Witness Name: Timothy Wright

Exhibits: None

Dated: 24th July 2026

THE SOUTHPORT INQUIRY

FIRST WITNESS STATEMENT OF TIMOTHY WRIGHT

This witness statement contains information which may be considered sensitive or triggering to some individuals

1. I, Timothy Wright, am an officer of the National Crime Agency ('NCA'), Floors 12-14, 12 Endeavour Square, Westfield Avenue, Stratford, London, E20 1JN.

2. I am the Temporary Deputy Director for Child Sexual Abuse and Modern Slavery and Human Trafficking in the Threat Leadership Command within the NCA. I have held this role since April 2026 and my remit involves leading the UK operational response to combat Child Sexual Abuse ('CSA') and Modern Slavery and Human Trafficking ('MSHT').

3. I joined the NCA in March 2014 and I have spent the last 5 years working to tackle CSA and, latterly, MSHT. Prior to joining the NCA, I had been a civil servant for nearly 20 years, working in the Serious Organised Crime Agency (the precursor Agency to the NCA), the Home Office, His Majesty's Prison Service and Crown Prosecution Service, specialising in serious and online crime.

4. I am authorised to make this witness statement on behalf of the NCA following a request for evidence from the Southport Inquiry dated 25th June 2026 pursuant to Rule 9 of the Inquiry Rules 2006 ('the Rule 9 request'). I have prepared this statement with the assistance of solicitors and counsel and, in doing so I have discussed the facts with relevant colleagues within the NCA. In so far as the contents of this statement are within my own personal knowledge they are true, otherwise they are true to the best of my knowledge, information and belief.

The Role of the NCA

5. The NCA's mission is to protect the public from serious and organised crime ('SOC').

6. The NCA has two main functions set out in the Crime and Courts Act 2013:
   - Crime-reduction function: to ensure that efficient and effective activities to combat organised crime and serious crime are carried out (whether by the NCA, other law enforcement agencies, or other persons); and
   - Criminal intelligence function: to gather, store, process, analyse and disseminate information relevant to, among other things, activities to combat organised crime or serious crime and activities to combat any other kind of crime.

7. The Home Secretary determines the NCA's Strategic Priorities, while the Director General sets the Operational Priorities and decides which operations are mounted by NCA officers and how those operations are conducted. The NCA is therefore operationally independent.

8. The NCA has officers based in England, Wales, Scotland and Northern Ireland. We also have global reach, with liaison officers based in more than 50 countries worldwide. We work closely with policing partners, the intelligence agencies, regulatory authorities and other operational agencies - including in Scotland and Northern Ireland - to lead and coordinate a comprehensive response to SOC in the UK and overseas.

9. The NCA is responsible for:
   - Maintaining the single national intelligence picture of the SOC threat facing the UK, as set out in the Agency's annual National Strategic Assessment;
   - Collecting and exploiting data and intelligence to detect and disrupt SOC, pursuing the most serious and dangerous offenders;
   - Investigating and taking action against the highest-harm offenders and their enablers, including through criminal justice outcomes, civil recovery and tax proceedings;
   - Setting operational priorities for the SOC system (including roles and responsibilities for a cross-system threat response), providing a prioritised view of demand on the system, and measuring and assessing Agency and national system performance against those priorities; and
   - Hosting and providing partners with access to national and specialist capabilities, including support to serious and major crime investigations across policing.

10. The main categories of SOC, which reflect successive Home Secretaries' Strategic Priorities, are: child sexual abuse, illegal drugs, illegal firearms, fraud, money laundering and other economic crime, bribery and other forms of corruption, organised immigration crime, modern slavery and human trafficking and cybercrime.

11. Any referral received by the NCA containing a credible threat of real world violence identified in an online space is triaged to Counter Terrorism Policing (CTP) or the applicable territorial police force (see paras 13-15 and 48 below).

Phase Two of the Southport Inquiry

12. As set out in the Terms of Reference ('ToR') for Phase Two of the Southport Inquiry, the focus appears to be on examining the adequacy of arrangements in England and Wales for identifying, assessing and managing the risk posed by individuals at risk of extreme violence where ideology is not the Primary driver ('Violence Fixated Individuals'[1], or 'VFIs') and for disrupting the circumstances in which such violence may be enabled. The NCA attended the Opening Hearing for Phase Two held on 8th July 2026, and this strong focus on VFIs was apparent throughout the opening statements of the Chair of the Inquiry, Sir Adrian Fulford, and Counsel to the Inquiry, Mr Nicholas Moss KC.

13. As set out above the NCA, in accordance with its strategic and operational priorities, does not play a role in identifying, assessing or managing the risks posed by VFIs[2], but has a role in triaging cases which pose a risk of real-world violence to the appropriate agency. The NCA focusses on identifying and tackling the wider harms and complex risks in the online environment posed by 'Com Networks' (see paragraphs 17-23 below).

14. However, Topic Two of the ToR states that the Inquiry will be looking at the role of the internet and social media in influencing and enabling VFIs to prepare and carry out violent attacks. The internet and social media are also the environment in which Com groups

[1] I am aware that there is no fixed definition of a VFI, the NCA uses the Home Office's descriptor and definition applied to this cohort.
[2] The NCA Major Crimes Investigative Support Team and the Serious Crime Analysis Section may, if requested, provide **post arrest** support to police forces investigating major crimes, including those perpetrated by VFIs. Support may include post-arrest risk assessments and Clinical Forensic Psychologists advising on search and interview strategies and/or Behavioural Investigative Advisors advising on offenders from a behavioural science perspective. I have not included further information on this work in this statement on the basis that the NCA has provided evidence in response to separate Rule 9 requests from the Inquiry regarding the Case Studies and I am aware that the Inquiry will be hearing expert evidence during the Case Studies, including from psychiatrists and psychologists on VFIs.

operate and I believe that the underlying drivers and motivations of both VFIs and Com group members appear to be similar. I believe that the NCA's work on this online environment, and its work disrupting Com groups, may be relevant to the Inquiry's ToR and this statement sets out a high-level outline of the NCA's work in this area.

15. The NCA's operational response to identify and combat the threat posed by Com networks is via Project Rhyobasalt; a project jointly set up and delivered with Counter Terrorism Policing ('CTP'). I have set out an overview of the threat in the online environment and of Project Rhyobasalt below, including how the project fits with wider government initiatives to combat online harms, its operational activity and the nexus with VFIs.

16. I am also aware that when approaching Topic Three, the Inquiry will look at the current legal landscape, including existing court orders, for disrupting the activities of VFIs. Serious Crime Prevention Orders ('SCPOs') were referred to at the Opening Hearing and I have set out below how the NCA uses SCPOs (although not in respect of VFIs), along with the NCA's work with the Home Office on developing Cyber Crime Risk Orders ('CCROs') which I believe may also be of interest to the Inquiry.

The Online Environment: COM Networks

17. In 2024, the NCA and partners became increasingly aware of groups, predominantly consisting of teenage boys, sharing extreme materials (such as child sexual abuse material ('CSAM'), extreme right-wing terrorist material ('ERWT'), occult and misogynistic material, racist ideologies, animal cruelty, as well as cyber threats such as ransomware and malware) on online forums to cause users harm and distress. These groups were inciting their victims, mainly young teenage girls, to commit horrendous acts, including sexual and degrading acts, cutting and carving letters and symbols into their bodies, abusing/killing family pets, sexually abusing their siblings or other children, and in some cases coercing their victims to commit suicide.

18. Due to the complex nature of the offending, frequently involving multiple types of criminality (for example sexual offences, cyber and violence) being carried out simultaneously, it was proving difficult to identify where the appropriate law enforcement response should sit.

19. These groups came to be known as Com (short for 'community') Networks, with the online environment in which they operate known as 'the Com'. The NCA defines the Com as the

collective online subculture of Transnational Virtual Networks ('TVN') consisting of criminal actors who engage in a variety of illegal acts in furtherance of their own personal gain, development of their infamy, or in furtherance of their extreme harmful views and behaviours.

20. The NCA assesses Com Networks as a significant form of non-ideological extremism. These online communities promote and facilitate extreme behaviours, including violence, on a variety of forums, including mainstream online platforms. These communities do not demonstrate cohesion and their activities are not in furtherance of any ideological element, which distinguishes Com Networks from traditional extremism.

21. The NCA has categorised Com networks into three subgroups focusing on the dominant type of offending behavior and harm:

    a. Sextortion Com Networks

    Categorised as groups operating online, primarily involved in extorting minors to commit digital and real-world sex crimes; criminal acts against the person, property and/or animals; and the coerced promotion of self-harm and suicide.

    This includes the grooming and extortion of young people (often, but not exclusively females) into sharing indecent or degrading images of themselves. These images are then used for further manipulation and coercion. Coerced acts may include self-harm, cutting symbols and initials into their bodies and suicide attempts, the ingestion of toxic/harmful materials, or burning themselves. In some cases, victims have been coerced to involve and/or harm other family members or pets.

    Victims are groomed and coerced into recording or livestreaming these acts, which are then shared within networks to increase the status and notoriety of the perpetrator. These groups adopt grooming and extortion methodologies traditionally employed by adult child sexual abuse offenders. A competitive element can also arise, where offenders seek to 'dox' (publicly expose) or revictimize victims of other offenders.

    The victim may not appreciate the seriousness of their involvement or impact on their physical and mental health, or their families. The injuries sustained as a result of this offending have resulted in hospitalisation, serious injury, and death.

    b. Cyber Com Networks

    Categorised as groups who have a common purpose to conduct criminal activities that maliciously use digital technologies that target commerce or infrastructure aiming to

cause severe disruption and harm. They do so using malware, ransomware, network intrusion and other specialist malicious tools for cybercrime purposes. While there are many overlaps in techniques used by Cyber Com Networks and other cybercriminals, a hallmark of Cyber Com Networks activity is social engineering, whereby helpdesks are fooled into assisting offenders to take over target accounts.

c. Offline Com Networks

Categorised as groups acting online who hold extremist mind-sets and who promote a real-world violence and a nihilistic world-view. They encourage damage to property, harm to individuals and potentially acts of terrorism. This offending may be opportunistic and occur offline. Such violence includes: graffiti, arson, assault, and murder. Violence can be indiscriminate or may be targeted towards those perceived to be weak or inferior.

22. A Com Network may be involved in multiple crime types, for example a group may be engaging in real world violence, the deployment of ransomware and child sexual abuse activity at the same time. Com group membership is fluid; individuals appear to move from network to network in order to gain greater credibility and notoriety.

23. In addition to sharing extreme material, Com networks may also share terrorist material. Generally, the motivation for sharing terrorist content is not in furtherance of terrorist ideologies, but to share this material because it causes harm. Likewise, CSAM is shared to shock, rather than for sexual gratification.

Pathways to Com Offending and Parallels with VFIs

24. There are numerous pathways into Com offending and a variety of factors converge to result in young people joining Com networks. Factors may include boredom and social isolation, unsupervised time online and thrill seeking. Bullying or rejection by peers can lead to retreat into an online environment, where charismatic personas can be constructed and some young people seek belonging in online communities which validate their identities. This increases their vulnerability to online influence, offending, and group dynamics within Com networks.

25. Com Offenders seek acceptance, kudos and notoriety; displaying extreme beliefs and behaviour online and sharing extreme material in order to do so. They are predominantly,

but not always, males between the ages of 14-17 years old who may be socially rejected and isolated offline, hence displaying a preference for these online interactions.

26. The NCA assesses that many of the characteristics, drivers and underlying factors for engagement in Com networks are similar to those of VFIs, for example Com offenders who are socially isolated in the real world who have a fascination with weaponry. In my opinion, there is an opportunity (for example via the Home Office Non Ideological Extreme Violence Taskforce ('NIEV' – see paragraph 57 below) to tackle the wider online harms threat by developing a whole system early intervention response to these wider threats, which would then have a positive impact on HMG's ability to tackle VFIs. The NCA's position is that the Com reflects a broader pattern of young people being drawn into harmful online spaces, putting them at risk of coercion, exploitation and escalation of harmful behaviours. These young people may be victims, participants or perpetrators across a spectrum of harms.

27. Given the nature of Com group offending, there will be individuals who meet the definition of a VFI but who are not necessarily labelled as such. It is inevitable that such individuals will sometimes fall within Com group investigations without being specifically identified as a VFI.

The Role of the Internet and Online Platforms in Facilitating Com Offending

28. Online platforms play a central role in enabling and shaping Com offending. Com networks operate as international online subcultures that exploit widely used social media, messaging, and gaming platforms to connect offenders, recruit participants, and target victims. Commonly used platforms include Discord, Roblox and Telegram.

29. The digital environment enables both anonymity and visibility. Encrypted platforms, invite-only servers and coded language provide privacy and protection from detection. Social media engagement design incentivises recognition and reward. 'Likes', shares and comments function as validation mechanisms, helping to provide a social framework in which abuse and extremist narratives are normalised, reinforced and escalated.

Formation of Com Networks

30. Online spaces encourage like-minded individuals to identify and connect with each other. This is exploited by Com offenders to create spaces for networking and communications dedicated to the normalisation and incitement of offending and the sharing of knowledge and tradecraft. Discord and Telegram are frequently seen as primary platforms used by Com offenders for operating and communicating. This is likely due to:

    a. The ability for offenders to create private groups and servers on both platforms;

    b. The ease with which they can re-establish groups and servers if the platform has identified illegal or prohibited content and closed the group; and

    c. The perceived security and limited age verification and attribution of user identity which limits the platforms' ability to prevent and detect offending.

Proliferation of Extreme Content

31. Research into the role and level of online content in developing, influencing and reinforcing negative interests and behaviours in young people is ongoing (see paragraph 64 below). However, prosecutions of Com offenders have revealed an interest in gore, violence, sexual abuse, and animal abuse[3]. Content around such themes is easily available and viewed on online platforms.

32. It is highly likely that searches around these topics link users to Com networks on open social media and networking platforms. Generally, algorithms on social media sites target user behaviours; this results in the user being shown more extreme content which increases the likelihood of exposure to Com networks.

33. Members of Com networks have been identified discussing topics such as CSAM and inciting victims to self-harm on open platforms. It is highly likely that the presence of Com

[3] For example, the prosecutions of Cameron Finnigan and Vincent Charlton in 2025 and the prosecution of a 16 year old, who cannot be named for legal reasons, earlier this year.
Child abuse terror warning as 'Satanist' teenager jailed - BBC News
Gateshead Satanist neo-Nazi jailed over terror offences - BBC News

members in open online spaces creates opportunities for engagement with, and recruitment of, new members. Individuals linked to Com networks have been identified on open platforms posting recruitment messages and links to closed forums, where there is then increased exposure to harmful content.

34. The availability of such content on open online platforms can normalise and reduce the perceived severity of these behaviours, de-sensitising those who access it and lowering barriers to encouraging or inciting such offending behaviours.

Connecting Com Offenders with Victims

35. Online platforms have millions of users, providing abundant networking opportunities for offenders to connect with each other and to target and groom victims.

36. This is the predictable outcome of platform design choices, such as mass discoverability, unrestricted contact, algorithmic amplification, unmoderated or encrypted private messaging, ability to livestream and take and share nude pictures, and weak or inconsistent age assurance. It is not restricted to social media; these features and these risks exist, in different combinations and to different extents, on social media, gaming platforms, messaging apps and AI chat bots.

37. Victims are opportunistically targeted by offenders online. Offenders will often seek to identify victims from marginalised groups, or with particular vulnerabilities, such as those suffering from mental health illnesses, including suicidal ideation and eating disorders.

38. Offenders have been found identifying vulnerable online communities, for example female self-harm chat forums, and circulating the forum information amongst their Com network to facilitate other Com group members enticing and engaging with victims. Offenders befriend and send victims invite links to join groups, servers or restricted areas on other platforms, particularly those which encourage private chat or the sharing of imagery.

39. Offenders may also scrape[4] victims' social media profiles for contacts and information to use in extortion or blackmail attempts.

40. Gaming currency[5], such as 'Robux' used on Roblocks, is also being misused by Com networks in furtherance of their offending behaviours; for example, gaming currency is being used as a coercive tool with offenders offering victims gaming currency in return for participating in voice and video calls where coercion, abuse and extortion occur.

Operational Response to COM Networks: Project RHYOBASALT

Project Overview Including Governance Structure

41. To respond to the emerging threat posed by Com Networks, the NCA and Counter-Terrorism Policing ('CTP') jointly built Project Rhyobasalt. The project started in June 2024 as the national response to the Com Network threat. The project seeks to bring together a coherent response across law enforcement, safeguarding partnerships, industry, academia, Non-Governmental Organisations, and international partners, to deliver a public health approach to reduce harm. At a senior governance level, the Online Harms Taskforce (Silver Group), co-chaired by CTP and the NCA, oversees the project and brings together partners across policing and across government.

42. At a working level, Project Rhyobasalt is overseen by the Online Harms Working Group (Bronze Group) consisting of partners from across policing and government, including the NCA, CTP, National Cyber Crime Unit ('NCCU') that sits within the NCA and local force Police Online Investigation Teams ('POLITs')[6].

43. At a tactical level, the Rhyobasalt Intelligence Coordination Cell ('RICC') was established in October 2025, to bring together intelligence functions and capabilities across Cyber, Counter Terrorism ('CT'), CSA and police forces with an objective to safeguard, disrupt, and coordinate the domestic and international response to Com groups. The NCA hosts the RICC and it sits under NCA Threat Leadership Command. The RICC provides a point of entry for law enforcement intelligence (domestic, international and counter-terrorism),

[4] 'Scraping' is an automated process for extracting data from websites.
[5] Gaming currency refers to virtual coins, tokens or points used within video games to purchase items, upgrades or other in-game content. The hook used by offenders to engage victims might be progression within a game, increased functionality within a game (for example weapon upgrades).
[6] Every police force has a POLIT, dedicated to online CSA investigations. A POLIT may also be called an Online CSA Investigation Team or similar.

triaging referrals, developing intelligence packages, identifying and targeting high risk Com group offenders and victims for safeguarding, coordinating investigation teams and delivering training to policing and wider partners.

44. Between October 2025 and June 2026, the RICC has:
    - Received over 1200 referrals, including 252 referrals from international partners;
    - Supported executive action leading to 37 arrests in the UK; and
    - Ensured the safeguarding of 58 vulnerable individuals in the UK and abroad.

45. The RICC is a small team consisting of full-time and part-time officers temporarily deployed from the NCA, CTP and policing. The team was set up at pace, is bedding in and rapidly developing new ways of working to respond to the threat posed by Com networks, which is increasing in terms of scale and complexity.

46. The RICC works with a network of regional policing Com leads to ensure a coherent response that links referrals, including international referrals, with a policing and safeguarding response.

47. The RICC receives referrals on individuals originating from several sources, including the National Center for Missing and Exploited Children ('NCMEC') based in the US[7], other international partners, domestic police referrals, referrals from industry and referrals from members of the public (via 'the NCA's CEOP Safety Centre[8]'). On receipt, referrals are assigned a case officer within the RICC and are triaged.

48. During triage, any referrals with evidence of suspected terrorist activity or radicalisation into a terrorist ideology are sent straight to CTP.

49. The majority of referrals into the RICC are received via NCMEC. NCMEC disseminates reports relating to UK CSA offenders and victims to the Child Sexual Exploitation Referrals Bureau ('CSERB') within the NCA. CSERB triages and actions CSA referrals. In all cases, child safeguarding is the priority. If the NCA receives a referral which indicates that a child may be at risk, the referral is disseminated directly to the police force where the child is. If the report refers to Com activity, CSERB also disseminates the referral in parallel to the

[7] Under US legislation, electronic service providers, including social media platforms, are required to report suspected online enticement of children for sexual acts, child sexual molestation, child sexual abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet to NCMEC.
[8] The NCA receives reports from members of the public via www.ceop.police.uk/Safety-Centre

RICC, who may then provide tactical operational support to the force.

50. In order for a referral to be progressed by the RICC the individual should be suspected of being a member of a Com group, ie. they[9]:
    a. Operate within an online chat group/ platform;
    b. Communicate or claim credit for their offending;
    c. Use identifiers distinct to a Com network; and
    d. Be involved in sextortion, and/or involved in cyber criminality, and/or involved in sharing extremist content, and/or encouraging real-world violence.

51. Each referral is considered on its own merits and the onward dissemination of the referral will depend on the dominant nature, scale and urgency of the risk identified. The NCA investigates only serious and organised crime:
    a. Depending on the nature and scale, Cyber Com networks may be referred to the NCA National Cyber Crime Unit ('NCCU')[10] or to local cyber police teams;
    b. Sextortion Com groups may be tasked to the NCA Child Sexual Abuse Investigations team ('CSA Investigations')[11] or local POLITs; and
    c. Offline Com networks are referred to CTP or local police forces depending on the severity of the real-world violence.

52. If referrals are made externally, for example a Sextortion Com group referral is sent to a local POLIT, investigating forces may come back into the RICC for tactical advice.

53. The NCA, through the RICC or otherwise, does not determine if someone is a VFI or not. If there is credible evidence within a referral that the individual poses a risk of real-world violence, but there is no evidence of other offending types and no evidence that the individual is in a Com group, the referral will be sent to CTP to assess and manage that risk, and consider next steps. Individuals posing a risk of real-world violence and Offline Com Networks are referred to CTP due to the risk of real-world violence that both cohorts pose.

---

[9] If a referral does not meet all of these criteria, the originator is informed that it does not relate to Com offending and that the RICC will be taking no further action on the referral. Any risk remains with the originator.

[10] On 16 July 2026 Owen Flowers and Thalha Jubair were each sentenced to over 5 years imprisonment for a cyber-attack on Transport for London. Both were members of a CyberCom network and the underlying investigation was carried out by NCCU.

[11] To date, no substantive Sextortion Com group referrals have been tasked by the RICC to the NCA CSA Investigations team. This may be because, as per paragraph 49, CSERB disseminates in parallel to local forces where the child is at risk and to the RICC if there is Com activity. The NCA CSA Investigations team have, however, conducted Sextortion Com group investigations prior to the RICC being established.

54. Regarding the safeguarding response for both offenders and victims, the NCA has a team of Child Protection Advisors ('CPAs') who sit within the NCA CSA Investigations team. If requested, the RICC can facilitate access to the CPA team, who will support both NCA and external investigations into complex cases through the development of strategies to enable appropriate safeguarding measures to be put in place for victims and vulnerable offenders. This may include signposting investigators to existing safeguarding mechanisms such as Multi-Agency Safeguarding Hubs and Prevent.

55. Project Rhyobasalt does not collate data or undertake any statistical analysis relevant to VFIs and their risk. I believe that CTP may be best placed to assist the Inquiry with data and/or any statistical analysis relevant to VFIs.

Collaborative Working and Partnerships

56. The NCA works with a number of domestic agencies and bodies to respond to the risk posed by Com groups, predominantly through Project Rhyobasalt. This multi-agency approach enhances intelligence-sharing, operational coordination, and the development of targeted interventions against Com networks' online infrastructure.

57. In particular, the NCA works closely with the Home Office ('HO') who chair the Non Ideological Extreme Violence Taskforce ('NIEV'), which is looking at the impact on victims, the behaviours and pathways of perpetrators and the role of the on-line environment. The NCA sits on this taskforce.

58. The NCA also works closely with Ofcom who are represented on both the Project Rhyobasalt Bronze and Silver Groups. The relationship is reciprocal, sharing both information on harms posed by the Com and information around harmful content and platforms that host it. I am aware that Ofcom carries out a range of regulatory activities, including investigations into online service providers, for example, into whether Telegram is complying with its duty to prevent CSAM being shared and into TikTok's compliance with its duties to protect children from encountering harmful content.

59. The NCA directly engages with social media platforms and tech companies such as Meta, Snapchat, Discord, Roblox, TikTok, and Telegram on a regular basis across the range of

SOC threats. Given the CSA offending by Com networks, the NCA's established relationships with social media companies and tech platforms are also being used to raise awareness of this threat and prompt an appropriate response from industry.

60. The threat posed by Com groups has been recognised internationally and there is significant buy-in and collaboration with international partners, including the Five Eyes Law Enforcement Group ('FELEG')[12], Europol[13] and the Virtual Global Taskforce.[14]

Project Rhyobasalt Outreach and Training

61. Project Rhyobasalt recognises that front line agencies need to be able to identify Com offending. To that end, the NCA/ Project Rhyobasalt has issued alerts to policing, industry and child safeguarding partnerships to help identify Com offending, with one of the characteristics being indicators of fixators with violence where ideology is not the primary driver.

62. We have different means of measuring how well these products have been received and used. For example, the Alert to safeguarding professionals (social workers, childcare safeguarding responsibilities) is available online and it has been accessed 6624 times since it was issued on 24 October 2025. There is positive anecdotal evidence regarding outreach initiatives with law enforcement and industry, and every police force in the country has made a referral into the RICC. However, there is not a complete understanding of what a Com group is across local policing. When conducting outreach initiatives, the Project Rhyobasalt team continue to encounter police officers who are unaware of Com networks.

63. Project Rhyobasalt has also provided training on Com networks in various forums, including:
    a. Domestic and international law enforcement communities;
    b. Cross-Whitehall policy partners;
    c. Police and Crime Commissioners;

[12] FELEG consists of international law enforcement agencies from the UK, USA, Australia, Canada and New Zealand. FELEG members work together to share intelligence, conduct international operations and enhance tools and techniques to tackle the most serious criminal enterprises with a global footprint.
[13] Europol's mission is to support EU member states, and many non-EU states, in preventing and combating all forms of serious international organised crime, cybercrime and terrorism. www.europol.europa.eu
[14] The Virtual Global Taskforce is made up of 15 dedicated law enforcement agencies from around the world working together to fight child sexual abuse. www.afp.gov.au/virtual-global-taskforce

d. NGOs (eg. National Organisation for Tackling Abuse);
e. Child safeguarding partnerships (eg. Lancashire Association of Secondary Headteachers and Gloucestershire Children's Safeguarding Partnership);
f. Academia (eg. The Journal for Sexual Aggression); and
g. Professional bodies (eg. The Royal Society of Psychiatrists).

64. In terms of further training outside of that delivered, and planned for delivery, by Project Rhyobasalt:
    a. I understand that the College of Policing is developing an online harms training module for policing which will include modules on the Com; and
    b. Feedback from teachers who have attended Child Safeguarding Partnership events has highlighted the need for PSHE teaching resources on the Com, along with resources for parents and children. The NCA's CEOP Education Team are designing these resources, which will be delivered to teachers, parents and schools in Autumn 2026.

Project Rhyobasalt Research

65. Project Rhyobasalt is establishing an academic research working group. This research working group consists of over 20 members from a variety of academic institutions, such as the NetworkPlus for Analytical Behavioural Science in Security and Defence ('NABS+'), the Child Online Harms Policy Thinktank and the Jill Dando Institute at University College London.

66. The aim of this research working group is to further inform the development of early intervention initiatives through a better understanding of offender pathways to Com offending and victim vulnerabilities[15].

67. To date, members of this group have contributed to a report commissioned by Project Rhyobasalt from T1D identifying pathways to Com networks. In addition, Project Rhyobasalt has also commissioned NABS+ to conduct a literature review of existing material published by other entities researching this area. The NCA is in the process of considering this review, with a view to developing behavior change initiatives[16].

[15] Terms of Reference for this group are currently being agreed.
[16] Behavioural and Social Scientists within the NCA will assist with developing behaviour change initiatives.

Current Laws for Monitoring and Disrupting SOC Offenders

68. In light of the comments made by Counsel to the Inquiry during the Opening Hearing of Phase Two, I have set out below some of the mechanisms used by the NCA to disrupt CSA and SOC offending. There are established civil and post-conviction order making powers in relation to sex offenders and SOC offenders. Monitoring offenders' compliance with orders in the community and online is obviously resource intensive.

Sexual Risk Orders ('SROs') and Sexual Harm Prevention Orders ('SHPOs')

69. SROs are civil orders used by the NCA and police forces to restrict the behaviour of individuals believed to pose a risk of sexual harm. They can be imposed without a conviction, where on application the court is satisfied to the civil standard that the Defendant has committed 'an act of a sexual nature'. This term is intentionally left undefined by the Sexual Offences Act 2003 to enable the Court to consider a broad range of behaviour.

70. SHPOs are available as a 'free-standing' order under the Sexual Offences Act 2003 but are more commonly imposed as a post-conviction ancillary order under the Sentencing Code. Monitoring of individuals subject to orders is generally carried out by police officers within the force area where the subject in question resides, or is intending to reside.

71. Both SROs and SHPOs can, if appropriate, be made against those under the age of 18.

Serious Crime Prevention Orders ('SCPOs')

72. SCPOs were specifically referred to at the Phase Two Opening Hearing in the context of managing and disrupting VFIs. As the Inquiry will be aware, SCPOs under the Serious Crime Act 2007 ('SCA 2007'), are available upon conviction for a 'serious offence' in the Crown Court and applications can be made in the High Court for stand-alone SCPOs [17].

[17]. Up until this year, such applications could only be made by the Director of Public Prosecutions; the Director of the Serious Fraud Office; and in cases that were terrorism related – a chief officer of police. Since the Serious Crime Act 2007, only one High Court application has been granted over an NCA subject. The Border Security, Asylum & Immigration Act 2025 has introduced amendments to the SCPO regime to enable High Court applications to be made by the NCA and police forces. Further, amendments (not yet commenced) give the court the power to impose interim orders.

The focus of SCPOs is preventative, not punitive, with terms proportionate to restrict and/or disrupt 'involvement in serious crime'. 'Serious Crime' is defined in the SCA 2007 to include, for example, drug trafficking, child sex offences, money laundering, fraud and certain terrorism offences.

73. Where, following consultation with the investigative agency, it is deemed appropriate to seek a post-conviction SCPOs, it is the Crown Prosecution Service who will have conduct of the application proceedings. The NCA or force is thereafter responsible for monitoring compliance with the terms of the SCPO. Since 2008, the NCA has monitored and managed 328 post-conviction SCPOs, with the serious crime underpinning the majority of these orders relating to drug offences, firearms offences and illicit finance. To date, no post-conviction SCPO has been sought in any NCA matter where the primary threat is 'violence'.

74. However, whilst the NCA pursues SCPOs to manage and mitigate the risk posed by those involved in serious crime, individuals under the age of 18 may not be the subject of a SCPO. As Com group nominals are largely young people under the age of 18 years old, this mechanism is not available for the vast majority of this cohort.

Proposed Legislation - Cyber Crime Risk Orders ('CCROs')

75. The NCA is currently working with the Home Office to develop a Cyber Crime Risk Order regime. The process leading to the proposals for Cyber Crime Risk Orders ('CCROs') arose from several high-profile cyber-attacks which highlighted a need for new civil intervention measures to support an enhanced risk management regime for those suspected of being involved in such activities ('cyber-offenders'). Principally focused on cyber-offenders while under investigation (where existing pre-charge police bail powers under Police & Criminal Evidence Act 1984 are insufficient), the NCA are proposing that the regime would also provide for ancillary orders (on conviction), as well as free-standing orders. I am hopeful that the introduction of an effective CCRO regime will be a significant tool in the fight against Com offending in this online environment.

Conclusion

76. The NCA is keen to assist the Inquiry in the most helpful, efficient and effective way possible. As I set out at the beginning of this statement, I am mindful that the NCA's work

in the online environment is tackling the wider threat posed by Com networks generally and, as set out in paragraph 13 above, the NCA has no role in identifying, assessing and managing the risk posed by VFIs. The NCA's position is that the approaches we are taking to disrupt Com groups may be relevant to Topic Two of the Inquiry, in that VFIs and Com offenders have some shared characteristics. If, having considered this high-level overview of work that the NCA does, the Inquiry would like further detail on any of the information provided in this statement the NCA would be happy to assist.

Statement of Truth

I believe that the facts stated in this witness statement are true. I understand that proceedings many brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed:____Signature_____

Dated:___24/7/26_____