

HEADLINE NEWS

Online and phonline fraud disruption sees NFIB save millions

A major NFIB campaign to shut down the websites, email addresses and telephone numbers fuelling much of today's fraud has already stopped at least £7 million being lost to fraudsters in the last 2 months.

During September and October the NFIB has suspended **12 websites, 179 telephone**

numbers and 155 email accounts, which were enabling organised crime gangs to target and steal from individuals and the public and private sector.

The threat of personal information being stolen through phishing e-mails is now being tackled in partnership with UK Payments Administration (UKPA). 978 emails have been passed to the UKPA-run www.banksafeonline.org.uk, for suspension.

NFIB analysis has shown how fraudsters can be resilient, with the ability to quickly reinvent their criminal operation.

Re-creation of websites

In recent months the NFIB has identified fraudsters who are reproducing suspended websites with a similar sounding name and/or signing up for new phone numbers with a different provider. The public is told this has been done for 'technical reasons'.

The NFIB has moved quickly to block this new line of attack.

People who visit certain suspended websites are now being automatically redirected to an alert page on the NFIB website. This provides users with a fraud warning and directs people who believe they have been a victim of fraud to Action Fraud. For legal reasons some ISPs have not been able to comply with the redirection but overall the system is making a positive impact.

Click on www.saltzmankramer.com to see how the NFIB is unmasking the criminal practices of online fraudsters.

The NFIB is taking a similar approach with phone numbers. Once a number is identified as part of a fraudulent operation, the NFIB looks to suspend the line and leave a message to callers explaining exactly why, along with details on how to contact Action Fraud. The aim is to stop the same victim being repeatedly conned and to protect any new, prospective victims.

To hear an NFIB message call:
020 3318 1273 or **020 3318 1274**

NFIB launching response to the threat of cyber crime

In November, the NFIB and Action Fraud will launch a response to financially-motivated cyber crime and computer enabled fraud.

Phase 1 will see the introduction of a system able to deliver fast-time response to the threat of phishing emails that often seek to extract people's personal information for use in fraud. This will be followed by the launch of cyber crime reporting and analytical tools.

The threat to the UK from cyberspace (including the internet, wider telecommunications networks and computer systems) has been identified as one of the highest priorities for UK national security over the next five years.

The NFIB and Action Fraud will be part of a close partnership between the Government, industry and the counter-fraud community in delivering a multi-faceted approach to the

cyber threat, providing a core front line reporting and analytical function.

Deputy Director of the NFIB, Richard Waight, said: "When you consider the UK consumer already spends £4.4 billion shopping online there is no surprise this is also our largest area of fraud reporting. This new resource will play a key role in making cyberspace a safer place to do business."

Message from Tony Crampton



Welcome to our new look NFIB newsletter to keep you fully updated on how the Bureau is helping to combat national and international fraud. The fraud landscape is constantly evolving

for those good and bad, and so must the NFIB. I hope you enjoy reading about how we are responding to this ever changing challenge.

The NFIB is already demonstrating its commitment to the UK's strategic plan for reducing fraud, *Fighting Fraud Together* and its core objectives to be **tougher** on fraudsters by **disrupting** and **punishing** them more efficiently and effectively.

In the last couple of months we have successfully focused on reducing harm from

an early stage through the suspension of the key enablers that facilitate fraud – websites, emails and phone numbers.

We are also increasing our public and private sector engagement, delivering on a number of initiatives. Our work with the Department for Work and Pensions' Identity Assurance Programme and the launch of our cyber response demonstrates the importance we place on greater online security.

Close ties with UK Payments Administration are also bearing fruit, with the Know

Fraud system finding a high number of links between Action Fraud reports and bank reported information, which is being disseminated to law enforcement.

Looking further afield we are working with SOCA and our US and Canadian partners to counter India-based criminal call centres targeting people on both sides of the Atlantic. An international threat combated with an international response.

Tony Crampton
Director of the NFIB

eNewsletter

NFIB eNewsletter is published quarterly by the National Fraud Intelligence Bureau

Contacts

Director of the NFIB: Det Supt
Tony Crampton: 020 7601 6908
tony.crampton@cityoflondon.police.uk

Deputy Director of the NFIB:
DCI Richard Waight: 020 7601 6916
Richard.waight@cityoflondon.police.uk

Head of National Fraud Desk:
DI Amanda Lowe: 020 7601 6977
Amanda.lowe@cityoflondon.police.uk

Communications: Harry Watkinson:
020 7601 2015
harry.watkinson@cityoflondon.police.uk



Intelligence and information for the counter fraud community and beyond

The power of the Know Fraud system and the potency within Action Fraud reports are now well harnessed. During the last quarter the NFIB circulated 71 themed intelligence products alerting law enforcement, the wider counter fraud community and the general public.

These reports included:

- The public alerted to fraudsters offering tickets online to Coldplay's sell-out tour.
- City of London Police, Surrey Police, Durham Constabulary and the FSA

received an intelligence summary about a fraudulent land banking scheme

- Banks via UKPA were sent a warning of commodities being sold by bogus brokers
- Dissemination of an intelligence network alerted the MPS to a property rental fraud
- CIFAS members were alerted to a payment diversion fraud. Victim companies received false invoices purporting to represent genuine suppliers and instructions to change account details for future payments

- A networked series of fraudulent insurance claims was sent to West Mercia
- A bank has launched an investigation after being alerted to Green Carbon Credits potentially linked to a boiler room fraud
- Intelligence from the NHS linking an organised crime gang involved in theft, burglary and payment card fraud was sent to West Midlands Police
- Kent Police was informed of two suspects linked to card not present fraud suspected of other crimes in the Kent area.

Charity bag fraud: major strike

Charity bag fraud targets the people working to help some of the most vulnerable in society both at home and abroad. In the last year, tens of millions of pounds worth of second hand clothes destined for charities have been stolen off the streets and sold in shops across Eastern Europe.

In September, intelligence from the NFIB Charity Fraud Desk led the City of London Police to make a major strike against an organised crime gang suspected of stealing charity bags worth hundreds of thousands of pounds.

During an early morning raid at an Essex depot, four men were arrested and £20,000 in cash was seized, along with charity bags and criminal evidence. This operation generated considerable media interest, featuring prominently in *The Times*, *BBC One Show* and *BBC London TV news*.

Importantly the charity desk has noticed that some gangs are altering their approach to

avoid getting caught. When this crime was first reported as a problem, the gangs posed as either legitimate charities or completely fake ones. But in recent weeks a new strategy is emerging, with bags and flyers being produced giving the impression the cause is charitable but does not mention a charity at all. This could be considered as fraud by false representation but could be difficult to prove.

Investigations have also provided further evidence of the links between the Lithuanian organised crime gangs involved in charity bag fraud and other crimes that include driving insurance fraud, fuel theft and human trafficking.



CoLP officer asking questions during the early morning operation

The Fundraising Standards Board held a meeting in September to discuss the problem of charity bag fraud. Nick Hurd, the Minister for Civil Society was the keynote speaker and DI Amanda Lowe, who heads up the National Fraud Desk, provided an update on the work of the NFIB and City of London Police.

Hajj fraud

In November, hundreds of UK citizens are likely to find their dreams of making a once in a life-time pilgrimage to Mecca damaged or destroyed by fraudsters disguised as travel agents.

For the second year running, the NFIB and City of London Police are working with the Muslim community to raise awareness of Hajj fraud and encourage victims to report the crime to Action Fraud.

The Muslim Council for Britain's Deputy Secretary General, Dr Shuja Shafi, said:



"Prospective Hajjis are urged to remain careful and vigilant and do due diligence by checking that their tour operator is a current ATOL holder. The MCB also encourages Muslims to report immediately to the police any fraudulent activity."

Go to www.nfib.police.uk, for a Hajj fraud leaflet available in seven languages.

International investigations

More often, NFIB intelligence is being used by law enforcement operating far beyond these shores to disrupt frauds committed within or running through their jurisdiction.

In September the NFIB uncovered evidence of a major share purchase fraud using a network of national and international bank accounts to launder stolen money. In response, analysts circulated intelligence summaries via Interpol to law enforcement in Hong Kong, Spain and Italy alerting them to accounts registered within their borders suspected of facilitating the fraud.

As a result, Hong Kong Police has launched its own money laundering investigation. At the same time details of addresses linked to the criminal network were sent to UK police forces, with local intelligence checks being fed back into a wider City of London Police investigation.

Boiler room fraud

In separate cases NFIB intelligence has directed Seychelles Police to a bank account suspected of being used by a boiler room company and alerted Dubai Police to a possible boiler room fraud operating on their patch.

Partners against crime

During August and September, the NFIB assessed more than 7,500 Action Fraud reports. From this data, 672 crime reports containing total losses of more than £19 million were disseminated to UK police forces.

The most prevalent of these were:

Online shopping	278
Other Consumer Non Investment	108
Other financial investment	75
Other advance fee frauds	62

And the main recipients of crime reports were:

MPS	271
Trading Standards, Merseyside and City of London Police	47
Greater Manchester Police	43
Sussex Police	36

Notable and continuing trends include growing cases of companies claiming to sell voluntary and government funded carbon credits, money transfer services being used as a key enabler of fraud and voucher based e-money products being used in loan lender fraud.

A new form of reporting

A new Crime Related Information tool has been developed to enable the public and small businesses through Action Fraud to

report information that does not constitute a crime. This has already become an invaluable data source for the NFIB in the assessment of crimes for national distribution and intelligence development. The top five information categories are banking and credit industry fraud, computer software service fraud, inheritance fraud information and lottery scams.

Action Fraud in forces

Leicestershire Police is the latest force to join the pilot and refer all reports of fraud to Action Fraud. Learning from the City of London Police pilot is already being incorporated into the reporting tool. For example, corporate bodies and financial institutions revealed problems in reporting large corporate frauds via the Action Fraud web reporting tool. System and process development is underway to address this.

Making sure police forces have the training and support to use Action Fraud and understand their role and responsibilities is critical to the success of both the pilot programme and the national roll out. The NFIB and Action Fraud are currently working on an

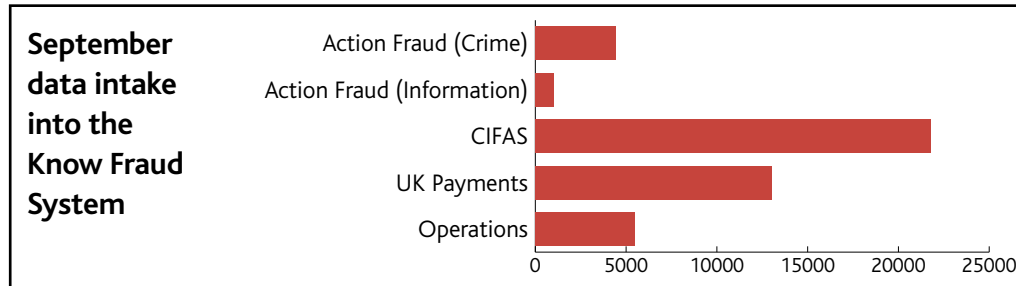


e-learning training package to help forces that are preparing to change the way they handle reports of fraud.

Feedback

The NFIB has just finished collecting feedback from those forces which have received Action Fraud-generated crime reports. But we will not be stopping here. Feedback from all our partners is essential to the improvement of our service. The information you provide is invaluable. It enables us to better understand what you want so we can provide the products that best fit your needs.

To provide feedback please contact DI Amanda Lowe & DCI John Osibote (see page 2 for contact details). Please give as much information as possible on the quality of crimes disseminated to you, operational learning gained from investigations and any other relevant information.



Specialist police unit to tackle insurance fraud

A new specialist police unit to tackle insurance fraud is being set-up in January.

Paid for by the insurance industry and housed and run by the City of London Police, the Insurance Fraud Enforcement Department (IFED) will act with operational independence to combat a crime valued at £3 billion per year.

By working with the NFIB and drawing on its intelligence and expertise, the unit will be capable of bringing to justice hundreds of offenders each year. It will also benefit from the City of London Police's position as national lead force for fraud and forge close ties with UK law enforcement and the insurance industry.

Ahead of the launch the NFIB is finalising the General Insurance Threat Assessment for publication in November. As well as reporting on the problem, the recommendations will assist direction of IFED's enforcement response. Special thanks to RBS Insurance for seconding one of their team to us in support of this activity.