



The National Fraud Intelligence Bureau's

Prevention & Disruption Team:

We are a team of Detectives dedicated to assisting UK Policing and Government departments in disrupting economic crime.



What We Do:

We work with service providers to take down:-

UK Phone Numbers,

UK Domains (Email/Websites)

Social Media Accounts (including Facebook/Instagram)

you have identified as used in Fraud.

How To Make a Disruption Request:

Send the team an email to:

NFIB-Disruptions@CityofLondon.pnn.police.uk

We will respond Mon-Fri between 8am-5pm

You will receive a short form to complete and an update will be provided following review by the team.

Guidance For The Submission of Disruptions Requests

Circulation Date: October 2023

Handling Conditions: This information is intended for the recipient only and should be treated in confidence. It should not be passed to another partner organisation without the permission of City of London Police. This information should not be uploaded to the Internet

The following guide will cover:

1. *Who The NFIB Prevention & Disruption Team Are.*
2. *What The NFIB Prevention & Disruption Team Can Do For You.*
3. *What Information You Need To Provide.*
4. *What Happens Next*

The National Fraud Intelligence Bureau (NFIB) Prevention & Disruption Team:

We are a team of 7 Detectives, led by a Detective Sergeant and a Detective Inspector within the NFIB & funded by the Home Office to identify and prioritise the takedown of Phone Numbers/Emails/Websites/Social Media Accounts used to commit fraud and cybercrime.

Through established and trusted relationships with the public and private sector we supply evidence to enable the takedown of these entities. We prioritise entities causing the most harm & loss to the public, to prevent further harm and help make the UK a hostile environment for fraud.

We accept referrals from UK Policing, government agencies, partner organisations and agencies.

We work closely with UK Registrar Nominet enabling us to check existing and newly registered domains and disrupt those created for fraud. We have established relationships with a number of service providers nationally and internationally and understand the best way to present evidence to secure a quick takedown.

We work with other partner organisations to share intelligence and build a fuller picture of criminality which we use to support our requests for takedowns. We work closely with the NCCU and UK Broadband providers to have fraudulent domains blocked from access, protecting UK Consumers when International providers refuse to act.

What Information You Need To Supply:

The following Information is required before a disruption request can be pursued, failure to provide this info will result in the rejection of your request:

- ✓ Check the entity is still live.
- ✓ Complete the P&D Team Referral form with an **NFRC Action Fraud reference number**
- ✓ Provide sufficient information to describe how the entity you want suspended is used to commit fraud/cybercrime.
- ✓ Confirm any checks you have carried out already and provide a summary on the referral form.

Guide Per Entity Referred:

Websites:

- ✓ We can suspend National AND International websites
- ✓ Tell us if you have reported the case to local police, this will enable us to image the website before requesting takedown.

Emails:

- ✓ In cases of Mandate Fraud **be careful** you provide the SUSPECT email account and not the genuine spoofed email account – we recommend enhanced research/enquiries to ensure the correct suspect account is referred (we have on a number of occasions, been sent a genuine email account as the suspect account to suspend).
- ✓ Include the FULL EMAIL HEADER and a couple of examples of any offending content (we don't need it all). This is required by the service provider and without this we may not be able to act.

Social Media Accounts:

- ✓ For Instagram and Facebook requests include a few example screenshots of the FULL URL and relevant offending content (ie – screenshots of cryptocurrency advertisements, messages requesting payments).
- ✓ We don't need everything, just a few examples to justify the request, this is required by the service provider, without which we cannot act.

Telephone Numbers:

- ✓ Check if it connects and is live before you refer it.
- ✓ Record on the referral form any response you receive when ringing the number.
- ✓ Phone numbers are critical to peoples daily life therefore a higher level of proportionality is required before suspension is considered.
- ✓ Date range of reports: this is important when referring telephone numbers for suspension- numbers can be **sold on** and have different customers within certain periods, we require the date range of when the number was used to facilitate the fraud so the service provider can identify who the customer was during that period, this will ensure genuine customers are not targeted.
- ✓ Spoofed Numbers: These are legitimate phone numbers which have been misused and we cannot suspend them.
- ✓ We CANNOT suspend non-UK telephone numbers.
- ✓ We CANNOT suspend WhatsApp numbers.

We will not consider a suspension request if there is no corresponding report of fraud. We do not cover brand protection or issues of brand misuse, this is a civil matter.

What Happens Next:

After you have sent your referral form to our inbox at : NFIB-Disruptions@city-of-london.pnn.police.uk you will receive confirmation from the officer managing your request, within 3 working days depending on demand and the size of the request.