



HEADLINE NEWS

NFIB at the heart of a new order

The kaleidoscope that is the national fraud landscape has been shaken up, and as the pieces begin to settle into place and a new picture emerges, the NFIB is at the forefront.

The National Crime Agency will have an Economic Crime Command as part of its structure when established in 2013. To start the work of developing the national drive against fraud, an Economic Crime Co-ordination Board has been established, with Prevention, Intelligence and Operational Sub Groups.

The NFIB is a key player on the new Economic Crime Intelligence Sub Group (ECIG), which has a particular focus on identifying the national fraud threat and intelligence gaps.

The multi-agency group met for the first time in January, with the NFIB working alongside partners to provide current assessments on the greatest fraud threats and their likely impact on the UK, money laundering typologies and fraud related organised crime groups.

Importantly the NFIB is also working with UK

law enforcement and counter fraud agencies to identify intelligence gaps that continue to hinder the national response to economic crime, and is using the *Know Fraud* system to feed the Economic Crime Operations Sub Group (ECOG) with enforcement opportunities.

In the first weeks of 2012 information from UK banks was passed to the NFIB by ECOG. Analysts ran the data through *Know Fraud* – and within days had provided ECOG with intelligence packages containing evidence of criminality. This led to a multi-agency

operation, headed by the City of London Police, which saw 13 people arrested.

Another major stride forward this month came when the Chief Constables' Council supported the City of London Police's proposals to establish a national economic crime capability.

An integral part of this three-phased programme will be the placement of two regional intelligence officers within each of the ten ACPO Regional Intelligence Units (RIU's) providing a two-way flow of information with the Bureau.

The new Director of the NFIB, Det Supt Dave Clark, said: "The NFIB has forged a strong foothold as the country's thematic intelligence hub for fraud, drawing on an expanding knowledge base and enhanced technological capabilities to provide a better understanding of the fraud threat we now face."

Spotlight on industry: In this edition we speak with PROFIT's Barry Gooch about his ideas on tackling fraud in the UK's travel industry. (see page 4)

Listening to you: our top priority

Engaging with our stakeholders is a top priority for 2012. We need your feedback to ensure we are delivering the products and services that you need.

Part of the new vision and purpose of the NFIB is a commitment to make a more effective contribution to combating organised crime groups. To better understand our stakeholders' needs in this area we recently

held a police and law enforcement agency tasking workshop, with representatives from regional intelligence units, the FSA, SFO, HMRC and UKBA attending. The event included a demonstration of *Know Fraud* in action and was an opportunity for agencies to meet their dedicated NFIB SPOCS.

We will be holding other similar events for our partners in 2012 while also expanding the

liaison officer concept. This will be supported by a programme of stakeholder surveys, one-to-one meetings and forums. We have also set up a dedicated email for your feedback.

Please feel free to email ideas and questions to:

NIFBfeedback@cityoflondon.police.uk

Message from Det Supt Dave Clark



Welcome to the first NFIB eNewsletter for 2012!

I am now one month in as the new Director of the NFIB, and in this short space of time subtle changes

have already been made to the way we do business. At the same time foundations have been laid that I believe will see the NFIB become a cornerstone of the counter fraud strategy as we work towards the launch of the National Crime Agency in 2013.

My first priority has been to speak with each of my staff members to hear their thoughts on the way forward. Their feedback has helped restructure the Bureau, which is now built to complement our core functions. I believe this set-up will make us a more efficient and innovative organisation that is more respondent to the views of our partners and

national responsibilities. This will enable us to provide improved products that will lead to better fraud prevention and increased fraud detection nationwide.

As part of the new programme we are also investigating new innovative ways to use our systems and the millions of fraud reports held by us.

During this period of reconfiguration I have also undertaken a series of face-to-face meetings with major commercial stakeholders. To ensure this two-way exchange of information becomes the norm we have begun appointing

NFIB SPOCs, who are responsible for liaising with individual agencies.

2012 has already been marked by a number of milestones. We held our first NFIB event – an intelligence Tasking and Coordination workshop for regional police and enforcement agencies; we actively participated in the first Economic Crime Intelligence Group; and witnessed ACPO agree to proposals for a national economic crime capability. And this is just January!

Det Supt Dave Clark
Director of the NFIB

eNewsletter

NFIB eNewsletter is published quarterly by the National Fraud Intelligence Bureau

Contacts

Director of the NFIB:

Det Supt Dave Clark: 020 7601 6908
d.clark@cityoflondon.police.uk

New Business, Projects and Concepts:

DCI Richard Waight: 020 7601 6916
Richard.waight@cityoflondon.police.uk

Crime and Intelligence Operations:

DCI John Osibote: 020 7601 6806
john.osibote@cityoflondon.pnn.police.uk

Products and Outputs:

Steve Prideaux: 020 7601 6772
steve.prideaux@cityoflondon.pnn.police.uk



Action Fraud update from the NFA



In August 2011, Action Fraud launched the capability for victims and witnesses to report fraud intelligence. On average over 1,600 information reports are being received each month and sent to the NFIB.

The Government's Cyber Security Strategy published in November 2011 outlined Action Fraud's developing role as the place to report internet crime.

In December, Action Fraud introduced a "light touch" reporting tool, giving the public the ability to report online scams, such as

attempted phishing attacks, and viruses. During this month, 2,199 attempted online scams and 123 viruses were reported. These were primarily related to phishing and phone fraud with 95% of reported incidents concerning malware attacks aimed at computers and other online devices.

Expanded reporting capability

In January Action Fraud expanded its reporting capability to accept internet crime, including crimes that infringe the Computer Misuse Act. Examples of these are hacking and denial of service attacks. Internet crime occurs when

an individual is specifically affected by financial or other loss.

As a part of the ongoing development work Action Fraud's website will be refreshed to reflect this new function, improving customer journeys. The first phase will go live in March.

Viral campaign – looking to the future

A viral campaign produced in partnership with the banking and telecoms industries and focusing on protecting personal information is planned for mid-2012.

NFIB: Fine tuning the way we do business

The NFIB engine is now divided into three key parts that combined together are driving our performance and ensuring we are delivering the right products and services for stakeholders, partners and the UK public. The **Products and Outputs, New Business, Projects and Concepts and Crime and Intelligence Operations units** are at the heart of everything we do and produce.

1 Products and Outputs

Crucial to the ongoing development of the NFIB is increasing the volume of data and range of data sets held in *Know Fraud*. This will enhance the NFIB's core crime datasets, which increases the quality and quantity of the crime packages and intelligence reports that our desk officers produce.

As part of the programme to reduce fraud error and debt in the public sector, the NFIB is running data sharing projects with government agencies and other public sector organisations. Important milestones were reached in December with the completion of initial data trials for the NFIB's data sharing programme with HMRC and UK Border Agency.

Particularly good progress has been made with the UKBA following the incorporation of two significant samples of crime related data. Initial data matching enhanced a significant number of networks within the database. Early indications with the HMRC crime data sample are also very encouraging and we will be exploring options to provide data packages for action, and develop a flow of new information back to the NFIB.

Steve Prideaux

2 New business, Projects and Concepts

Report Lite and the NFIB response to phishing and malware attacks opened for business in December 2011 and have already received more than 4,000 referrals. Noticeable trends include phishing emails purporting to be from the telecommunications industry and social networking sites seeking personal credentials and cash.

One of the first cases saw analysts working with the travel body PROFIT on an online airline ticketing fraud where fraudulent websites are purporting to be accredited airline ticket agents promising cheap deals. The fraudsters buy tickets on behalf of consumers and then cancel them at a later date once the tickets have been issued. Victims only find out the tickets have been cancelled when they go to confirm their flights days before they leave or even when they arrive at the airport.

The Cyber Crime team has worked with internet service providers and domain registrars to suspend the websites, the banking industry to block bank accounts, and with the telecoms industry to suspend listed phone numbers.

DCI Richard Waight

3 Crime and Intelligence Operations

NFIB continues to work on improving the quality of the crime products to forces. Recent examples include:

- The NFIB received a dating scam allegation where a US-based victim had transferred \$60,000 to a UK bank account. There were no viable lines of enquiry until an NFIB assessment of the intel resulted in the MPS fast tracking the case and arresting two people, with one making a full confession.
- The Bank of Ireland was alerted by the NFIB to a suspect account and soon after a man came into a branch and tried to withdraw money. Local police arrested the man and the NFIB disseminated Action Fraud reports for the subsequent investigation.

In December the *Financial Crime against Adults* report, commissioned by the Home Office, Department for Health and ACPO, and collated by the NFIB, was published. It highlighted how vulnerable adults are being exploited by apparent friends, family, small-time fraudsters and organised criminals alike, suffering losses ranging from a few to millions of pounds.

DCI John Osibote

42,000

Nov data ingest into
Know Fraud (25,000
CIFAS + 10,000 UK
Payments)

133 + 8 phone
numbers and
websites

suspended by NFD
in November and
December

6%

of all Action Fraud
reports coming
from overseas in
November

In this edition we speak with PROFIT's Barry Gooch about his ideas on tackling fraud in the UK's travel industry.



PROFIT: just the ticket to fight travel fraud

In the past 12 months hundreds of travel businesses have closed down or reduced their operations across the UK. Barry Gooch from industry body PROFIT (Prevention of Fraud in Travel) believes it is not just ash clouds or the 'Arab Spring' which are to blame.



With a global footprint, patchy training, often non-existent vetting procedures and tens of thousands of employees working online from home and in overseas call centres, there are many opportunities for fraudsters to actively

target the industry. In addition travel fraud can be an enabler for other crimes.

Barry Gooch explains: "There are tens of billions of pounds tied up in thousands of companies, many of them are small operations which struggle to survive on slim margins and with limited funds to invest in counter fraud measures. The fraudsters consider them easy pickings."

But fraudsters are not just targeting travel businesses.

"Payment, credit card and ticket fraud are growing issues within the sector with travellers and the banks ultimately bearing the cost. The evidence shows that with often non-existent staff checks and little in the way of regulation, criminals can easily get jobs in call centres or work from home.

"They commit the fraud then move on quickly, remaining under the radar and repeating the same crimes over and over again."

PROFIT is working with the NFIB to produce, industry guidelines which will help design-out fraud by improving internal procedures, training and vetting. There is also a desire to improve data sharing across the public and private sectors.

"The only way we will truly get a hold on fraud is to streamline data-sharing across all industries and sectors. The NFIB has made a good start with its data matching projects and things are moving in the right direction."

STATATTACK

- ◆ In November Action Fraud received a total 6,949 reports with a total value of £52.9 million.
- ◆ Online shopping remained the most reported crime and other financial investment the highest value.
- ◆ The NFIB distributed 413 Action Fraud crime reports to 30 ACPO and ACPOs forces, valued at £4.1 million.
- ◆ NFIB also Issued 8 intelligence summaries to Interpol, GMP, FSA, Lancashire Police, MPS and CoLP. Additionally, it issued seven fraud alerts to UK Payments, Interpol, BBA and CIFAS, and one to more than 800 firms regarding home reversion loans.
- ◆ Action Fraud crime reports linked to 3,690 *Know Fraud* networks containing 66,324 reports.

Partners against crime – CIFAS and NFIB

NFIB expertise combined with CIFAS data led to the arrest of a woman who hi-jacked the identity of her brother-in-law's wife and then used a counterfeit foreign passport to get a job in a primary school.

The Metropolitan Police's Operation Amberhill and the Criminal Records Bureau (CRB) uncovered how a counterfeit French passport had been used in an application to

a teaching agency which had processed the vetting certificate and placed the individual in the school.

True identity

Following a request from the investigation team a search on the NFIB Know Fraud system pin-pointed a CIFAS case with a key address linked to the individual, enabling the true identity of the suspect to be confirmed and an arrest to be made.