

HEADLINE NEWS

Delivery, delivery, delivery

The NFIB's number one priority can now be summed up in one word: Delivery.

The second quarter of 2012 and beyond is all about the NFIB delivering the products and services partner agencies need to combat economic crime in their jurisdictions.

At the same time the team is focusing on expanding and enhancing its own crime prevention work, particularly in the arena of

cyber crime and technological take-downs.

In the first quarter the NFIB developed and disseminated 32 alerts, including one to all forces regarding credit card skimming and several international alerts on bank accounts used in boiler room fraud. A further 29 assessed intelligence products, including summaries to the FSA regarding land banking were also circulated.

More than 1,300 crime reports were also distributed, with 95% of ACPO forces and 38%

of ACPOS forces handed information. In March alone, crime packages covering a total loss of £15.4 million were developed.

Crime prevention is also a key focus for the NFIB. Between January and March, analysts completed disruption requests from several partner agencies, closing down:

- 591 telephone numbers
- 119 websites
- 10 foreign currency exchange accounts.

Plans in action

Behind these numbers are real life stories of how the NFIB is shutting down criminal enterprises. The Cyber Co-ordination and Development team recently identified two websites set up to appear as legitimate sellers of tickets for high profile music concerts.

Using a *denial of service attack* (DDOS) the administrator closed down the legitimate ticket selling sites, and 'ad-listed' the bogus sites to ensure they appeared high on search engine hit lists. The NFIB Cyber team moved quickly, suspending the fraudulent website and related phone number within 24 hours and alerting the artist's record label to the crime.

Analysts also identified the merchant service companies who had already processed transactions, warning them of the criminal threat and providing crime prevention advice. Just one example of how swift and focussed NFIB disruption activity can stop fraudsters in their tracks.

Getting to grips with fraud:

Hear from Anne Sheedy, CIFAS Head of Financial Crime and Strategic Alliances

New National Tasking

Counter fraud agencies and law enforcement from across the country were recently brought together for the first NFIB national tasking.

The ten ACPO Operational Command Units (ROCUs), SOCA, SFO, FSA and HMRC came to the City to share intelligence and identify new forms of fraud disruption and prevention.

The NFIB team provided an overview of the current threat areas and agreed to provide assistance on issues linked to serious organised crime from the Yorkshire and Humber, North West and South Eastern regions, and the FSA.

Regional intelligence has been run through the Know Fraud system and is being assessed by analysts ahead of the meeting.

The Director of the NFIB, Det Supt David Clark, said:

"Working in silos is no longer an option if we want to get to grips with a crime that is costing the country tens of billions. These national tasking meetings will enable us to share knowledge and information like never before."

Message from the Director of the NFIB, Det Supt Dave Clark



Time seems to be racing by. The NFIB continues to spread its impact and reach across the UK, further evolving into the central hub for all fraud intelligence and co-ordinating

the national fight against fraud related organised crime gangs. An important part of this jigsaw was fitted into place in March when we hosted the first National Tasking of NFIB resources (see front page).

A major priority for me is forging even closer ties with key partners from different sectors. The success of this is borne out by UK Payments and the Charities Commission providing us with new secondees for bespoke pieces of work, and one of our analysts being seconded to work with the British Recorded Music Industry (BPI) to work with them. In the upcoming weeks I will be sitting on

a panel at an event hosted by the British Bankers Association (BBA) Olympic sub-group, and setting-up quarterly NFIB stakeholder breakfast workshops. And never far from my thoughts is the work of the NFIB in the build up towards the Economic Crime Command and the National Crime Agency.

Looking forwards, the NFIB has a number of significant challenges on the horizon. A priority for us will be the national roll-out of Action Fraud, and working with ACPO regions to place NFIB intelligence officers in all the Regional Intelligence Units (RIUs). This work fits in with the City of London Police's wider

project of establishing a national economic crime capability, designed to counter what the NFA recently valued as a £73 billion area of criminality. This is money the country could ill-afford to be losing at the best of times.

We should also not forget the upcoming European football championships and, of course, the Olympic Games. These are great summer events to be enjoyed by the nation. The reality is they will also be targeted, in some shape or form, by fraudsters and it is up to all of us to work together to limit their opportunities and ensure offenders quickly feel the full force of the law.

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 Pete O'Doherty: 020 7601 6806
peter.odoherty@cityoflondon.police.uk

Products and Outputs:

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



Action Fraud update from the NFA



The launch of the Devil's in Your Details campaign has been Action Fraud's key milestones in the past 3 months along with the introduction of a new website and branding.

An online campaign is raising awareness of the importance of keeping personal information safe, targeting 35 to 55 year old women and 18 to 26 year old men and women – two key segments within the National Fraud Segmentation. Launched in March, the campaign featured two YouTube videos and a Facebook app that directed people to Action

Fraud for more information. It has been very successful, reaching over 350,000 views of the videos, surpassing the campaign target, and is well on its way to meeting targets for the app. The Action Fraud site has seen over 50% more traffic over the duration of the campaign.

With the introduction of cyber reporting and a new police address, a review was undertaken to ensure consumer interface of Action Fraud was fit for purpose. Consumer testing showed that customers responded positively to the name but wanted a more authoritative look and feel to the branding and website. Phase 1 changes

to the website have now been completed. Phase 2 has now begun which will incorporate a review of the information architecture and content of the site.

On fraud reporting, the past 6 months has seen an additional 12 fraud types now being reported through Action Fraud to the NFIB; this includes cyber crimes such as hacking and 'Denial of Service' and frauds such as ticket fraud and mandate fraud. The service is now undergoing a structural upgrade to match the requirements needed to deliver the service growth, availability and customer reach planned.

NFIB: Actions speaking louder than words

The NFIB is divided into three commands, each with their own objectives but all operating with the same aim: delivering the services and products needed by partner agencies and providing an improved and effective performance to tackle organised fraudsters.

1 New business, projects and concepts – Richard Waight

We continue to extend our reach into the public, private and charity sectors, forging new relationships with the airline industry, charity commission and the National Anti-Fraud Network.

Phase 1 of the NFIB contribution to an Identity Assurance Programme has launched with new analytical and research support in place at the Bureau for the 16 weeks of this key project stage. In partnership with Amberhill at the Metropolitan Police and initially the DVLA, our objective is to provide a greater understanding of the threat false and fraudulent identities pose whilst creating opportunities to tackle those profiting from criminal impersonation.

Continuous system improvement is essential to the Business Development Team delivering a better counter fraud and cyber response. Cross agency engagement with partners i.e. Action Fraud and the OCPB National Coordinators Office is complimenting the work of our internal user group by defining an up-to-date system user requirement. Recent work includes developing the ability to capture and understand 'Grant Fraud', a crime that exposes the UK to losses approaching £500m per year.

2 Crime and Intelligence Operations – Pete O'Doherty

In the next few months, we will be placing NFIB regional intelligence officers to operate from within the ten Regional Intelligence Units across England Wales.

These intelligence officers will act as regional arms of the NFIB, enhancing the ability to ingest, assess and disseminate intelligence across the UK. This will ensure that local police forces and other regional policing structures such as Regional Asset Recovery Teams and Regional Organised Crime Units can easily access the Know Fraud system to assist in prevention, disruption and enforcement capabilities for all crime where fraud is either a primary or secondary method.

In the last quarter the NFIB, in conjunction with the NFA, provided an assessment of the top 20 victim locations by Police Force jurisdiction. It found 25% found of fraud victims are within the Met Police area and the rest distributed evenly across the country.

We also produced three monthly threat updates that were circulated across law enforcement and industry, providing a richer tactical perspective in preventing and disrupting key fraud types and trends.

3 Products and Outputs – Steve Prideaux

The priority for the Outputs team is ensuring the right products are reaching the right people at the right time.

This includes assessing the current disseminations and how we seek feedback from the recipients. We are in the process of introducing a new programme that will see an enhanced portfolio of outputs with a more efficient process of delivery to our partners. A part of this process includes a pilot with the retail industry around their phishing tools and with the British Banking Association (BBA) utilising their existing alerts system.

Our role coordinating the response to cyber crime continues to develop, with the NFIB being a part of public sector briefings and industry forums, and working across the cyber intelligence community to produce national strategic intelligence reporting. Notable successes in the field include shutting down an airline ticketing fraud, facilitated by seven websites, three bank accounts, five VOIP numbers and five companies with registered addresses across the UK. Rapid action by the NFIB saw all of them closed and alerts issued to the BBA and UK Payments on the suspects and their activities.

21,937

victims in NFIB ingested reports from CIFAS, UK Payments + Action Fraud (March)

40%

cyber related reporting of all Action Fraud reports and crime-related information (first quarter)

7%

of all Action Fraud recorded crime comes from computer misuse (March)

In this edition we speak with Anne Sheedy, CIFAS Head of Financial Crime and Strategic Alliances



“Each arrest presents an opportunity to obtain knowledge that can be used to prevent further frauds”

If we are serious about getting to grips with fraud we need to be smarter about what fraud the police investigate. We then need to listen when detectives tell us about what they have uncovered.

This is the message from Anne Sheedy, Head of Financial Crime and Strategic Intelligence at CIFAS, who sees the arrest of these criminals as just the start, with each one presenting an opportunity to obtain knowledge that can be used to prevent further frauds. Anne also stresses the need for more problem-orientated policing in respect of high volume fraud.

“The police have been hugely successful using this approach with other types of crime and there is no reason why, now that we have the NFIB, they could not be just as successful using this strategy to tackle volume fraud.”

Opportunity

“It is only the police that can actually get hold of the fraudsters and find out exactly how they commit the crime and why they are doing it. Any arrest and interview presents the opportunity to learn more about a particular offence; information that can then be fed back to the fraud prevention community, via the



Data sharing is essential

NFIB. With this information we can then work together to tackle the key conditions that give rise to the fraud.”

Facilitate investigation

CIFAS has been involved in the NFIB project since 2009 and feeds its members’ fraud data into the Know Fraud System daily. CIFAS makes these crimes available to the NFIB to facilitate investigation against the criminals responsible. As one of its main partners they are particularly well-placed to deliver a progress report.

“The NFIB has brought together a number of very important data sets and has begun to put structures in place for a greater number of fraud investigations to be undertaken.

“For this to succeed the NFIB needs forces to investigate packages and to have good end-to-end processes in place to capture and analyse the results. Without these processes more investigations will not help solve the problem.

“This is a significant challenge, but the NFIB is definitely heading in the right direction. CIFAS continues to support the NFIB and believes it can make a real difference. I would like to see it succeed with this approach and see more organisations share data consistently so we can make it a truly national agency.”

NEWSINBRIEF

The NFIB assisted in getting a pair of barristers arrested for advertising their professional services, even though they had been struck off by the Bar Council. A crime report was disseminated to Sussex Police providing them with an action plan to identify further possible victims. The Law Society and the Bar Council were sent the evidence of disbarment, signed by the Minister of Justice and we are currently waiting news on future charges.

NFIB and BPI – partners against crime

Secondees form an integral part of the NFIB, using their skill sets and sharing their expertise to make a better, more innovative agency. But it is not all one-way traffic.

In April an NFIB analyst was seconded to the BPI (British Recorded Music Industry) for a year to work within the Anti Piracy Unit, focusing on gathering intelligence relating to the unauthorised distribution of BPI members’ copyrighted material.

The analyst will be preparing intelligence packages to be used by the BPI or disseminated to the relevant law enforcement agencies.

Collating intelligence

They will also lead on collating intelligence relating to Organised Crime Groups (OCGs) involved in music piracy as well as enhancing the profile of music piracy by participating in relevant crime groups.

CIFAS is a not-for-profit membership association representing the private and public sectors. Its 260 members share information about identified frauds in the fight to prevent further offences.