

Fighting fraud in 2012/13

A message from the NFA's Chief Executive, Stephen Harrison

I am pleased to say that the NFA's Business Plan has now been approved for the 2012/13 financial year.

Developed to fit into the context set by national strategies such as *Fighting Fraud Together*, *The UK Cyber Security Strategy* and *Local to Global: Reducing the Risk from Organised Crime*, our business plan has been produced following discussion with our stakeholders to create objectives that will make a significant impact on the counter fraud agenda.

This financial year, we will:

- Raise awareness of fraud among individuals and the private, voluntary and public sectors,

launching targeted initiatives to help these groups self-protect (see [page 3](#))

- Improve fraud intelligence sharing by overseeing the creation of an Intelligence Sharing Roadmap, providing a framework to encourage the exchange of intelligence both within and across sectors
- Identify the common factors that are used to facilitate fraud, creating prevention plans to reduce fraudsters' abuse of these enablers (see [page 6](#))
- Improve our measurement of the fraud problem and develop more rigorous measures of performance

across all areas of fraud awareness, prevention and enforcement

- Deliver the Action Fraud service, making it the single point for all fraud and internet crime reporting, and to improve the quality of victims' experience (see [page 9](#))
- Support the implementation of arrangements by the local authority sector to deliver the *Fighting Fraud Locally* strategy (see [page 7](#))

To achieve these goals, we will continue to lead and coordinate Fighting Fraud Together, working in close partnership with the public, private and voluntary sectors to make our country more resilient and less



Stephen Harrison

damaged by fraud.

I would like to thank these partners for continuing to support the work of the NFA and Fighting Fraud Together, and I look forward to working towards our objectives over the next year.

A copy of the NFA's 2012/13 Business Plan will be published on the [NFA website](#)

NFA highlights in 2011/12

We have recently published our annual report and accounts for the business year 2011/12. It is available on the [NFA website](#), but here's a quick reminder of some of our achievements over the last year:

Annual Fraud Indicator

Our most comprehensive analysis yet of the scale of fraud in the UK – an estimated £73 billion annual loss

Fighting Fraud Locally

Developed and published the first ever strategy to tackle the estimated £2.2 billion fraud loss to local government (see update on [page 7](#))

The Devil's in Your Details

A groundbreaking, targeted communications campaign in partnership with the financial services and telecoms sectors to raise awareness of the importance of protecting personal information (see results on [page 4](#))

Fighting Fraud Together

Published the first ever national strategy for reducing fraud, as a four year joint commitment between the public sector, private sector, law enforcement and voluntary sector

Central Government Anti-Fraud Culture

Produced an e-learning tool and worked with the cross government Fraud, Error & Debt taskforce to embed a zero tolerance approach to fraud in every central government department

Action Fraud

Expanded and enhanced the service for reporting fraud and now internet crime, taking 50,000 crime reports and 140,000 calls (with a 97% satisfaction score)

Insurance Fraud Enforcement Department

Worked with the City of London Police & Association of British Insurers to secure private sector funding for this dedicated police unit to investigate insurance fraud

What makes small businesses vulnerable to fraud and internet crime?

Following the success of the fraud segmentation for individuals, the NFA and the Department for Business, Innovation and Skills have developed a segmentation of small and medium-sized businesses (SMEs), exploring their attitudes, behaviours and risk levels in relation to fraud and internet crime.

We have identified six distinct segments which we and our partners will use to develop a greater insight and understanding of the vulnerabilities that smaller businesses face. In turn, we will coordinate awareness raising and prevention activities to target the different segments and measurably increase

their ability to protect themselves from fraud.

SMEs are integral to the future growth of the UK economy and helping them retain revenue is central to this agenda. Traditionally, SME fraud risks and online security have not been given as much attention as other sectors so the segmentation provides an innovative way of understanding and focusing on their needs.

The SME segmentation will be published shortly but in the meantime, some of the top-line observations are:

- Online trading increases SMEs' experience of fraud and internet crime
- Once a business' annual turnover reaches £20 million, there is a marked spike in fraud risk
- Some SME sectors are more prone to fraud and internet crime than others
- The more employees a business has, the greater the fraud and internet crime risk

Next steps

As well as using the segmentation to inform prevention activity, we will explain the segmentation's findings to interested organisations and add insight on SME needs.

We will also help partners apply the results to their own data to improve their understanding of SME risk and help them create targeted messages and activities that will keep their SME customers safer from fraud and online crime.

If you would like further information on the SME Segmentation, get in touch with Alex Daley at alex.daley@nfa.gsi.gov.uk



The Devil's in Your Details: The Results

70% would change how they protect personal information.

The groundbreaking Devil's in Your Details campaign used targeted YouTube videos and a Facebook application to highlight the importance of keeping personal information secure.

It was aimed at two groups highlighted by the NFA fraud segmentation as being particularly at risk – younger people aged 18-25 and women aged 36-55.

Post campaign research has shown its success in reaching these audiences and 70% said they would take more proactive steps to protect themselves from fraud after seeing the videos.

Action Fraud also received a 55% increase in unique website visitors during the campaign and continues to

have more website visitors, spending longer on the site, than last year.

We, and our private sector partners, are now developing proposals for more targeted behaviour change campaigns focused on online security as well as a separate campaign aimed at very vulnerable adults.

Our awareness and behaviour change activities are overseen by a steering group comprising public and private sector partners with responsibility for coordinating and maximising the impact of fraud prevention initiatives. It reports to the Economic Crime Prevention Group which oversees awareness and prevention work under *Fighting Fraud Together*.



The videos and further information on the campaign can be viewed at www.actionfraud.police.uk/thedevilsinyourdetails

Get Safe Online Week

Get Safe Online Week 2012
will be held from 22 – 26 October.

The objective is to get as many people as possible across the UK to pass on online safety tips to friends, family, colleagues, neighbours, vulnerable people... in fact anyone who could benefit from even the most seemingly insignificant advice. The theme – hard hitting and intuitive – will be 'Click & Tell'.

Get Safe Online Week will encompass a roadshow visiting five major UK cities, engaging with the public in high traffic areas such as shopping centres, railway stations, leisure centres and other public locations. The message will also be cascaded

by Get Safe Online's partners as well as other interested parties, and a number of well-known personalities are being recruited to endorse the message.

To find out more, including how you can participate, please visit www.getsafeonline.org

**GET
SAFE
ONLINE**.org

WEEK

22nd-26th
Oct 2012

Tackling fraud enablers

The NFA and SOCA have started a project to map and identify the key enabling factors that facilitate the most harmful fraud types.

Tackling an enabler often disrupts a wider range of frauds and is more effective than chasing individual occurrences. Fraudsters can use common methodologies or tools (such as for communication or transferring money) to facilitate their crimes. Reducing the exploitation of an enabler can therefore have far reaching knock-on effects.

We want this project to:

- Reduce the use of enabling instruments and organisations by fraudsters
- Reduce the capability of fraudsters to communicate with their victims
- Make it harder for fraudsters to receive money from their victims

Working with partners from across the counter fraud community, we are mapping high priority fraud types to identify the common enablers.

These fraud types include:

- Online Shopping & Auction Fraud
- Cheque, Plastic Card & Online Bank Account Fraud
- Advance Fee Fraud
- Share Sale & Boiler Room Fraud
- Dating Scams

We will then use the analysis to produce proactive prevention plans to reduce the harm caused by enablers.

By the spring of 2013, we will collate the experience and information gathered through the project to:

- Produce a fraud prevention manual to contain the variety of legal powers and proven methods to tackle fraud enablers and provide common solutions for reducing fraud
- Provide a central repository of fraud typologies detailing how frauds are committed

When complete, these will be shared with the counter fraud community on a secure basis.



New fraud prevention tools and guidance

Two new pieces of guidance have been produced for the charity sector, focusing on fraud prevention within charities and how the public can donate safely. These materials have now been published and are hosted on the Fraud Advisory Panel's (FAP) website at

www.fraudadvisorypanel.org

The FAP have also issued two new fraud factsheets - *An introduction to fraud investigations* for businesses and *Fraud and charities: the role of internal audit*. These too can be found on the FAP website.

Fighting Fraud Locally Update

Fighting Fraud Locally (FFL) is the counter fraud strategy developed for local government, by local government. Over the last few months, we have been working with our partners and stakeholders to help to implement the recommendations of the strategy:

The counter fraud e-learning training course referred to in the last edition of Fraud Focus has been circulated to local authority chief executives

The course is designed to help councils raise levels of awareness among staff and improve detection rates.

Collation of examples of anti-fraud best practice also continues

The NFA is working with local authorities to enhance the guidance that is already available on the TISonline Good Practice Bank. The information is helping local authorities implement tried and tested ways to make savings from reducing fraud.

If you are interested in any of the recommendations put forward by the strategy or in working with the FFL Oversight Board, please email [Mosi Akenzua](mailto:Akenzua@nfa.gsi.gov.uk) (Omosede. Akenzua@nfa.gsi.gov.uk)

For a full copy of Fighting Fraud Locally, visit the [NFA website](http://www.nfa.gov.uk). Online fraud resources for local authorities can be found at www.tisonline.net

**FIGHTING
F R A U D
L O C A L L Y**

Building the National Crime Agency

The Queen's Speech to Parliament on 9th May saw the inclusion of the Crime and Courts Bill which will establish the National Crime Agency (NCA) as the centrepiece of the reformed policing landscape charged with combating organised and serious crime in the UK.

The Bill lays out the intended functions and powers of the NCA and is currently progressing through the House of Lords, for the planned establishment of the agency in 2013.

The NCA will consist of four operational commands, each dedicated to tackling one of the following areas:

- organised crime
- border policing
- economic crime
- child exploitation

These commands will be able to call on support from a national cyber crime unit and an intelligence hub housed within the NCA.

The NFA is heavily involved in planning for economic crime functions of the NCA: we have members seconded to the project team and chair the Economic Crime Prevention Group (ECPG), a delivery group feeding into the Economic Crime Coordination Board (precursor to the NCA's Economic Crime Command).

When operational, the Economic Crime Command will be responsible for drawing together other agencies and coordinating the UK's response to combating economic crime.

The NFA is also working with a number of partners to lay the foundations for the strategic intelligence capability of the NCA, producing a strategic assessment to improve understanding of the scale and nature of all economic crime threats.



To view a copy of the Crime and Courts Bill and see its current status in Parliament, visit

<http://services.parliament.uk/bills/2012-13/crimeandcourts.html>

The roll out of Action Fraud to police forces is underway!

Action Fraud is to become the single place where non-emergency reports of fraud and internet crime are captured in England and Wales.

This means that by April 2013, all reports that were previously processed by police forces will instead be taken by Action Fraud, before being sent on to the National Fraud Intelligence Bureau (NFIB).

This centralisation of fraud reporting will enhance the intelligence picture and allow for reports from across the country to be directed by the NFIB to the most appropriate place.

An event hosted by the NFA and City of London Police in early June brought together police forces to discuss how the Action Fraud service will be used to capture and process all reports of fraud and internet crime. A regional roll out plan is being agreed and the Action Fraud team and the NFIB will brief force planning teams in sequence on what needs to be done to achieve an efficient implementation of the service.

This will involve the training of operational police officers and support staff throughout England and Wales to ensure that

communities and business sectors are aware of the changes being made to reporting of fraud.

Discussions are also underway regarding the roll out of Action Fraud in Scotland and Northern Ireland too.

Five pilot police forces – City of London, Leicestershire, Cumbria, Kent and Greater Manchester – have already begun to use the Action Fraud service to process reports of fraud and internet crime. Valuable lessons have been learned through their experience and we are very grateful to those forces assisting.

National Fraud Intelligence Bureau update: an expanded and enhanced service

The National Fraud Intelligence Bureau (NFIB) continues to expand its operation and improve the products and services it delivers for partner agencies.

In recent months there has been a stream of new recruits arriving to work within the NFIB's three command units: New Business, Projects and Concepts; Crime and Intelligence Operations; Products and Outputs. A number of secondees have also joined the team, including representatives from CIFAS, The British Recorded Music Industry and Financial Fraud Action UK.

This enlarged team is providing an enhanced service to law enforcement, the public and private sectors, and other key partners across industry,

continually driving forward the quality and volume of crime and intelligence products. In May alone, the NFIB developed and disseminated 449 crime packages, 28 tactical intelligence products and 112 alerts via a new key partnership with the British Bankers' Association.

The Cyber Crime Team is an integral part of this operation, sitting within the Products and Outputs command unit. Cyber reports make up 46% of all Action Fraud reporting and recent trends identified include the hacking of

social media and email accounts. The NFIB has also now hosted two national tasking meetings in the City of London, giving local, regional and national law enforcement teams the opportunity to share intelligence and request assistance with their own investigations.

**National Fraud
Intelligence Bureau**


Fraud Alerts

The NFIB has recently issued alerts on the dangers of buying carbon credits from cold callers and a 'ransomware' scam that misuses NFIB and Action Fraud branding to dupe people into paying to have their computers unlocked.

For more information and to keep up to date with other Fraud Alerts, please visit <http://www.nfib.police.uk/fraud-alerts.html>