

To: COMMUNITIES, HOUSING & PLANNING POLICY BOARD

On: 30 OCTOBER 2018

Report by: DIRECTOR OF COMMUNITIES, HOUSING & PLANNING SERVICES

**Heading: COUNTER TERRORISM AND FRAUDS & SCAMS WITHIN
RENFREWSHIRE**

1. SUMMARY

- 1.1. Renfrewshire Council has a duty under the Counter Terrorism and Security Act, 2015, to have due regard to the need to prevent people from being drawn into terrorism and to work with partners to be vigilant and work together to identify signs where someone may be in danger of becoming radicalised or involved in terrorist activities. This is known as the Prevent Duty.
 - 1.2. During 2017 5 attacks took place in the UK and the nature of the threat from terrorism and our understanding of how to address this has changed. Updated guidance was published earlier in 2018 that puts safeguarding at the heart of the prevent agenda and this paper highlights the work undertaken in Renfrewshire in conjunction with Police Scotland to form a divisional Multi-Agency CONTEST and Serious Organised Crime Group for Renfrewshire/Inverclyde to highlight and tackle key issues of vulnerability and to co-ordinate work across the public sector to tackle terrorism and serious organised crime. This group is an important part of the governance framework to oversee these issues.
 - 1.3. While vulnerable people can be targeted by serious organised crime groups to become involved in criminal activities they may also become the victim of frauds and scams. This paper also highlights what Renfrewshire Council and partners are doing to prevent vulnerable residents from becoming victims of these crimes and some of the wider implications of these types of activity.
-

2. RECOMMENDATIONS

- 2.1 It is recommended that the Communities, Housing & Planning Policy Board:
- (i) notes the implementation of a Divisional Multi-Agency CONTEST and Serious Organised Crime Group for Renfrewshire/Inverclyde;
 - (ii) notes the new CONTEST strategy 2018; and
 - (iii) notes the update on frauds and scams within Renfrewshire.
-

3. BACKGROUND

CONTEST 2018

- 3.1 An updated version of the CONTEST strategy was published by the Home Office in June 2018. This new document replaces the previous UK CONTEST strategy and updates the Prevent Strategy, both published in 2011 and updated in 2015. Scottish guidance on Prevent is now being updated in line with the CONTEST 2018 strategy.
- 3.2 The response to counter-terrorism is built around the objective of leaving no safe space for terrorists to recruit or act. The CONTEST strategy, is the framework that enables the public sector to organise the work required to counter all forms of terrorism. The overarching aim remains to reduce the risk posed by terrorism to the UK and its citizens, including interests overseas, so that citizens can go about their lives freely and with confidence. Last year's attacks in London and Manchester served as a stark reminder of the continued threat that terrorism poses, both to our people and to our way of life.
- 3.3 For all of the successes of the original strategy, in the years since it was implemented the threat from terrorism has not stood still. The war in Syria, which was in its infancy when the last Strategy was published, has created both a haven and a training ground for British and foreign terrorists.
- 3.4 Across the UK since 2013, counter terrorism arrests have doubled with over 500 charged and over 400 convicted. Since 2017, 12 Islamist and 4 extreme right-wing plots have been foiled. As of 2018 there are over 500 live investigations, 3,000 subjects of interest and over 20,000 individuals in post-investigation stage. An emerging threat is the development of radicalism in communities that seeks to detract against the state and the counter terrorism response to build structures that widen the divide between communities and the state.

- 3.5 In considering the current position, the Director General of the Office of Security and Counter Terrorism (Tom Hurd) views that the nature of attacks has changed, with a shift in the nature of the threat rather than a spike in overall threat and a much faster move from conception to execution of attacks and a trend towards low sophistication attacks. Vehicles are increasingly used as weapons with which to kill and maim innocent people and there is an increasing role for the internet, making the cyber resilience and cybercrime agenda much more closely linked to the counter terrorist agenda. This has implications for how counter terrorism activities can be policed and particularly for the role played by the wider public sector.
- 3.6 In the wake of the attacks in London and Manchester the Prime Minister pledged to undertake a comprehensive review of the approach to counter terrorism to ensure it was working as effectively as possible. This delayed the planned refresh of the CONTEST strategy for a period and the new Strategy is the result of that review. The CONTEST 2018 strategy builds on progress made since 2011 and has evolved to reflect the changing situation around the world and learns lessons from the tragic attacks in the UK and elsewhere.
- 3.7 Because the threat is large and multi-faceted, and it is considered that we are facing at least 2 years of heightened threat, there is a greater focus in the refreshed Strategy on the known threat and expanding interventions to rehabilitate and disengage those engaged in terrorism. There will be a focus – particularly in metropolitan highest threat areas in England and Wales, in piloting new multi-agency approaches to early intervention, developing a desistance and disengagement programme and in working in prisons with conflict zone returners, half of whom will be coming out of prison over the next 4 years.
- 3.8 The 2018 strategy continues to focus on developing increased co-ordination across the public sector to support more local interventions that will share information and data with a broader set of partners, seeking a more integrated approach with the private sector to protect our economic infrastructure. By linking up not just the intelligence agencies but also local authorities, health providers and many others, it will make it harder for terrorists and those who support them to plan and carry out attacks. There will also be a concerted effort to make the internet a hostile environment for terrorist activities through work with communities, service providers and the technology industry. Facebook now remove 99% of Daesh and Al-Qaeda content using automated systems – 83% within the first hour of it being posted. During 2017/18 the counter extremism, Research Information and Communications Unit, RICU produced over 4,000 products to counter terrorism online with more engagement than in the previous 3 years combined.

- 3.9 While the threat from Islamic terrorism is still foremost in most people's minds the strategy reflects the growing threat from extreme right-wing terrorism and also acknowledges that left wing terrorism is a developing threat. Northern Ireland related terrorism also remains a threat. In December 2016, the then Home Secretary proscribed the first extreme right-wing group, National Action, under the Terrorism Act 2000. The Government took further action in September 2017, proscribing Scottish Dawn and National Socialist Anti-Capitalist Action as aliases of National Action. For the Director General of the Office of Security and Counter Terrorism non-proscribed groups are an issue of concern. In his view, while we know what to do about groups or individuals of concern and are getting better at supporting groups that want to strengthen our society and approach there is a need to focus more on those that are seeking to create structures that target those that are vulnerable and radicalise them.
- 3.10 Last year's attacks in London and Manchester highlighted both the challenge of detecting individuals who may be inspired to commit terrorist acts in the UK, and the pace at which individuals or small groups can move to commit acts of violence. This places a renewed importance on developing our understanding of those individuals who are vulnerable to radicalisation or who are (or have been) of interest to the police and the security and intelligence agencies due to their possible links to terrorist-related activities, but who are not currently the subject of any active investigations. This information will be shared more widely and will support local interventions with individuals in our own communities who are potentially vulnerable to being groomed or incited to commit or support acts of terrorism.
- 3.11 It is important to note that there is no single profile for a person that might be vulnerable to becoming involved in terrorism. While the majority are male, there are female terrorists. While some live alone or are relatively isolated, some are involved in steady relationships - and the group is ethnically diverse. The majority are British citizens and half are UK born. A range of education and career levels have been attained. Few have a deep knowledge or understanding of faith – but there is a disproportionately high level of converts to religious belief. While mental health issues or autism or aspergers can be present and have been noted in some terrorists, there is absolutely no causality link with these that can be made.
- 3.12 For individuals to become susceptible requires a level of background vulnerability, together with an ideological opening that makes them question their beliefs and a number of initial influences that come together in the absence of protective factors and/or obstacles that would otherwise mitigate or reduce their susceptibility.

- 3.13 The updated and strengthened CONTEST 2018 strategy reflects the challenges of operating in this environment and the findings of a fundamental review of all aspects of counter-terrorism, to ensure the best response to the current position and heightened threat in coming years. Overall however, the review found CONTEST to be well-organised and comprehensive and seeks to update and build on a successful approach rather than develop an entirely new strategy. As a result the tried and tested and well understood strategic framework of four 'P' work strands has been retained:

- Prevent: to stop people becoming terrorists or supporting terrorism.
- Pursue: to stop terrorist attacks.
- Protect: to strengthen our protection against a terrorist attack.
- Prepare: to mitigate the impact of a terrorist attack.

Divisional Multi-Agency CONTEST and Serious Organised Crime Group

- 3.14 On a wider level, research and analysis has highlighted that groups and individuals that engage in or are vulnerable to becoming involved in terrorist activities are also vulnerable to becoming involved in serious organised crime. In addition, serious organised crime groups and terrorist organisations operate across a wider geography than simply Renfrewshire and are best understood locally at a Police Divisional level covering both Renfrewshire and Inverclyde Council areas.
- 3.15 The agreed response to this has been to replace the current Renfrewshire CONTEST/Prevent group with a strategic CONTEST and Serious Organised Crime Multi Agency Group operating at a Police Divisional level. This group will still require to be supported by a Renfrewshire Council Prevent / Divert Group and potentially a number of tactical and operational sub groups with a focus on serious organised crime.
- 3.16 Establishing a strategic meeting that has the responsibility and a role to consider both CONTEST and Serious Organised Crime issues is a positive step. There is significant academic and operational evidence to support that terrorism and serious organised crime are linked – even if only in relation to the groups and individuals that they seek to prey on. There is also evidence that serious organised crime groups are sometimes more directly involved in fundraising or other support for those with terrorist sympathies.
- 3.17 Progress has now been made, with agreement across key partners on the key purpose of the new group and its way of operating. This is attached in Appendix 1 to this report. A key priority for the group will be the development and use of Emerging and Residual Threat Profiles for both terrorism and serious organised crime to assist in understanding the nature of risk in the divisional area, and in prioritising the areas of focus and nature of response for the partners involved in the group.

- 3.18 The proposed group will also have a particular focus on addressing the key indicators and issues that make people vulnerable to becoming involved with serious organised crime or terrorist groups or that might indicate that they are already becoming involved in activities that are of concern. The group is chaired by the Head of Communities and Public Protection and the first meeting of the group was held on 4 September 2018. At this meeting the approach and principles outlined in Appendix 1 were agreed and a focus on a number of key challenges was also agreed. These included Drugs; Human Trafficking; Missing Persons; Cyber and Social Media; Sexual Exploitation and Brexit. In order that swift progress on the development of a risk and threat profile can be made it was also agreed that the next meeting should be held in November 2018.
- 3.19 Alongside the Counter Terrorism / Serious Organised Crime Divisional Group a specific Serious Organised Crime Group will also be established and is referred to in Appendix 1. This will be chaired by the Detective Superintendent with responsibility for Serious Organised Crime across the division and will be responsible for strategic oversight of this agenda and tactical governance. It is proposed by the Divisional Commander for Renfrewshire that regular reports on Serious Organised Crime be brought to the Community Protection Chief Officer Group by the Detective Superintendent.
- 3.20 The information and strategic understanding of the nature of the risk to Renfrewshire that will be developed by the Divisional CONTEST and Serious Organised Crime Multi Agency Group will also be used to guide the work of the local Renfrewshire Multi Agency Prevent Group, will inform the focus and agenda of the Renfrewshire Community Protection Steering Group and the Renfrewshire Council Integrity Group.
- 3.21 These new multi-agency approaches will support Police Scotland in sharing relevant information with partners and allow the partnership to establish robust and effective referral and review pathways. The revised strategy's increased focus on safeguarding those at risk of radicalisation and rehabilitating those that have previously been identified as being vulnerable or having committed relevant offences is also welcome as it reflects to a significant extent the position that has been developed successfully in Scotland over a number of years in relation to Prevent.

4 Frauds and Scams

- 4.1 Anyone can become a victim of a scam or fraud. However, some people are traditionally more vulnerable to becoming a victim. This vulnerability could be a result of a range of factors including age, capacity, loneliness and uncertainty in the use of technology.

- 4.2 Fraudsters target the elderly and the vulnerable and prey on their insecurities. This can be done by visits, letter or increasingly by e-mail/computer or social media. Sometimes the person being defrauded may feel they are helping someone whilst there have been other cases of people simply wanting social interaction and therefore knowingly being scammed.
- 4.3 As well as Police Scotland with an obvious role to play in tackling fraud, Trading Standards Officers tackle both local and national issues and are often the first port of call for advice and support in relation to what can appear initially to be solely a “civil” issue e.g. a dispute between a trader and a consumer, over goods or a service. Upon discussion however, it can become evident that the consumer may have fallen victim to a scam or fraud and may require help and support to prevent recurrence in the future.
- 4.4 The nature, scale and threat posed by frauds and scams is also changing. Frauds and scams are becoming increasingly sophisticated and can be difficult to spot. Perpetrators are often based outside the UK and can use modern technology to contact vulnerable people and organisations. They can be difficult to trace. There is also a trend of using some of the approaches and techniques developed to target individuals and organisations to defraud them of money, to target large businesses and governmental organisations in a form of online terrorism – sometimes even in the form of state sponsored attacks. In these cases the object is not always to defraud, but can be to destabilise or undermine. These attacks can be indiscriminate – the victims are not always specifically targeted – they are simply caught up in wider events. The costs of attacks of this nature can be very significant for those impacted – in one recent attack one company had to fund the replacement of all their IT systems worldwide at a cost of \$300M - and the attack was swift – with complete destruction of their IT system happening within 17 minutes after they were breached. During this attack a number of companies were impacted in the same way.
- 4.5 The types of scams and frauds currently impacting on communities in Renfrewshire are very wide ranging - however some of the more common types of fraud that are currently being experienced in Renfrewshire include but are not limited to:
- 4.6 Social Engineering Fraud, where malware and phishing emails are used to obtain customers’ details. Offenders are increasingly using social engineering tools, particularly obtaining information by phone and SMS text message. Police research shows that approximately half of the total loss from fraud could be attributed to crime groups using these techniques.
- 4.7 The primary techniques used include:
- Posing as a bank or security company employee, cold-calling complainers to inform them that their savings are at risk and monies in their account therefore had to be transferred to a 'safe account' (in reality, an account in the control of the perpetrator);

- Posing as a Microsoft employee and calling complainers purportedly in relation to a computer virus, thereafter inducing them to pay a fee for the virus to be removed (or with the complainer's assistance installing a remote access terminal in their PC to obtain financial information)
- Calling complainers and posing as an HMRC employee and thereafter requesting due payment via iTunes vouchers - a technique which Action Fraud identified as having first emerged in the UK in May 2016.
- Hacking complainers accounts, transferring money to their accountant and then telephoning the accountant and convincing them to transfer the money to a different account.

Key Issues

- iTunes vouchers are an increasingly attractive commodity due to the fact that they are easily and instantaneously redeemable, non-physical (the perpetrator merely has to get the victim to read out the serial number over the phone), essentially untraceable and unrecoverable.
- The capability of some fraudsters alleging to be calling from banks and other financial institutions to mask their true telephone number and 'spoof' genuine numbers recognised and trusted by complainers represents a significant threat, as this capability allows them to bypass the concerns of many 'security conscious' victims.
- The sheer scale of attempted phone frauds is evidenced by the fact that one single number associated with 'HMRC' phone frauds has been checked nearly 34,000 times by members of the public on the 'Who-Called' website.

4.8 Online Fraud – includes both failure to supply goods, services or payment following online advertising on sites such as eBay and Gumtree and hacking into eBay, Paypal and online banking accounts to transfer funds. This technique is indicative of a high degree of technical expertise in some cases. Recent threat analyses have highlighted that online fraud is set to become increasingly sophisticated, in order to bypass advancing fraud prevention solutions. This is an area where internet fraudsters are exploiting the growing volume of online personal data and the diversification of internet connected devices, eg 'The Internet of Things' to maximise their chances of successfully perpetrating criminal acts. Meanwhile, the continuing move towards digitalisation of major currencies including sterling is encouraging fraudsters to gravitate towards digital currency and goods.

4.9 Credit/Debit Card Fraud continues to be a threat, with unauthorised use of complainers' bank accounts, personal details or credit cards to purchase items online, Presenting stolen cards at banks while purporting to be the account holder Using stolen cards and PINs to make unauthorised withdrawals from ATMs and more recently using the contactless function of payment cards to purchase goods in person.

- 4.10 Mandate Fraud relates to the act of intercepting emails between businesses who are paying invoices and the perpetrators thereafter sending a similar email requesting a change in bank details for the funds to be paid into. Cybersecurity intelligence assessments suggest that the method for perpetrating mandate frauds is likely to be malware disguised as an email attachment - often a word document containing a malicious macro - which then infects the target computer and allows network traffic (including emails) to be intercepted - providing the information required to develop a customised mandate fraud.
- 4.11 Small businesses and contractors are identified as being particularly vulnerable to this type of fraud as they are used to receiving invoices on a regular basis. Research suggests that small business owners aged 18 - 35 are much more likely to be a victim of this type of attack with more than a third of young business owners stating they have been a victim of mandate/invoice or similar frauds - increasing to 55% for businesses with owners aged under 25. In a similar manner email attachments or other malware can be used to infiltrate computer systems and defraud through the use of Ransomware – software that denies access to information or systems until a payment is made.
- 4.12 Romance Frauds are primarily the result of internet-initiated dating, with perpetrators using dating websites and social media platforms to meet potential victims, develop a relationship with them and then attempt to exploit their trust to request monies (usually transferred electronically). These frauds are arguably one of the most distressing frauds as victims suffer both financially and emotionally. Complainers may be repeatedly victimised by the perpetrator before realising that they have been 'scammed'.
- 4.13 Responding to these risks is an ongoing focus for the work of the Renfrewshire Adult Protection Committee and a specific sub group has been established and a financial harm work plan developed to assist in tackling the issues. This plan sets out the actions and targets for addressing Financial Harm within Renfrewshire, covering the period 2017 – 19. It outlines the local multi-agency plans of Police Scotland, Trading Standards (Renfrewshire), Renfrewshire Adult Protection Committee, Renfrewshire Health and Social Care Partnership, and local partners, based on the resources available.
- 4.14 On 22nd March 2018, a Financial Harm Event was held within Paisley Town Hall. This event highlighted the key issues and what could be done to minimise the risk and impact for vulnerable people.
- 4.15 Responding to the use of some of these techniques to perpetrate damage on communities and organisations as well as to defraud will be an area of focus for the Divisional CONTEST and Serious Organised Crime Group as one area of activity where the approach and impact of both crime and terrorist activities is beginning to merge.
-

Implications of the Report

1. **Financial** – None
2. **HR & Organisational Development** – None
3. **Community Planning** –

Renfrewshire is safe – the Renfrewshire Community Safety Partnership continues to work to keep people that live, work and visit Renfrewshire safe. The Divisional Multi-Agency CONTEST and Serious Organised Crime Group will assist in this process.

By monitoring and actioning frauds and scams, Renfrewshire Council will ensure vulnerable people do not fall victim to frauds and scams.

4. **Legal** - None
5. **Property/Assets** - None
6. **Information Technology** - None
7. **Equality & Human Rights**
8. **Health & Safety** – None
9. **Procurement** – None
10. **Risk** – None
11. **Privacy Impact** – None
12. **Cosla Policy Position** – None

List of Background Papers

None

Author: Oliver Reid, Head of Communities & Public Protection

Renfrewshire and Inverclyde Divisional Multi Agency CONTEST / Serious Organised Crime Group

The purpose of the Renfrewshire and Inverclyde Divisional Multi Agency CONTEST / Serious Organised Crime Group will be to identify priorities and opportunities for jointly tackling terrorism and organised crime across the communities of Renfrewshire and Inverclyde so that residents and businesses can go about their lives freely, safely and with confidence.

The Group will achieve this by:

- **Understanding the nature of the risk and threat posed by Serious Organised Crime and Terrorism in Renfrewshire and Inverclyde**

We will do this by –

- *Improving information sharing to enrich our understanding of the risk and threat posed by serious organised crime and terrorism at the local level*
 - *Preparing and maintaining a risks and threats assessment for terrorism and for serious organised crime to guide the priorities and response of all agencies*
 - *Sharing this assessment as relevant with neighbouring areas to ensure that relevant cross border issues and focus are understood and addressed*
- **Ensuring appropriate preventative action is being taken to protect Renfrewshire and Inverclyde communities from the threats faced by terrorism and serious organised crime groups**

We will do this by –

- *Intervening early - to safeguard and support those at most risk of radicalisation or becoming involved in organised crime and to identify business practices and models of operation that indicate potential organised criminal activity*
- *Avoiding duplication of effort. The group will look to existing fora such as the Local Resilience Partnership (LRP) and the newly established Divisional Serious Organised Crime Group for elements of supportive strategic and tactical activity, and act as a strategic oversight body, only identifying and engaging subgroups as and when required or if necessary.*
- *Working across agencies and with communities to identify those vulnerable to becoming involved in serious organised crime or terrorism and developing appropriate interventions that reduce these risks*
- *Taking robust action to ensure that there are no safe places for terrorists or serious organised crime groups online or in our communities and that strong counter – terrorist or organised crime narratives are developed and disseminated through our communities that empower communities and individuals*

- *Identifying and targeting groups or individuals that are seeking to groom or incite individuals in our communities to commit or support serious organised crime or terrorism.*
- *Reinforcing safeguarding activities to ensure that communities and families are not exploited by serious organised crime or terrorism*
- **Identifying and encouraging innovative ways of working together to interdict Serious and Organised crime or Terrorism in Renfrewshire and Inverclyde**

We will do this by –

- *Obtaining and sharing intelligence on those individuals/groups involved in Serious Organised Crime and/or Terrorism.*
- *Using creative intervention tactics to deprive and prevent Organised Crime Groups from accessing or subverting legitimate business*
- *Working collaboratively to identify ways of protecting public, private and third sector organisations working in Renfrewshire and Inverclyde from being targeted by serious organised crime groups or terrorists.*
- *Working collaboratively to identify ways to support and promote legitimate businesses and encourage them to succeed*
- *Targeting the insider threat by strengthening information sharing about those working in sensitive environments across all agencies to ensure that persons of concern do not have access to restricted environments, data or information that would benefit organised crime or terrorist activities*
- *Improving security at crowded places through closer more effective working across all agencies*
- *Working online and offline to empower communities and individuals and tackle the causes of radicalisation and serious organised criminal activity*
- *Intervening early using safeguarding principles to provide tailored multi-agency support to those identified as most at risk of radicalisation or involvement in serious organised crime.*
- *Providing support to those already engaged in serious organised crime or terrorism to disengage and rehabilitate*
- **Sharing best practice and improving coordination of multi-agency partners at a local and national level**

We will do this by –

- *Working together to target those persons responsible for the creation, storage and distribution of counterfeit and illicit goods.*
- *Considering how individual public agencies and Council services can take co-ordinated action to make a significant difference and contribution to this agenda e.g. Planning Permissions, Environmental Services, Licencing, Trading Standards*
- *Working together to identify, disrupt and record any businesses or individuals involved in the sale of New Psychoactive Substances (NPS) / Adulterants.*
- *Sharing information to achieve common goals*

- *Working with industry and partners to improve security at venues, gain faster alerts to suspicious purchases and design out vulnerabilities to infrastructure or in products or contracts that organised crime groups or terrorists can exploit*
 - *Exploitation of regulatory powers - where possible, to treat these groups with extreme prejudice (recognising processes and procedures often need to be followed).*
 - *Removing organised crime groups from acting as landlords and making substantial profits due to sharing of information.*
 - *Contributing to work at a national level to co-ordinate the response of all agencies to ensure that opportunities are minimised in Renfrewshire and Inverclyde for organised crime or terrorism groups*
 - *Developing appropriate local performance and monitoring data and contributing to developing and building a clear picture of progress at a national level*
- **Mitigating the impact of a terrorist attack and organised crime activity within Renfrewshire and Inverclyde**

We will do this by –

- *Encouraging the public to report any suspicious activity*
 - *Diverting vulnerable members of the community away from organised crime or terrorist activities*
 - *Increasing the number of persons arrested who are associated with Organised Crime Groups (SOCG) and/or Terrorism*
 - *Utilising the Proceeds of Crime Act 2002 to deprive criminals of financial wealth.*
 - *Ensuring appropriate joined up multi agency support to residents affected by serious organised crime or terrorism.*
 - *Regularly testing and exercising the local multi agency capabilities required to respond to and recover from terrorist or serious criminal attacks e.g. cyber resilience*
- **Addressing where there are risks of radicalisation or pathways towards Serious and Organised crime activity**

We will do this by –

- *Maintaining established links to the Grey Space Group as an invaluable source of intelligence around community vulnerabilities and concerns and as an informal tasking partner.*
- *Building on the existing learned and developed understanding of Counter Terrorism across Renfrewshire and Inverclyde, where partners have worked closely together.*
- *Obtaining and sharing intelligence on those individuals/groups involved in Serious Organised Crime and/or Terrorism.*
- *Raising and increasing training and awareness amongst the public, voluntary and private sector workforce on issues of concern and how to report concerns*