General guide to the NFIB

Information for Data Providers and the Public

National Fraud Intelligence Bureau

Issue 1 : Jul 2010

Contents

Contacts directory

NFIB Management Team

Head of the NFIB

D/Supt David Clarke – 020 7601 6802

david.clarke@cityoflondon.pnn.police.uk

Deputy Head of the NFIB and Head of Operations

DCI Richard Waight – 020 7601 6916

richard.waight@cityoflondon.pnn.police.uk

National Fraud Desk & Analytics Team

DI Amanda Lowe – 020 7601 6977

amanda.lowe@cityoflondon.pnn.police.uk

Fraud Focus Desks

DI Ian Gray – 020 7601 6807

ian.gray@cityoflondon.pnn.police.uk

Know Fraud Technical Lead

DI Steve Strickland – 020 7601 6978

stephen.strickland@cityoflondon.pnn.police.uk

National Fraud Desk

Telephone – 020 7601 6999

nfd@cityoflondon.pnn.police.uk

Fax – 020 7601 6938

NFIB Website

www.nfib.police.uk

Action Fraud contact details

www.actionfraud.org.uk

action fraud
report and support

Call
0300
123 2040

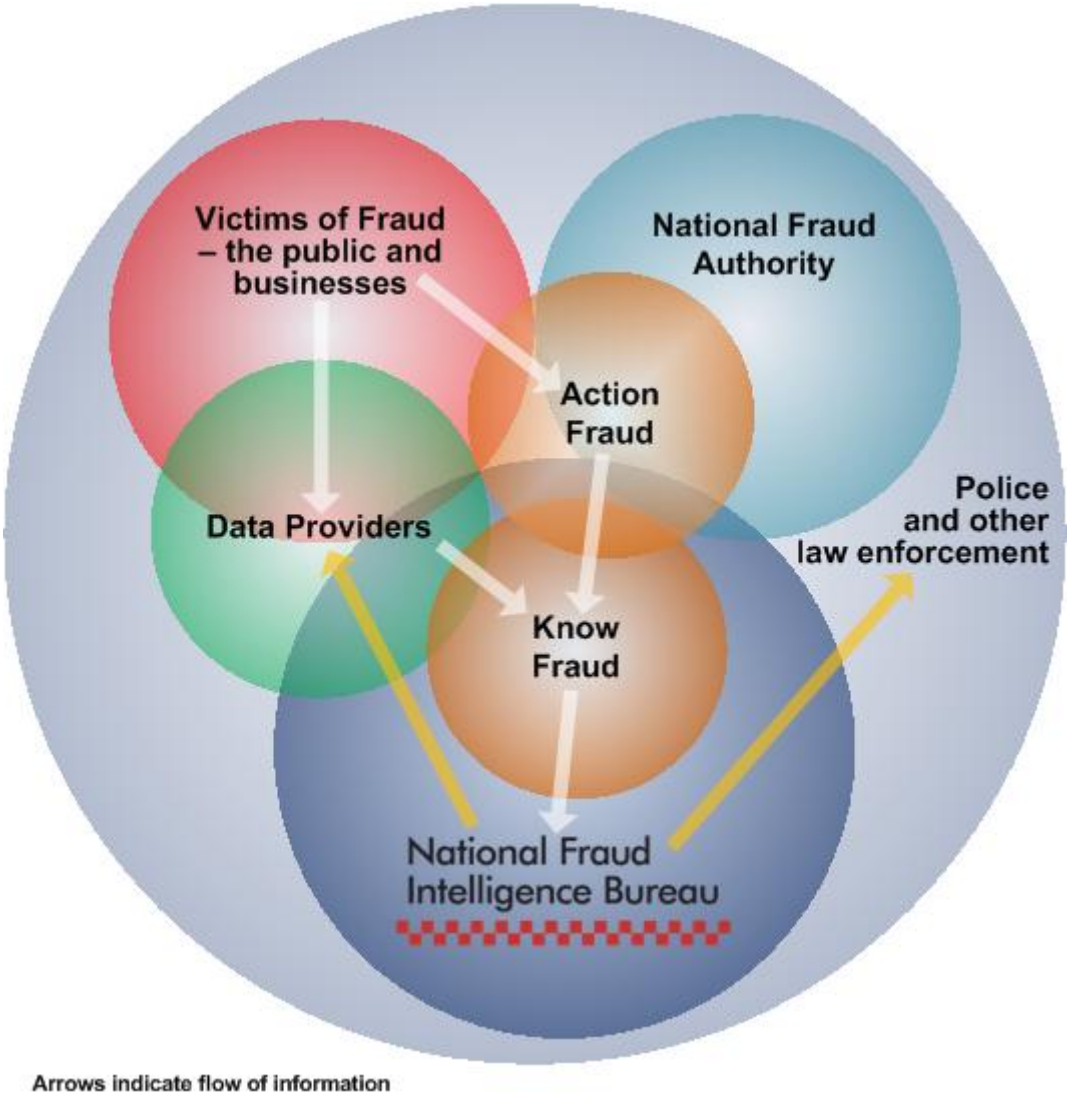
Purpose of this guide

This is a general guide to explain how the National Fraud Intelligence Bureau (NFIB) operates and how you, as a **counter-fraud partner**, can work with us to share knowledge on fraud.

This guide provides background to the NFIB including:

- A summary of each aspect of our work.
- Details of how individuals and organisations can work with us by providing the fraud intelligence and engage in joint working through secondments.
- The types of intelligence products and services different partners can expect from the NFIB.

Collaborating to fight fraud – serious about fraud



1. Introduction and background to the NFIB

Fraud is estimated to cost the UK economy more than £30 billion per annum and is responsible for wrecking lives, devastating businesses and helping to fund organised crime and terrorism.

Historically, many frauds go unreported to the proper law enforcement agencies. This, in turn, has reduced the quantity/quality of available information, which is vital to an effective, legal remedy to such offending. This situation allows fraudsters to operate 'underneath the radar', permitting them to commit and perfect further frauds that can damage thousands of people's lives.

The National Fraud Intelligence Bureau (NFIB) was created to help the police and their partners catch and disrupt these criminals and make the UK a more fraud-resistant society, by alerting our communities to threats from fraud and working together to prevent crime occurring.

This is achieved in three stages:

1. **Harvesting** of large volumes of information on fraud that is known to have occurred but which, in most cases, is not reported to, or made routinely accessible to, the police.
2. **Analysis** of the large number of fraud reports and turning them into intelligence, such as identifying the scale of fraudsters' criminal activities, which would otherwise not be visible.
3. **Use** this intelligence to support law enforcement operations and issue intelligence and alerts to partners and the general public.

How was the NFIB established?

In 2006, the Government commissioned the National Fraud Review, to assess the impact and scale of fraudulent activity across the UK. The review recognised that attempts to tackle fraud were being undermined by the lack of a joined-up approach to the reporting, recording and analysis of fraud. This was tied to the lack of a central repository for reports of fraud.

These findings led to a new, three-pronged approach to combat fraud:

- Formation of the **National Fraud Authority (NFA) –** a government organisation, to co-ordinate and oversee the fight against fraud.
- **City of London Police (CoLP) –** named as the National Lead Force for fraud, giving them responsibility for mounting additional counter-fraud operations across England and Wales.
- Creation of the National Fraud Reporting Centre, known as **Action Fraud**, and the **NFIB**.

What resources does the NFIB have?

The NFIB has one of the most advanced police intelligence systems in the world, capable of storing, then automatically matching and analysing millions of reports of fraud, to help catch serial fraudsters and provide a better picture of the nature of fraud.

Staff within the NFIB also have access to other, conventional intelligence and information systems, to support operations across agencies, sectors and national and international boundaries.

The Bureau is currently staffed by police and intelligence personnel from public, private and third-sector organisations, including:

- **CIFAS** – The UK's Fraud Prevention Service
- **CoLP** – City of London Police
- **NFA** – National Fraud Authority
- **SFO** – Serious Fraud Office
- **SOCA** – Serious Organised Crime Agency
- **SRA** – Solicitors Regulation Authority

Who funds the NFIB?

The Bureau is Government-funded and run by the City of London Police, as part of its remit as the National Lead Force for Fraud, in partnership with police forces and public and private sectors.

How does NFIB work?

The NFIB is looking for criminals who attempt to hide the extent of their crime. To find these offenders, the NFIB harvests reports of fraud that can help identify them. There are many organisations that record fraud committed against them or their associates, and an increasing number are sharing this data with the NFIB. These include reports from the public and small-to-medium enterprises, received via *Action Fraud*, plus confirmed fraud data from industry and the public sector, including organisations in the banking, insurance and telecommunications sectors.

Data providers supplying large-volume data to the NFIB include the Office of Fair Trading, CIFAS, UK Payments, Dunn & Bradstreet and Royal Mail.

The National Policing Improvement Agency (NPIA) are also looking to facilitate the transfer of police fraud data from forces into the Police National Database (PND) and then on into the NFIB's data warehouse. This process will commence when the PND becomes fully operational.

Millions of fraud reports are transferred to the NFIB system called '*Know Fraud*', located externally (within the UK) and accessed from the City of London Police. These reports are ingested into the NFIB's data warehouse and then, using analytical software, studied to identify patterns in offending. NFIB analysts and police officers assess and measure relevant data against set criteria. Frauds identified as having viable leads are then passed to the police force or other law enforcement organisation best placed to capitalise on this information. The receiving law enforcement body is responsible for deciding how to use this information, whether it is to launch a full investigation or take disruptive action.

The NFIB is the point of feedback for outcomes of any enforcement action resulting from disseminated viable leads. In this way, success metrics of disseminated leads and resulting enforcement activities can be established and evaluated and any gaps identified.

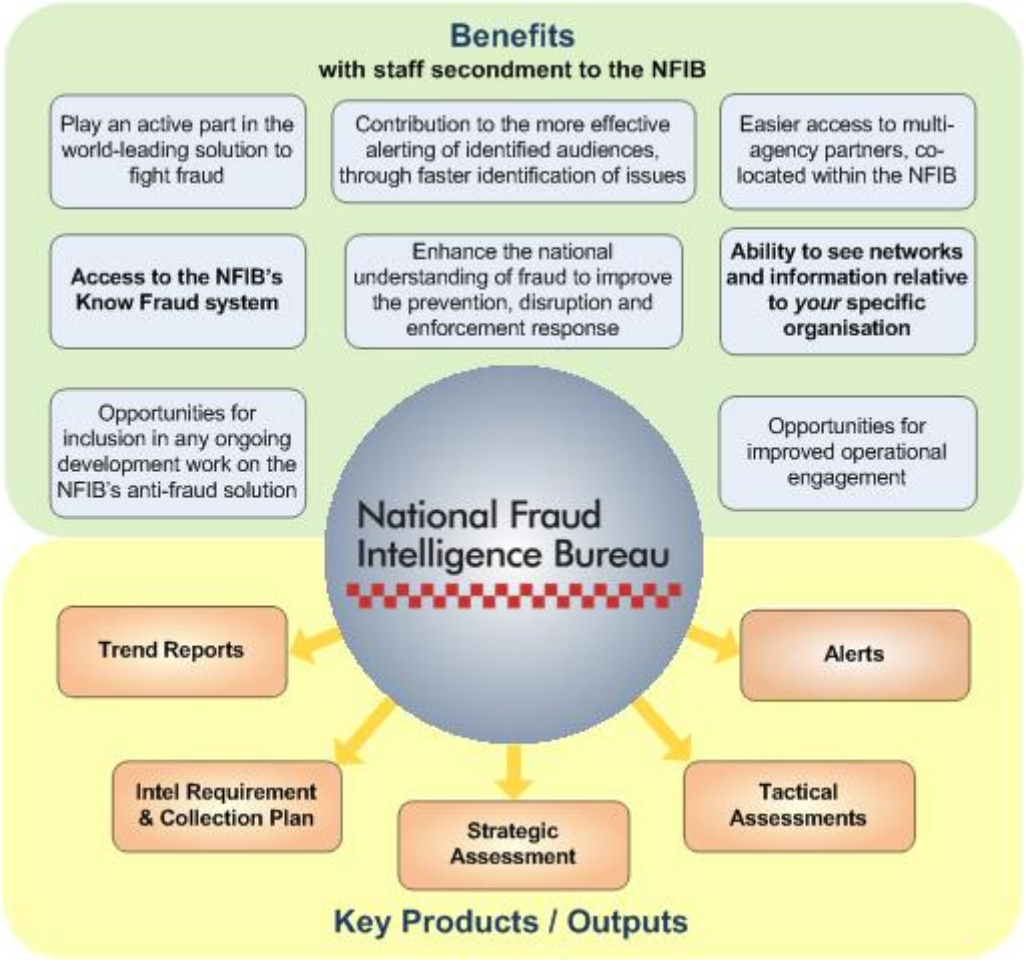
The NFIB's second major objective is to create an improved picture of the nature of fraud offending across the UK. This will enable closer working and more targeted prevention activity for police, industry and the public sector, over the short and long term.

Outputs from the NFIB include:

- Identification of the volume and value of confirmed fraud crimes in the UK.
- Identification of geographical fraud hot spots.
- Area maps, showing where specific types of fraud occur and against whom.
- Identification of reports linked to Organised Crime Groups (OCGs).
- A national picture, for law enforcement, illustrating where fraud-related crime occurs.

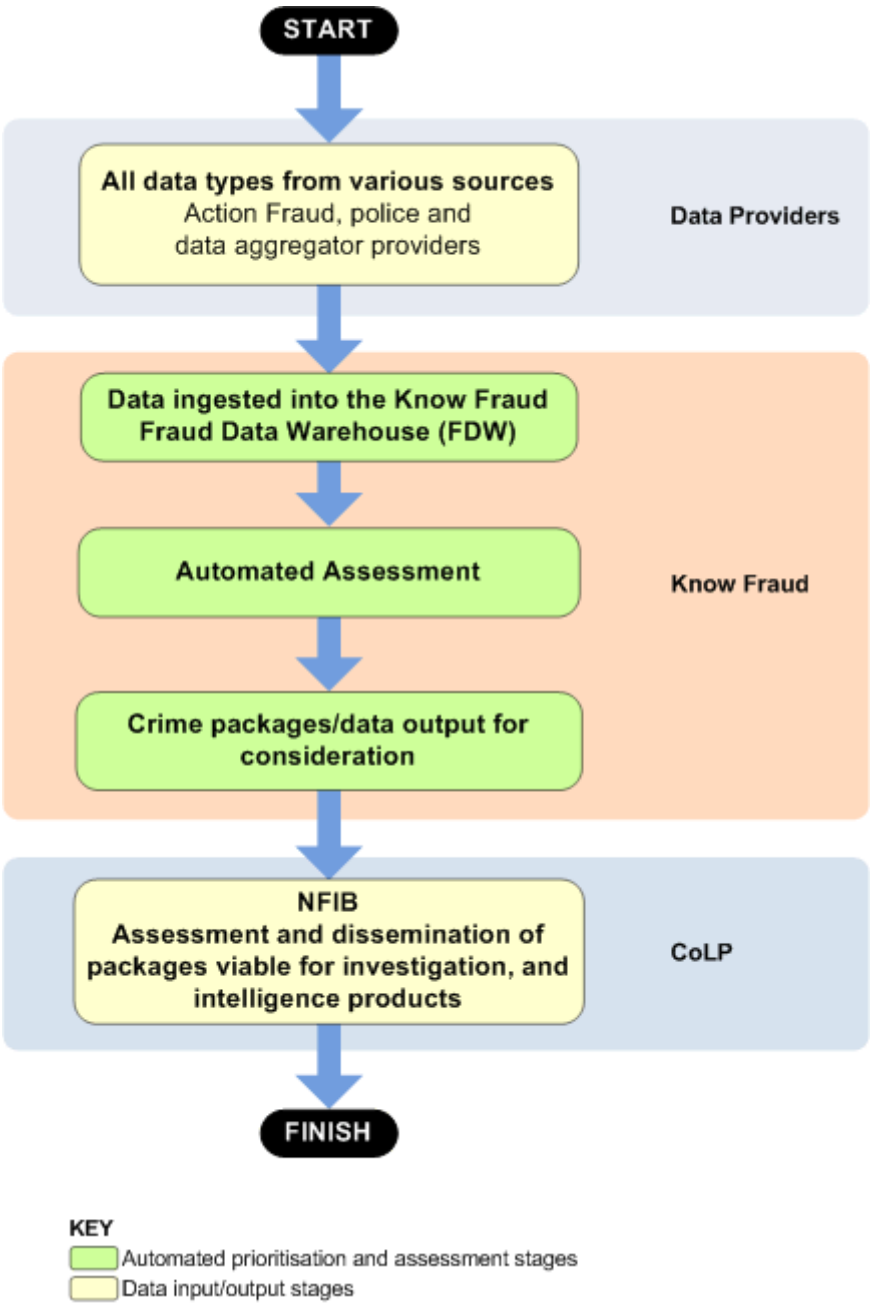
Benefits of working with the NFIB

While data providers and the wider public may receive product outputs from the NFIB, there are specific benefits for counter-fraud partners who second their staff to the NFIB. Key benefits are outlined in the diagram below:



Process overview

A simplified overview of the data acquisition, processing, assessment and dissemination process is shown below:



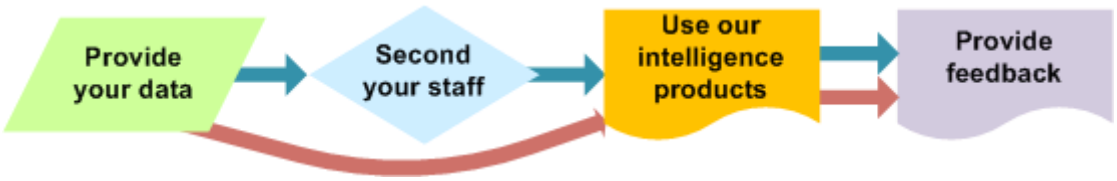
2. Working in partnership with the NFIB

How can I work with the NFIB?

As a counter-fraud partner, there are three ways that you can work with the NFIB:

1. Provide us with the data you hold on fraud,
2. Second your staff to work with us,
3. Use intelligence products we produce for you and provide us with feedback on these.

Typical examples of these arrangements are depicted below, with and without staff secondment to the NFIB:



Providing data to the NFIB

Individuals and small / medium enterprises

Whether you are an individual victim, or running a small business, we would like you to provide information on fraud committed against you, or your customers, by reporting the crime to *Action Fraud,* your local police, or one of the other fraud reporting channels that exist in the UK, such as CIFAS. These organisations will share all their fraud data with NFIB.

To contact Action Fraud for support, advice, or to report a fraud 24/7

Call: 0300 123 20 40

www.actionfraud.org.uk

Large business enterprises and public sector partners

Organisations that hold a large number of reports of incidents that are known to be fraud (and may not have been passed to the police) are encouraged to transfer this data to the NFIB, electronically, in regular, bulk updates.

There are two main methods for supplying fraud data directly to the NFIB:

- Via an existing, generic data transfer template.
- Via a bespoke data transfer and ingest mechanism.

For descriptions of both these methods, please see:

- *Chapter **3. Fraud data from large business enterprises and public sector partners**, on page 12.*
- ***Appendix A – New data set assessment tests**, on page 18.*
- ***Appendix B – Operational Spreadsheets – generic data transfer process**, on page 20.*

Seconding staff to work with the NFIB

We would like you to second staff to the NFIB, particularly where they have expert knowledge on aspects of fraud, or specialist skills in investigation or intelligence analysis.

The Government funds the NFIB, but its success relies upon support from the wider population in the UK and overseas, to help deliver its objectives. The City of London Police, CIFAS, SOCA, SFO, FSA, NFA and the SRA are just a few of the organisations that support the NFIB by funding staff who add value to its operation.

In arranging secondments to the NFIB, an assessment of mutual benefits is made, to ensure that both parties achieve best value and consistency with the NFIB's business strategy and secondment terms are maintained.

Key benefits for seconding partners are:

- Opportunities for improved operational engagement.
- Easier access to multi-agency partners, co-located within the Bureau.
- Ability to see networks and information relative to their specific organisation, law enforcement agency and/or business sector.
- Contribution to the more effective alerting of identified audiences, resulting from combined expertise and faster identification of issues.

For further information on secondments to the NFIB, and associated benefits, please contact the Head of Operations at the NFIB:

DCI Richard Waight – 020 7601 6916

richard.waight@cityoflondon.pnn.police.uk

Using our products and providing feedback

We want you to gain the maximum appropriate benefit from our crime and intelligence products. As far as possible, they will be tailored for the particular audience and be sanitised, or modified, to allow optimum dissemination.

Feedback from you will be an essential requirement, to enable us to measure national impact against fraud, the effectiveness of the counter-fraud community working together, and to ensure that each of our products are meeting your needs.

For further information on the dissemination and feedback process, please see:

- *Chapter **4. NFIB intelligence products – receiving them and providing feedback**, on page 15.*
- ***Appendix D – NFIB products and where they can be disseminated**, on page 23.*

3. Fraud data from large business enterprises and public sector partners

If your organisation has significant data on fraud that meets our adoption criteria, we would like to discuss its inclusion in the NFIB's Know Fraud data warehouse.

The intention is to increase the breadth and depth of data held in Know Fraud, in tranches, every 3-4 months, until NFIB reaches a position when the benefits associated with taking on new data sets are outweighed by the costs of bringing them in to the system.

Before it can be taken into the system, each new data set, identified as a potential ingest into Know Fraud, must be subjected to a comprehensive evaluation (known as the Data Ingest Management Process – DIMP). This involves a business and operational assessment by the NFIB, together with a system and technical assessment, undertaken by the supplier of the intelligence software.

*For information about the adoption tests we apply, please see **NFIB assessment tests for new data sets**, on page 18.*

FAQs

What large organisations currently supply fraud data to NFIB?

The NFIB's Know Fraud system has already gone live with a number of data sets, designed to be representative of the types of confirmed and attempted fraud information that is held outside the police service.

The initial tranche of data providers participating when the Bureau switched to fully live operation, in June 2010, is listed below:

Initial Data Providers

- Action Fraud
- AVCIS (ACPO Vehicle Crime Intelligence System)
- CIFAS
- Companies House
- Dun and Bradstreet
- Land Registry
- OFT – including Consumer Direct
- PhonePay Plus
- Royal Mail Security
- UK Payments
- Vodafone
- Law Enforcement Operations[1]

The NFIB has submitted a Request for Change, to take in additional data sets in tranche 2, which is planned to be available by the end of August 2010. We are working with a significant number of other counter-fraud partners to expand this list, shown on the following page:

[1] This consists primarily of operational police data, including Operation Halo, Operation Prime and the Metropolitan Police data on false identities. This also includes live operational feeds from other law enforcement and regulatory bodies.

Anticipated data providers

At the time of publication, talks were underway with a number of potential data providers from public and private sectors.

The NFIB has dedicated staff working to identify new, high-value data sources that will enrich the quality and effectiveness of the existing data set.

Will the NFIB only take data from sector representatives?

No – where there is a significant benefit to do so, the NFIB will consider taking data from individual organisations.

Our preferred approach is for organisations that hold large volumes of fraud data to partner with others in the same sector and to feed their fraud data into one central hub. This collective, consolidated data can then be passed to the NFIB electronically, in the same way as CIFAS operates, for example.

It is clearly more effective and efficient for the NFIB to operate as a 'Hub of Hubs', harvesting information from one place for each industry sector rather than many. However, we are also encouraging organisations in the same industry sector to work more collaboratively, to combat fraud across their sector and help protect each other from similar fraud attacks.

The majority of data providers operate as a 'hub' for other organisations to feed their fraud data sets into. Their data feeds into the NFIB's fraud data warehouse effectively make it a 'hub of hubs', as illustrated below.

Can the NFIB ingest all fraud data or are there specific assessment criteria?

Although we are looking to build a comprehensive picture of all fraud across all sectors, there is a significant cost associated with ingesting new fraud data sets into Know Fraud. Therefore, we have designed a data assessment process, which all data sets must be considered against before a decision is made to accept the data for ingest.

*For further information, please see **Appendix A – New data set assessment tests**, on page 18.*

Is there a simpler method for getting my organisation's data into the NFIB?

Yes – the NFIB has implemented a generic template, designed to provide a mechanism for ingesting data quickly from police forces on active operations.

We are also able to use this facility to ingest data on a one-off basis from organisations.

*For further information, please see **Appendix B – Operational Spreadsheets – generic data transfer process**, on page 20.*

How will data providers know whether fraud data they have provided has been used for law enforcement action?

If a data provider's fraud report forms part of crime report that is referred to a police force or other law enforcement agency, the data provider will be informed of this referral.

The provider will receive a monthly Tactical Assessment, advising them of recent NFIB-linked activity.

*For further information, please see **Appendix C – NFIB products**, on page 21.*

4. NFIB intelligence products – receiving them and providing feedback

What crime and intelligence products does NFIB produce?

The NFIB uses its wealth of data and access to key resources to produce a range of strategic and tactical products that are tailored for different audiences.

These include:

- The Strategic Assessment.
- The NFIB Control Strategy.
- The NFIB Intelligence Requirement and Collection Plan.
- Tactical Assessment, Subject and Problem Profiles.
- Alerts.

*For further details, please see **Appendix C – NFIB products**, on page 21.*

How can I commission specific intelligence assessments?

In addition to Control Strategy-led focus desks, the NFIB supports other organisations wishing to commission specific intelligence assessments.

An example of this is the Department of Health's request for an assessment of fraud affecting persons at risk ('No Secrets').

The procedure to commission such work is:

- Request made to the Head of the NFIB.
- Agreement obtained from the NFIB Strategic Assessment Review Board.
- Terms of reference agreed, including a funding agreement.
- Executive Board and Steering Group formed.
- Recruitment of appropriate team conducted in partnership with stakeholders.

The NFIB owns the finished products and agrees the audience for the finished assessment with the Executive Board.

Who can receive the various products?

Crime and intelligence products produced by the NFIB are tailored to the particular audience and can be sanitised or modified, to allow optimum dissemination.

*For further information about which products you can receive, please see **Appendix D – NFIB products and where they can be disseminated**, on page 23.*

Will you have a structured dissemination process?

Yes – the NFD is responsible for dissemination of all NFIB intelligence products to law enforcement and industry.

On completion of development, intelligence products are passed to the NFD, who ensure that the correct transfer protocol is used, relative to the Government Protective Marking System (GPMS), for dissemination. Where appropriate, products will be in compliance with National Intelligence Model 5 x 5 x 5 format.

How will you disseminate intelligence products to partner agencies?

- Intelligence products will be disseminated by the NFD to appropriate partner agencies on a need to know basis. These will generally be sent via the secure, **pnn** email system (CJX).
- Recipients are identified SPOCs within the individual agency.
- Where sharing with a partner is on a frequent basis, an information-sharing agreement will be required.
- Crimes referred to police forces from the NFIB will be disseminated in accordance with Home Office National Crime Recording Standards (NCRS). These determine the content of a crime report and provide guidance on how to identify the correct police force to which the crime should be referred.

Will you require feedback on disseminated products?

Yes – feedback will be an essential requirement, to enable us to measure the national impact against fraud, the effectiveness of the counter fraud community working together, and to ensure that each of our products are meeting your needs.

- A structured feedback process is in place for a quarterly review of the NFIB's service. This process will determine whether data quality meets the required standard, ensure that the process of effective and timely dissemination is in place and, most importantly, measure the impact and value of benefit realisation.
- The feedback process will be conducted every quarter. An electronic questionnaire will be distributed to those organisational SPOCs who have received products in the proceeding three months. Recipients will then be required to return questionnaires within an assigned three-week period.
- On receipt, the NFIB will engage in a results analysis. Results will be consolidated and any recommendations submitted to the Head of the NFIB for consideration. The Head of NFIB will advise on any matters of change management and timescales. The final report will then be submitted to recipients, to detail the feedback and advise as to any action being taken as a result.

- The feedback process will maximise the opportunity for organisational learning. Law enforcement agencies will be requested to provide any operational learning gained from investigations. This will include evidence gathering, prosecution guidance and investigative techniques.
- Similarly, any information surrounding the modus operandi and details of how the offence was perpetrated will also be required. Once collated and analysed, this information will be disseminated, in the form of either alerts or guidance documents, to law enforcement and/or industry.

Appendix A – New data set assessment tests

NFIB assessment tests for new data sets

Each new data set must pass the following explicit tests before it can be considered for ingest:

1. **Does it add breadth to the existing data sets?**

   Does it introduce data on new types of fraud that are not currently held in Know Fraud?

2. **Is it complementary to existing data sources?**

   Is the data set already provided in part, or wholly, via one of the existing data integrators (such as UK Payments or CIFAS)? For example, if a mobile phone number is included in an existing data set in Know Fraud, the provider's additional data could provide the name and contact details of the individual to which that phone is registered.

3. **Does the data set provide value to the NFIB's Control Strategy?**

   *For information on the Control Strategy, please see **Appendix C – NFIB products**, on page 21.*

   For example, is the data set in line with NFIB priorities and does it add value to one of the existing control themes?

4. **Does it meet the criteria for confirmed and attempted fraud**?

   On the balance of probabilities, is it believed to be fraud by the supplier? Or, is it intelligence-based or unclear whether it is fraud – sometimes referred to as 'Grey Data'?

5. **Can it be ingested into Know Fraud using an existing template?**

   For example, by using existing Operational Spreadsheets, rather than having to build a bespoke ingest system.

   *For further information, please see **Appendix B – Operational Spreadsheets – generic data transfer process**, on page 20).*

6. **Is the data set representative of a sector or industry grouping or individual company related?**

   The NFIB is most effective and efficient when acting as a 'Hub of Hubs' and would prefer to take data that has already been aggregated by companies in a specific sector, using fraud intelligence sharing mechanisms, rather than from several businesses in a sector.

7. **Can the data set be provided in a consistent format?**

   For example, if there were plans for a data set to be significantly revised in the near future, it would probably be an inefficient use of time and resources to ingest it in its current form into Know Fraud.

8. **Does the data set have sufficient volume and is it updated frequently enough to justify the design of a bespoke data ingesting mechanism?**

What are the technical tests criteria for new data sets?

Once a proposed new data set has passed NFIB business and operational tests, the NFIB will attempt to ingest a subset of the data into Know Fraud, using existing Operational Spreadsheets.

This may require the NFIB to omit particular field data from the ingest. However, it will enable an evaluation of the data set's potential to add valuable information to existing networks identified in the system.

If the data set passes these tests, then it will be passed through to NFIB's system partners under a Request for Change process, for technical evaluation and scoping.

They will consider:

1. Compatibility with existing data sets.
2. Technical complexities of ingest – does it contain a large number of fields of very specific meaning and potentially unique to a provider?
3. Impact on existing data sets.
4. Cost of designing a bespoke ingest process, if necessary.

After both the assessment test and technical test stages have been completed, the NFIB will then have a clear understanding of the potential value of the data set and any costs associated with designing an ingest mechanism. At this point, a decision will be made by the Director of the NFIB as whether to proceed with initiating the work, to establish an ingest for that data set.

Appendix B – Operational Spreadsheets – generic data transfer process

There are six individual Operational Spreadsheets:

- Persons
- Locations
- Organisations
- Vehicles
- Communications
- Finances

By using these Operational Spreadsheets, police forces and organisations can provide key pieces of data on suspected fraudsters, such as:

- Name(s)
- Address(es)
- Bank account(s)
- Business details
- Telephone numbers

This data will be compared against the Know Fraud system and any matches identified and the results then fed to appropriate forces.

Data ingested in this format is, by necessity of design, limited to structured, generic data items. Know Fraud is unable to ingest fraud modus operandi information, or free-text descriptions/notes, via this particular ingest route.

This does not remove the need for forces to request specific individual checks (as covered by standard operating procedures). It simply provides an additional facility for large quantities of data to be compared against the system.

The key benefit of this approach is that it automates what has previously been a labour-intensive task for the NFIB's Single Point of Contact and, because of the automated production; results will be available in a timelier manner than before.

Tranche 3, which is scheduled for ingest in November 2010, is beginning to take shape and will include:

- **Establishment of a PND ingest mechanism for police data.**
- **An extract from the Insurance Fraud Bureau (IFB) Red Flag database** – that will separate the IFB's confirmed fraud from grey data, to allow only confirmed fraud data to be passed to the NFIB.

Plans are also underway to ingest a selection of data from other law enforcement partners, such as the Department for Work and Pensions (DWP), using our Operational Spreadsheets.

Appendix C – NFIB products

Product	Description
Strategic Assessment	Knowledge and understanding is the key to succeeding against organised crime. The Strategic Assessment provides a national overview of fraud and an assessment of its link to other, organised crime. The assessment identifies emerging medium-to-long term issues that impact our communities and will influence organisational priorities and resource allocation in the arena of fraud investigation. The assessment gathers information from a wide variety of sources, including law enforcement, the public and business communities. A multi-agency Strategic Review Group agrees future assessments, determines the Control Strategy and intelligence requirements/collection plans. **Reviewed:** biannually, affording a changing view of the current UK fraud landscape. **Published**: in November of each year, the NFIB Strategic Assessment makes a significant contribution to the UK Threat Assessment (UKTA) on Organised Crime. The UKTA is intended to inform UK law enforcement priorities for tackling organised crime and other initiatives such as changes to legislation, regulation and policy.
Control Strategy	Informed by the Strategic Assessment, the Control Strategy provides direction on the UK response to those threats identified in the Strategic Assessment and informs prioritisation of national activity to combat fraud crime. Any control strategy derived from the Strategic Assessment is available. It highlights priority problems and proposed law enforcement/community responses in the following priority areas: • Prevention. • Intelligence. • Enforcement. **Reviewed**: biannually and prepared on an annual basis. The UKTA organised crime control strategy consists of 13 programmes, each with its own multi-agency plan, deliverables and governance arrangements. The NFIB Control Strategy seeks to maximise opportunities to reduce the harm of organised fraud crime. In doing so the NFIB is collaborating on activity aligned to it's current Control Strategy with the following programmes: • Non-Fiscal Fraud (payment card and share purchase fraud). • Criminal Finances and Profits (money laundering). • Organised criminals, their business structures and logistics (organised crime groups and professional enablers).
Intelligence Requirement & Collection Plan	This details the intelligence gaps identified by the Strategic Assessment, and provides practical direction on how they could be filled with suggested methods and avenues of collation. **Reviewed**: biannually and prepared on an annual basis.
Tactical Assessment	This is a review of recent NFIB activity and identifies short-term issue considerations in the fraud arena, which are reviewed in accordance with the Control Strategy. The assessment drives the tasking and co-ordination function of the National Fraud Desk (NFD), at the NFIB, which determines the specific commission of intelligence products. Included in the Tactical Assessment is a report detailing reported crimes, which are identified by postcodes falling within police force areas. These reports enable forces and wider partners to assess the amount of harm from those crimes that inform daily policing and business risk management priorities. **Produced**: monthly.
Crime Reports	A crime report can be either a single report, or an aggregation of a number of reports, identified by the National Fraud Desk. Once identified, a number of predetermined intelligence checks are made and, where appropriate, analysis conducted to provide receiving law enforcement agencies with an informed tactical product. The NFD Crime Manager may assign NFIB analysts to develop intelligence further, whether as a result of being aligned to the NFIB Control Strategy or due to specific, identified risks.

Product	Description
Subject / Problem Profile	Subject/Problem Profiles include sufficient detail to initiate, or add value to, ongoing economic crime investigations. They also provide: • Appropriate intervention and prevention opportunities. • Any relevant risks to be managed. • Intelligence gaps. • Any partner agency involvement that that may be required. The content of a profile varies depending upon the nature and significance of any particular issue, as follows: • **Subject profiles** – secure a greater understanding of either a person (suspect or victim) or group of people. • **Problem profiles** – secure a greater understanding of established and emerging crime or incident series, priority locations and other identified high-risk issues. Both are tasked by the NFD in line with strategic priorities as determined by the Tactical Assessment/tasking process.
Trend Reports	Trend Reports are published in the form of intelligence reports resulting from analysis of issues, such as: • Emerging crime trends. • New modus operandi. • Victim profiles that highlight a particular group being targeted by crime groups. • Specific geographical or community areas and business sectors at risk. • Offender information (not necessarily names and addresses). This information informs law enforcement, business, or specific sectors of the community, to enable better-informed decision-making around harm reduction and crime prevention activity.
Alerts	Alerts identify emerging or current threats that have impacted a particular area, such as a community, business sector or geographical area. There is no specific format for an alert, though they will complement existing structures; for example, the alert issue process managed by SOCA. Alerts are a valuable method of disseminating information for the prevention, disruption and enforcement of crime. The NFIB distributes alerts to a wide community, including the public, law enforcement and key counter-fraud partners. Types of alert can vary and each one is produced for a particular purpose, whether to prevent types of crime, or initiate an enforcement response. Alerts may include: • Current criminal methods used, particular to a fraud type. • Geographical information on crime trends. • Statistical information, such as the measurement of harm linked to a crime type. • Consumer advice and guidance on how to avoid problem issues. • Best practice advice on effective law enforcement options. • Calls for information, where wider assistance is needed to develop an intelligence picture. Methods of distribution for alerts are governed by content, target audience and the appropriate security that must be applied. Distribution methods include: • The media. • NFIB and Action Fraud websites. • Specific circulation groups. • Identified sectors, whether corporate or private, particular to an issue. Alerts are a valuable tool and to ensure maximum impact the NFIB collaborates with a number of key partners to ensure that this is maintained.

Appendix D – NFIB products and where they can be disseminated

NFIB Services and Products	Police	Other Law Enforcement	Regulator	Partner having staff in the NFIB	Data Provider	Counter-fraud associations	Public
Access to the NFIB's Know Fraud system	✓	✓	✓	✓	✓	✓	
NFIB Strategic Assessment	✓	✓	✓	✓	✓	✓	✓
NFIB Control strategy	✓	✓	✓	✓	✓	✓	
NFIB Intel Requirement & Collection Plan	✓	✓	✓	✓	✓	✓	
Tactical Assessments (TA)	✓	✓	✓	✓	✓	✓	
Crime Reports	✓	✓					
Subject and Problem Profiles	✓	✓	✓				
Trend Reports	✓	✓	✓	✓	✓	✓	✓
Alerts	✓	✓	✓	✓	✓	✓	✓

NOTES:

a. It is important to emphasise that access to the NFIB and its systems is restricted to those employed within their specific roles at the NFIB, and in accordance with agreed ACPO Doctrine and Standard Operating Procedures and conditions of data-sharing agreements with partners, details of which are held by the NFIB.

b. The content of any report is assessed before being disseminated and edited according to the management of risk associated to the provenance of the information. As a result, recipients of NFIB products will receive differing versions, based upon an assessed 'need to know' basis.

National Fraud Intelligence Bureau

General guide to the NFIB