry out an MF several skill sets are often required. This is because the victim is often remote to the offender (Police Foundation, 2018, p. 21), and thus, the money laundering process is more complex. As a result, numerous persons are involved in the process (Ebenezer et al., 2016, p. 156). Technical abilities are needed to facilitate the manipulation of digital systems (Interpol, 2018, p. 3). Language skills can be necessary to communicate effectively with potential victims (Levi, 2008, p. 392). Enablers capable of recruiting and controlling money mules are also necessary components for the commission of the crime (CIFAS, 2018, p. 7). This is a lot to organise and each component part needs to work with the other to ensure the process is effective. As a result, there is often a management element who oversee the component parts (Interpol, 2018, p. 14; Ebenezer et al., 2016, p. 155). Some of the decisions they would need to consider in the preparation stage are:

What are the right forums to recruit the necessary personnel? For example, technically skilled individuals willing to commit the computer misuse act offences (Levi, 2008, p. 389). In some prominent areas linked to digital fraud, poverty and unemployment play a big role in making this process easier (Interpol, 2018, p. 5). What local, national and international network is required to facilitate the offence? This network is needed to recruit and control money mules, as well as laundering proceeds of crime (Interpol, 2018, p. 10). The preparation taken by the network is worth noting. Mules are not always recruited knowingly or willingly. Social engineering can play a major role in recruitment with social networks and dating applications being used to deceive potential mules (CIFAS, 2018, p. 7).

What communication system is in place to coordinate all of the component parts of the fraud? Efficient collaboration is a vital component of fraud offences (Levi, 2008, p. 389, Interpol, 2018, p. 10). It will also be necessary to consider what hardware and software are required to carry out the offence? MFs, which involve the compromise of an email account
are known to be facilitated by malware purchased by perpetrators from underground markets. Steps will not always be sequential (Levi, 2008, p. 390), which is why the concept of permutations, alternative actions in the process, are included in crime scripting (van Hardeveld et al., 2017, p. 3.2). Preparation may not be a step completed on every occasion. If the perpetrators are well organised this stage may only need re-visiting when circumstances change.

**Target selection**

To maximise the chances of success in-depth reconnaissance and research is necessary to accurately identify a viable target (Interpol, 2018, p. 13). Possible decisions at this stage are:

- What information needs to be gathered to identify potential targets? Small to medium businesses are considered particularly viable targets as they will almost certainly have payment correspondence communicated through email (NAFN, 2018, p. 2; Interpol, 2018, p. 11). What technical compromises are currently available and possible? An example of this is the Office365 security issues, which have made accounts vulnerable to compromise (NCSC, 2018). Offenders are aware of these issues and take steps to identify/exploit them. Once a target is selected what information relevant to them needs to be obtained? This will focus on the specifics of the business in question including staff details and any other publicly available information (NCSC, 2015, p. 7). What information needs to be disseminated to the network to ensure the necessary infrastructure is in place? The perpetrators will often look to make sure the money mule is in the same country as the victim. This is to remove any suspicions arising from an international payment request (Interpol, 2018, p. 10).

**Compromise**

This is the point where the technical elements of gaining unauthorised access to the targets email account are completed. This is one of the stages where many permutations could exist as it depends on what technical compromise the offenders have exploited. Potential decisions are:

- What form of compromise is being used? The means of exploitation need to be in place at this point. One popular form is phishing emails, which convince the target to reveal credentials for the network in question. (NCSC, 2018, p. 4). This can necessitate the setting up of domains to facilitate the capture of credentials or servers to control malware deployed (Interpol, 2018, p. 18). What security measures are in place? This element is not well-documented in the literature, however, there are uncorroborated sources, which outline some interesting points. In particular, the compromise of other networks to be used as a proxy to hide the offender’s true location (Quora, 2018). How will access be maintained if the compromise is successful? Many frauds are time critical (Levi, 2008, p. 393). To mitigate this offenders will look to change the rule set within an email account to hide their presence (Commonwealth Bank, 2018, p. 8). From the information analysed in the victim inbox what opportunities for fraud exist? These centre on suppliers of services that the victim is currently in contact with or use on a regular basis (NAFN, 2018, p. 2). These communications can then be targeted to facilitate the fraud.

**Engage**

To successfully complete this stage of the process it is necessary to competently engage with the second victim. This is the entity who will receive the fraudulent payment request. The offenders need to be proficient in the victim’s language and imitate the normal frame of
conversation to credibly imitate the relevant entity and deceive the secondary victim (Europol, 2018b, p. 8). Possible considerations are:

Having established the fraud opportunity what is the most opportune time to engage the victim? Offenders are putting significant time and resources into accomplishing these offences. As a result, they wish to obtain the maximum possible reward. This means they will monitor an email inbox to identify when to target high value payments (Commonwealth Bank, 2018, p. 9). Is it necessary to include an invoice when engaging the secondary victim? Some businesses use invoices, which are sent as attachments. Offenders will need to mimic this to prevent any suspicion being aroused (NFA, 2009, p. 13). Which mules bank account information will be used? Offenders will seek to use mules not resident in the same area as the victims. Mules will often be the first suspect to come to the attention of LE as in many cases their bank account information will be easily traced (Europol, 2018a). Being in the same area as the victim could provide LE with an opportunity to respond quickly to the offence. By having separate locations for victims and mules, investigations need to be transferred between police forces, slowing the response and effectiveness of LE. This is corroborated in research, which states that 78 per cent of frauds involved a victim and a suspect who did not live in the same police force area (Police Foundation, 2018, p. 43). Who within the network of facilitators is being updated to manage the laundering process? Victims are advised is to notify their bank as soon as they realise the offence to try and get the relevant funds frozen (Commonwealth Bank, 2018, p. 9). Offenders need to have communicated effectively with the relevant facilitators to get the laundering process started as soon as possible.

**Laundering**

Effectively laundering the proceeds of the offence is vital to reward those involved in its commission. Unfortunately given the clandestine nature of this activity and a broad range of opportunities it is difficult to provide a definitive insight into the decision-making process (Gilmour, 2014, p. 37). There is, however, literature on the methodology behind money laundering, which can be applied to allow for some outline of possible decisions. In particular, research outlines three distinct stages, placement, layering and integration, which should be considered by offenders (Reuter and Truman, 2004):

What is the placement strategy? To contravene anti-money laundering procedures, it is necessary to break up large amounts of money rapidly into smaller ones (Vocalink, 2017, p. 3; Lartley, 2016, p. 2). This avoids sudden large deposits into mule accounts causing a financial institute to freeze assets whilst they investigate the context surrounding the deposit (Wilson, 2018). As such decisions to be considered would include how many mules are required? How have they been briefed to respond to money coming into their account? Who is engaging with the mules in question? How is complexity being added into the process (the layering stage) to disguise the audit trail, ownership and source of funds (Lartley, 2016, p. 3)? Options for this include cash transactions, bank transfers, moving money overseas or converting deposited cash into other monetary instruments (Vocalink, 2017, p. 5; Lartley, 2016, p. 3). It could be argued that the international nature of these networks makes moving the money overseas to reward those not in the UK a key component.

What is the integration strategy? This stage could look different depending on the part played. For money mules the reward received will usually be small and they are often participating due to financial difficulties (Leukfeldt and Jansen, 2015, p. 177, 182). Thus, the reward is likely to be re-integrated in normal expenditure meaning no particular caution is taken. Facilitators have an elevated position in the criminal enterprise and this their reward
is likely to be more than the mules. Research suggests that some reintegrate their proceeds by purchasing luxury goods, which they use to show off on social media (Interpol, 2018, p. 8). Others look to invest in longer-term assets such as property or land (McGuire, 2018, p. 21). The problem for facilitators is how to make the integration appear legitimate. Unlike the technical criminal element, they are often in the same country as the money mules and the victim, this makes them more exposed and vulnerable if LE investigates the offence (Leukfeldt and Jansen, 2015, p. 182). The researcher could find no literature on this part of the process but believes it would be a valuable area of further study. This is based on the belief that it could develop a crime script further providing more intervention points for LE. Unfortunately, it is beyond the scope of this piece.

For those involved in the technical and management elements of the crime, the integration process is potentially different again. It has been identified that countries such as Nigeria are hotspots for MF offences (Interpol, 2018, p. 3). Offenders based in these countries are potential beneficiaries of very particular circumstances. If the proceeds of the crime successfully reach these countries those receiving them can take advantage of issues of corruption and weak anti-money laundering efforts (Ebenezer et al., 2016, p. 158; Lartley, 2016, p. 4). This allows the integration of the proceeds into a wide range of possibilities including investments in property, businesses, importation of goods and political donations (Lartley, 2016, p. 4; Ebenezer et al., 2016, p. 158) (Figure 1).

**Intervention**

The script outlined provides corroboration for the assertion that digital fraud offences are largely committed by “financially motivated, organised global criminal enterprises” (Bryant, 2008, p. 87; McGuire, 2018). To counter this, it could be argued that LE also needs to be organised and systematic so intervention points can be exploited effectively. Unfortunately, the literature highlights that it is not even clear in the current environment who is responsible for investigating offences such as MF (Police Foundation, 2018, p. 6). To exploit the intervention points generated from the script it could be that LE first needs to clearly outline a structure and strategy to deal with the offence. For example, MFs cover all three of the offences outlined in the introduction, as such it could be argued that those investigating it need a skill set based on both digital and financial investigation. This would mean that one set of investigators could be tasked with being responsible for the issue. Recent research does corroborate the potential benefits of this approach (McGuire, 2018).

Efficiently targeting resources to achieve maximum effect also needs consideration. It is acknowledged that the international nature of much digital fraud causes jurisdictional challenges (Interpol, 2018, p. 14). One interpretation of this could be that resources are best focused on the intervention points, which exist in the UK. The issue here is that offenders move the proceeds of crime rapidly though the UK financial sector. Unfortunately, the current intelligence systems are not capable of dealing with this. Research has identified that the number of Suspicious Activity Reports (SARs) made by the financial sector are potentially overwhelming UK LE (Europol, 2017a, 2017b). As such how to counter this would also need to be considered.

The topic of effectively organising and applying a strategy to LEs approach is too broad for the scope of this study. As such the points prior to this just touch upon the subject to highlight the matter. It is worth noting that there is an argument that should LE get a clear strategy outlined, the legislation is in place to support their efforts. POCA, in particular, is a particularly powerful piece of legislation. As an example, the money laundering offences outlined (Sec, 327, 328, 329 POCA 2002) do not require the FA or CMA offences to be proven.
As long as an irresistible inference to crime can be drawn a money laundering charge can be sought (POCA, 2002).

Directly from the script one possible point of intervention could be identifying facilitators. As outlined if the money mules are based in the UK then these facilitators are also often based in the UK (Leukfeldt and Jansen, 2015, p. 182). Literature identifies that they reintegrate their proceeds from the criminality in particular ways (Interpol, 2018, p. 8; McGuire, 2018, p. 21). Using this information to inform intelligence research could lead to proactive financial investigation. For example, LE could use open source research on social media to identify individuals showing off luxury items. Proactive financial investigation could then be used to corroborate if this was appropriate and if any suspicions of money laundering are present. This could then lead to mapping out the profiles and connections of these individuals allowing for LE action to be taken if necessary.

**Conclusion**

The research carried out allows for the contention that crime scripts could assist in standardising digital investigation. They have been used in other areas of criminality (Light et al., 1993; Leddo and Abelson, 1986) and as with RAT it can be argued that they are just as applicable to digital crime (Grabosky, 2001, p. 248). The issue is whether LE are currently

---

**Figure 1. Crime script for MF**

<table>
<thead>
<tr>
<th>1. Preparation</th>
<th>2. Target Selection</th>
<th>3. Compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td>- What are the right forums to recruit the necessary personnel?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What local, national and international network is required to facilitate the offence?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What communication system is in place to co-ordinate all of the component parts of the fraud?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What hardware and software are required to carry out the offence?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What information needs to be gathered to identify potential targets?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What technical compromises are currently available and possible?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Once a target is selected what information specific to them needs to be obtained?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What information needs to be disseminated to the network to ensure the necessary infrastructure is in place?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What form of compromise is being utilised?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What security measures are in place?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- How will access be maintained if the compromise is successful?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- From the information analysed in the victims inbox what opportunities for fraud exist?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. Engage</th>
<th>5. Launder</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Having established the fraud opportunity what is the most opportune time to engage the victim?</td>
<td></td>
</tr>
<tr>
<td>□ Is it necessary to include an invoice when engaging the secondary victim?</td>
<td></td>
</tr>
<tr>
<td>□ Which mules bank account information will be utilised?</td>
<td></td>
</tr>
<tr>
<td>□ Who within the network of facilitators is being updated to manage the laundering process?</td>
<td></td>
</tr>
<tr>
<td>- What is the placement strategy? for example how many mules are involved? who is controlling the mules?</td>
<td></td>
</tr>
<tr>
<td>- How is complexity being added into the process (the layering stage) to disguise the audit trail, ownership and source of funds?</td>
<td></td>
</tr>
<tr>
<td>- How is money being moved overseas?</td>
<td></td>
</tr>
<tr>
<td>- What is the integration strategy? 3 aspects to this; money mules, facilitators and overseas offenders.</td>
<td></td>
</tr>
</tbody>
</table>
capable of using scripts appropriately. With research suggesting that LE are struggling to respond with a clear strategy and structure (Police Foundation, 2018), one potential is that they would not be capable of identifying and exploiting intervention points. Therefore, prior to spending time working through crime scripts, it could be beneficial for LE to concentrate on clearly identifying how they are going to respond to the digital fraud issue.

With clear leadership and direction LE could standardise investigation through a targeted approach based on a detailed knowledge of fraud (Dehghanniri and Borrion, 2016, p. 1). This could stimulate thinking on the operational structures and skill sets required to tackle such criminality. In particular, the effective use of existing legislation could boost LEs capability to be a more capable guardian. Using crime scripts to inform preventative interventions could reduce the opportunities to launder the proceeds of crime. Targeting elements of the criminal networks who reside in the UK could result in fewer facilitators and money mules being available. This would make the decisions at the laundering stage more challenging for the offenders. In making it more difficult to access the proceeds of any crime committed, the financial motivation of offenders could be undermined positively impacting the RAT elements. This would potentially reduce the number of offences committed.

Finally, overhauling the existing SAR regime to allow for LE to effectively engage with the financial sector could have several benefits. In allowing intelligence to flow more freely and rapidly between each entity LEs current capability to identify offenders, recognise the vulnerability and efficiently deploy resources could be augmented. It would also allow for crime prevention messages to be relevant and up to date (Police Foundation, 2018, p. 64). This would improve the knowledge of potential victims elevating their position as a capable guardian.

References
Action Fraud (2018), What is Action Fraud, available at: www.actionfraud.police.uk/what-is-action-fraud


National Anti-Fraud Network (2018), “Bank mandate fraud: business or public, we are all at risk of bank mandate fraud”, [PDF] Available at: https://nbcc.police.uk/article/?id=3d82e3f2e28b76f7b473db348dae60e4


Further reading


Birmingham City University (BCU) (2011), How to write references [PDF], BCU, Birmingham, available at: http://library.bcu.ac.uk/references.pdf


Corresponding author

Michael Donegan can be contacted at: peanutbtc@protonmail.com