National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

NFIB Fraud and Cyber Force Dashboards: FAQ

Data Sources

Fraud Force Dashboard

The Fraud Force Dashboard contains data from each of the following sources:

- Action Fraud Crime Data *http://www.actionfraud.police.uk/*
- UK Finance (formerly FFA UK) fraud data *https://www.financialfraudaction.org.uk/*
- Cifas fraud data *https://www.cifas.org.uk/*

Including data from each of these sources allows for a better overall assessment of fraud affecting each force area.

Cyber Force Dashboard

The Cyber Force Dashboard contains data from each of the following sources:

- Action Fraud Crime Data *http://www.actionfraud.police.uk/*
- NCSC Data *https://www.ncsc.gov.uk/*

National Fraud Force Dashboard

The data included in the National Fraud Force Dashboard does not contain data for the following police force areas: Guernsey Police, Isle of Man Constabulary and the States of Jersey Police. Although victims in the Police Scotland area are not required to report fraud via Action Fraud, where data is available for this area it has been included.

Data Limitations

Some of the data used is recorded directly by victims, for example via the Action Fraud website (*http://www.actionfraud.police.uk/*), and therefore may be subject to human error or inputting errors.

Victims reporting fraud offences, for example via Action Fraud, may not choose to disclose all information, including victim information, which leads to incomplete data used within the Dashboards. For example, there may be missing data linked to victim age, victim gender, victim type (Business or Individual) and victim location.

Date Ranges

The Fraud Force Dashboard represent six months fraud data for the period 01/10/2017 to 31/03/2018 inclusive.

The 'Cyber Attack Stage' sections of the Cyber Force Dashboard represent three months of data for the period 01/12/2017 to 28/02/2018 inclusive.

Reported Losses

Victim losses stated in the Fraud and Cyber Force Dashboards are based on loss amounts reported in Action Fraud recorded crimes.

We have tried to verify all reported losses over £500k and included them in the totals to give a more accurate reflection of the financial impact of fraud and cyber crime as reported by victims. When calculating average losses, only reports with a loss greater than £0 were included within the Dashboard.

Excluded Data

Action Fraud Information Reports

Information reports submitted to Action Fraud, which do not amount to recorded crimes under the Home Office Crime Recording Rules, are not included. Only fraud offences amounting to a crime under the Home Office counting Rules were included. *http://www.actionfraud.police.uk/homeoffice-fraud-counting-rules*

What do you mean by Volume of Frauds?

Crime volumes have been calculated using data from Action Fraud, UK Finance (formerly FFA UK) and Cifas.

Within the current period, crime volumes may be affected by a data issue identified in respect of 10,670 UK Finance reports, which have not yet been attributed to specific force area but have been included in the national trend figures. This is possibly due to a technical issue at the time of importing into the central NFIB database. Every effort is being made to rectify this issue as soon as possible.

See section on *Data Sources*

How are the Top 3 Fraud Types Determined?

The most reported fraud types for all police force areas exclude those reports that are categorised as **'**none of the above**'.** These are frauds which do not fit into any specific category. This exclusion only applies to the Force Fraud Dashboards.

The highest fraud type by volume is displayed first, followed by the second and third ranking.

What is reported under 'Businesses versus Individuals' on the Dashboards?

A small proportion of crime reports account for "unknown". These reports represent those victims that are unable to confirm whether they are either businesses or individuals, as data is dependent on victim self-reporting when completing a crime report.

The category **'**unknown**'** has been excluded from the total percentage of reports and does not feature on the Fraud Force and Cyber Force Dashboards. Only the percentage of reports that were from businesses or individuals are included within the Dashboards.

See section on *Data Limitations*

How are Victim Losses Calculated?

Victim losses stated in the Dashboards are based on loss amounts reported in Action Fraud recorded crimes.

Where possible efforts have been made to review and verify all losses reported in excess of £500k but further investigation may be required to determine if some of the larger loss amounts are a true reflection of the financial impact of the reported crime.

See section on *Reported Losses*

What is 'Victim Impact'?

Victim Impact is a self-assessment of impact the crime has had on the victim. It is determined by those reporting crimes via Action Fraud based on the following options:

Severe:	Have received medical treatment as a result of this crime and / or at risk of bankruptcy
Significant:	Impacting on health or financial wellbeing
Concerned:	Concerned about the fraud but it has not impacted on health or financial wellbeing
Minor:	Only a small impact on either health or financial wellbeing
Other or Unknown:	Impact assessment section has not been completed by a person submitting a report

What are the different types of Fraud and Cyber crime?

For more information relating to different types of fraud and cyber crime please see the Action Fraud and NFIB A-Z of fraud section on the Action Fraud website. http://www.actionfraud.police.uk/a-z_of_fraud

What is Cyber Enabled Crime?

The National Fraud Intelligence Bureau (NFIB) defines Cyber Enabled Crime as, '*Economic crimes that have been made possible because of computers*'. This is when a crime has been committed through the use of computers or other forms of information technology.

What is Cyber Dependent Crime?

The National Fraud Intelligence Bureau (NFIB) defines Cyber Dependent Crime as, '*Crimes against computers, also known as cyber dependent crimes under the Computer Misuse Act (CMA 1980)'*. This is in relation to crimes that can only be committed using a computer or other form of information communications technology. For example, the spread for computer viruses, hacking or Denial of Service (DoS) attacks.

What are 'Fraud Enablers'?

Fraud Enablers refers to the method employed which 'enabled' the crime to take place. The following list includes common enablers used by those committing economic crimes:

- E-mail
- Hacking
- Online sales
- Online Social Media
- Phone
- Post/Mail
- With Person Present

What do 'Delivery', 'Installation' and 'Communication' mean on the Cyber Force Dashboard?

When referring to the form of 'attack' in Cyber offences, there are three stages defined as:

Delivery:	The creation and sending of malicious internet traffic aimed at compromising people, devices and networks to gain access.
Installation:	Alteration of the target's computer system to preserve access and escalate the attack.
Communication:	Relaying commands to, and receiving information from, that system in order to gain control over valuable information and activity resources.

What are 'Crime Referrals'?

Crime Referrals are the number of National Fraud Intelligence Bureau (NFIB) recorded crimes disseminated to police forces for further investigation and enforcement during the reporting period.

This includes both Fraud and Cyber recorded crimes.

What is meant by 'Judicial Outcomes'?

Judicial Outcomes on the Fraud Force Dashboard refers to the final outcome of legal proceedings as reported by each police force. Those included are based on the disposal dates reported by the respective police force.

Outcomes are defined as per the Home Office Counting Rules. For further details on Home Office Counting Rules and Outcomes see: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/566188/cout-general-nov-2016.pdf