United Kingdom

High-Harm Fraud and Scams

Industry Referral Guide

United Kingdom

Executive Summary

This guide sets out the core principles for industry partners submitting proactive intelligence leads directly to law enforcement on fraud, including high-harm scams and other high-risk fraud typologies. In the UK, that is into the National Crime Agency (NCA) where it will be considered by the Fraud Targeting Cell (FTC). It is intended to complement local reporting rules, and regulatory expectations. The guide goes beyond reporting individual victims' losses[1] or general suspicious activity reports[2] (SARs) focusing on disruptions against serious and organised crime.

The scope of this guide is for intelligence concerning suspects, criminal networks and enabling infrastructure (e.g. fraudulent platforms, professional enablers, insider threats) that demonstrate potential for high harm / complex fraud. It outlines the essential suspect-based information required for law enforcement to quickly action intelligence. The guide also outlines the necessary administrative, technical and legal considerations, including the need for data protection compliance and the differences between direct intelligence reporting and submitting a SAR.

While the examples and jurisdiction in this guide focuses on the UK, the principles and requirements outlined are designed to be globally applicable to all international partners and referral streams seeking to share intelligence on high harm economic crime.

Reporting Intelligence

UK law enforcement focuses on leads that demonstrate the potential for high harm and complex fraud that has a clear connection to the UK – be that a victim or a potential criminal. There are no fixed 'entry requirements' or numerical thresholds for referring a case. Instead the focus is on the quality of intelligence, for example, cases that clearly define a fraudsters footprint and the specific harm they're causing.

Proactive Intelligence; reports of all fraud types that identify individuals and organisations engaged in criminal activity or enabling crime. The lead is suspect-based intelligence (e.g. professional enablers, fraudulent platforms / websites or insider threats) rather than victim-based narratives. Law enforcement needs to be able to verify the intelligence before any action can be taken.

Impact and Harm; ongoing suspected fraud where the actual or intended harm causes substantial damage to UK individuals or businesses or the financial system, including major losses, vulnerable victims, essential services or critical infrastructure. In considering whether to progress a referral an assessment of its complexity, financial loss and location of offending will be made. The primary focus is on threats requiring national intervention, such as those related to overseas networks and complex online / cyber-enabled activity. While there is no strict minimum financial loss for review, referrals should focus on cases meeting these high impact and strategic criteria.

Victim Profile; a clear link to UK individuals or businesses with a connection to the UK.

[1] Report individual losses via www.reportfraud.police.uk
[2] Report SARs via www.sarsreporting.nationalcrimeagency.gov.uk

Evidentiary Requirements; when preparing a fraud referral, private sector organisations should consider law enforcements evidentiary requirements. Referrals should include all available data that supports the allegation, and the referring organisation should be prepared to cooperate with subsequent legal processes. To help with this, organisations could provide upfront guidance on their specific legal process, such as instructions on how law enforcement can request the preservation and production of additional data related to the initial referral.

Wherever possible, referrals should set out the full scale of the network across all affected countries and regions, not only the primary jurisdiction. Doing so helps law enforcement understand how far reaching the activity is, where suspects, enablers and additional victims are located, and where critical infrastructure or financial flows are concentrated. A clear link should therefore be drawn to each relevant country or region, as this creates opportunities for joint international collaboration, coordinated disruption and parallel interventions by multiple agencies.

Furthermore, acknowledging that many organisations cannot provide all data points upfront, they should consider steps to preserve all relevant data related to the suspected fraud activity. Data that is not included in the initial referral should be secured to prevent its loss or deletion, ensuring that it remains available for law enforcement if required. Additionally, third party or open source data should be shared separately from user records, allowing law enforcement to independently validate those data points with the companies that host the data if required. Where there is a transnational element or multiple signals from a variety of sources may be present, intermediary data sharing platforms[3] may facilitate the data exchange with law enforcement.

Essential Information

To ensure leads can be developed quickly into operational targets, submissions must be accompanied by detailed information. The focus should be on resolvable suspect identifiers.

Key Details

Field	Requirement
Lead Name / Contact Details	A short descriptive title (e.g. Cross border investment scam targeting EU and UK retirees via social media) and full name, role, organisation and primary contact details.
Executive Summary	A brief, high-level overview of the leads entire content, focusing on the suspected criminal activity, target, and urgency.
Key Points	A list of three to five most critical pieces of intel that highlight the harm and nature of the referral.

[3] E.g. the Global Signal Exchange

Fraud or Scam Type	Specify the type of fraud (e.g. Investment Fraud, Phishing, Romance Scams, Payment Diversion Fraud).
Stage of Activity	Indicate where the criminals are in the process of committing the crime (e.g. preparing the scam, targeting victims, moving stolen money, etc).
Additional Jurisdictions	Relevant countries in addition to the UK.

High-Value Suspect Identifiers

The quality of suspect-based information (i.e. that can be directly linked to a real person and / or device) will support the speed and likelihood of a law enforcement response.

Suspect Information (non-exhaustive)

Identifier Type	Requirement and Rationale
Suspect Indicators	As much information as possible, user names, known names / aliases, associated email addresses, phone numbers, suspected country of origin.
Digital Footprint Identifiers	If possible, specific IP addresses associated with the suspect's activity and associated geo-located data including date / time stamp, type of IP address (e.g. broadband / mobile).
Victim Information	A brief description of existing or intended victim profile (confirmed reports are not required but evidence likely to impact UK is essential).
Verified Source	Indicate if and how this intelligence has been verified or corroborated either through alternative internal or public sources ahead of the submission to support law enforcement into independently validating those findings.
Limitations	Any legal, technical, or internal policy restrictions that prevent the organisation from obtaining further information or assisting with any follow up action.

Maximising Impact

When you can provide device-specific and geo-located data within the initial referral this allows law enforcement to move from an intelligence lead to an evidential phase much faster. If possible, submissions should include any relevant supporting information. For example, when reporting a telephone number, details such as the number of times you received a call, and the associated dates, times and voice recordings could lead to a quicker disruption.

It is helpful if your intelligence shows how the information can be independently verified. For example, if part of your intelligence was gathering from a public social media account, law enforcement may replicate your research to make an evidential collection. Often, intelligence leads may no longer be publicly available, preventing law enforcement from replicating research. In these cases, submissions should include the timestamp of collection and URL details.

In rare cases there may be a need for that intelligence submission to be developed into an 'evidential' submission and therefore organisations should consider if the submitter has the ability to provide a witness statement if required.

Referral Gateway

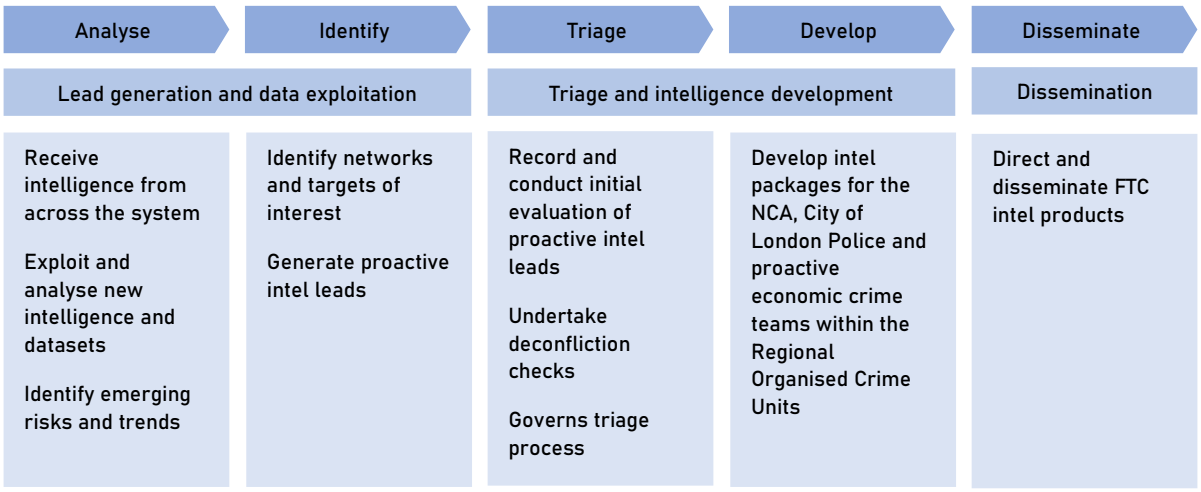
In the UK, proactive fraud intelligence referrals meeting the criteria outlined above can be sent to the FraudTargetingCell@NCA.gov.uk inbox for assessment. This is a dedicated email inbox for law enforcement and trusted partners. Details of this inbox should not be shared further than necessary or made publicly viewable.

The FTC can be contacted via this inbox to discuss a referral prior to formal submission. Submissions to the FTC are assessed and actioned to the most appropriate law enforcement body[4].

When making a submission, consider suggesting a specific law enforcement agency or team, especially if you have an existing relationship with them, as they may be able to advise on how to improve a submission and detail additional information. This aids law enforcement in quickly understanding the remit and severity of the referral.

This specific email inbox and triaging structure is operated by the National Crime Agency and designed for intelligence reporting within the UK. International partners should be aware that other jurisdictions will have their own reporting mechanisms and different legal gateways for intelligence sharing.

FTC Triaging Process



[4] The FTC does not accept any risk associated with a referral unless the case is formally adopted

The FTC works by analysing data to generate leads, triages them, develops intelligence, and disseminates packages to combat serious and organised fraud across regional, national and international borders.

Legislation

The lawful sharing of data[5] assists in providing legal gateways for sharing information with law enforcement. However, if such sharing is likely to become more than occasional organisations should consider a formal data sharing agreement with the relevant law enforcement organisation. Any such agreements should be accompanied by a Data Protection Impact Assessment to ensure the sharing is done securely and lawfully.

Security

Use encrypted emails if submitting material directly to any law enforcement team and ensure the document is encrypted at rest e.g. password protect the document and organise with the recipient for the sending of the password through an alternative, secure channel.

Suspicious Activity Reports vs. Direct Reporting

The practice of reporting suspicious financial activity is a global standard set by international bodies, however different jurisdictions may follow different legal frameworks. The information below details the specific reporting requirements used within the UK. International partners should always ensure they meet their own reporting obligations.

Suspicious activity reports are submitted to the UK Financial Intelligence Unit (UKFIU), which is part of the NCA. The UKFIU has sole national responsibility for receiving, analysing and disseminating SARs in the UK. Submitting a SAR provides law enforcement with valuable information about potential criminality. It may also provide you and your organisation with a defence to a principal money laundering or terrorist financing offence. By submitting a valid SAR to the UKFIU, you will be complying with your legal obligations to report suspicious activity under the Proceeds of Crime Act 2002 (POCA) or Terrorism Act 2000 (TACT).

SARs are solely for reporting knowledge or suspicion of money laundering under the Proceeds of Crime Act 2002 (POCA), or belief or suspicion relating to terrorist financing under the Terrorism Act 2000 (TACT). The SAR regime is not a route to report crime, including any predicate offences to the suspected money laundering.

Direct reporting to law enforcement should focus on intelligence that is time sensitive, strategic and operational. Reports should focus on leads that demonstrate the potential for high harm, complexity and a clear connection to the UK. This includes information on major threats, criminal networks or fraud that demonstrates high anticipated harm.

[5] Legislation such as Data Protection Act 2018 and Section 7 of the Crime & Courts Act 2013

Disclaimer

This guide has been developed with input from an informal multi-stakeholder working group involving experts from organisations across the banking, telecom and technology industries and the public sector.

The contributing experts and organisations include: Konrad Shek - Advertising Association; Dr. Simon Miller - CIFAS; Erica Stanford - CMS; Garry Lilburn - Cyber Defence Alliance; Jean-Jacques Sahel - Google; Marco Doeland - Dutch Banking Association (Nederlandse Vereniging van Banken); Carolina Caeiro and Emily Taylor - Oxford Information Labs; PayPal; TeamViewer; Helen Fairfax-Wall and Adil Munim - Stop Scams UK; Nick Sharp and Marc Knotts - UK National Crime Agency.

The views expressed in this guide do not necessarily represent the views of the organisations whose experts contributed to this work. Thanks, in particular for their work coordinating this effort and drafting to Carolina and Emily at OXIL, Nick and Marc at NCA, Simon at CIFAS and Jean-Jacques at Google.

Nothing in this guide should be relied on as legal advice

Annex. Case Studies

1. Major Scam Centre Targeted after International Operation

India's Central Bureau of Investigation (CBI) successfully raided a major fraud call-centre operating out of Noida, Utter Pradesh, resulting in the arrest of two individuals. This action was the culmination of an 18-month, collaborative investigation involving the CBI the NCA, the FBI, and Microsoft. The operation specially targeted a sophisticated Organised Crime Group (OCG) that fraudulently solicited payments from victims by posing as Microsoft employees. The criminals would display a deceptive screen pop-up suggesting the victim's device was hacked or infected, and then offer unnecessary software fixes for a fee. Victims in the UK alone are believed to have lost over £390,000.

The investigation was initiated after NCA International Liaison Officers (ILOs) in the US received intelligence from Microsoft, which was then cross-referenced with more than 100 Action Fraud reports from UK victims. The NCA and FBI worked together to confirm the same call centre was also targeting US citizens, leading to a coordinated partnership agreement via the NCA's Washington DC Liaison Office to share data. The OCG employed complex tactics to global servers via Voice Over Internet Protocol (VOIP).

The combined effort of the NCA, FBI and Microsoft successfully identified key suspects in India and compiled a robust file of evidence which included victim testimonies supported by the City of London Police (CoLP). This detailed intelligence was briefed to the CBI by NCA ILOs during a dedicated visit.

2. Identification of UK Smishing Farms

The Fraud Targeting Cell (FTC) – a joint National Crime Agency and City of London Police intelligence team worked with a Mobile Network Operator (MNO) to identify the locations of UK based Smishing Farms.

A Smishing farm refers to a location from where numerous SIM cards are used to send high volumes of scam text messages; often impersonating financial institutions or well-known companies. Smishing is a common method used by fraudsters to contact victims at scale.

The FTC worked collaboratively with the MNO to identify and prioritise the most significant subjects involved in this activity based on Industry held data such as 7726 fraud reporting and location information.

FTC developed and disseminated suspect based intelligence packages to UK Law Enforcement for intervention.

These packages resulted in warrants being conducted at numerous addresses, the arrest of subjects involved in high-harm smishing activity and the disruption of a SIM farm.

3. Blocked SIMs – Disrupting Fraud Routes Through Cross-Sector Collaboration

Pay-As-You—Go (PAYG) SIMs are increasingly being diverted in bulk from UK retail distribution to facilitate large-scale fraud. These SIMs are not used for legitimate calls, instead, they are used to receive one-time passwords (OTPs) to set up social media or messaging accounts that appear to be UK-based.

While telecommunications providers can identify and disconnect these numbers for breaching terms and conditions, the accounts previously authenticated through them often remain active and available to use for malicious purposes.

This challenge presents a cross-sector opportunity disruption. Stop Scams UK's (SSUK) tri-sector model has provided a platform for industries impacted by this activity to collaborate. By sharing blocked SIM data via SSUK, participating members can now identify and disrupt fraudulent accounts, as the initial breach of terms indicates a high risk of fraud. This data sharing allows for an ecosystem-wide approach to 'burning down' the fraud route.

Expertise from international law enforcement, industry[6], and regulators has converged through SSUK and the National Economic Crime Centre to map the extent of this vulnerability, focusing on matching data for account takedowns and gathering feedback. As the project evolves, it will expand to it will expand to additional industry partners and continue a full eco-system approach to mapping associated networks and implementing policy changes to increase the friction for SIM activation, closing the gaps criminals are exploiting to defraud UK consumers.

4. The Cyber Defence Alliance, Intelligence in Action.

The Cyber Defence Alliance (CDA) covertly collects intelligence from fraudsters' forums and groups to identify how they conduct frauds and cyber offending to enable organisations to defend against their techniques. It also allows for some of the criminal enablers, who provide services to many other criminals, to be identified.

Once the CDA determines the identity or other intelligence that can lead to an identification, this is reported to international law enforcement (LE) partners via an intelligence report. The CDA continues to support the investigation throughout, with intelligence being shared back and forth between them and LE partners.

This has led to hundreds of arrests in recent years including Operation Elaborate (malicious spoofing service) which led to 200 international arrests and a sentence of 13 years and 4 months for the main offender and also Operation Stargrew which targeted a Canadian phishing service targeting countries across Europe, North America and Australia. This led to 130+ international arrests and the main UK offender received an 8-year prison sentence. This sharing is underpinned with data sharing agreements and DPIA completion.

[6] BT, VodafoneThree, Meta, Match Group, Revolut, Santander, Monzo, Gamma.