ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

National Fraud Intelligence Bureau

City of London Police

eNewsletter

DECEMBER 2014

HEADLINE NEWS

Action Fraud specialist advisers now available to the public through social media

Action Fraud's specialist advisers are now able to offer help, advice and support on fraud and cyber crime through Facebook and Twitter.

This new integration allows members of the public to ask questions and receive help and support previously only available by calling the 0300 123 2040 number or chatting to advisers online via www.actionfraud.police.uk.

Victims can speak to the advisors on Facebook and Twitter pages during the centre's opening hours: Monday to Friday between 9am to 6pm and are reminded not to report through social media. The only way to report fraud and receive a police crime reference number is through the online reporting tool or by calling 0300 123 2040.

Victims can receive help and advice by visiting Facebook (www.facebook.com/actionfraud) or Twitter (www.twitter.com/actionfrauduk) pages and posting a message.

facebook

twitter

Det Supt, Pete O'Doherty welcomes Pauline Smith as the new Head of Action Fraud

With great pleasure I welcome Pauline Smith to the City of London Police as the newly appointed Head of Action Fraud and National Advisor to the Association of Chief Police Officers on police contact management.

Pauline brings with her a wealth of experience and expertise from across policing that will hugely benefit the force, including the programme management and delivery of the first ever single non-emergency number for the police service (101), which she introduced across the UK in 2011.

Pauline Smith, new Head of Action Fraud

Pauline's efforts were also recognised when she was named as European Call Centre Manager of the Year in 2005, the first ever public sector recipient of this prestigious award.

Pauline has been party to the production of a number of landmark studies into police contact management – a critical area of policing; including the National Call Handling Standards and more recently has written the National Contact Management Strategy and Interactive National Contact Management Principles and Practice 2012.

Her work has been acknowledged by Ministers as an innovative approach to underpinning good performance and management.

She was awarded an MBE for her services to policing in the Queen's Birthday Honours in 2008.

NFIB website disruption at its best

In late June this year, the City of London Police control room received a telephone call from a fraud victim, this victim who had also submitted a crime report via Action Fraud, told the control room operator that he was very concerned that his agricultural business and the safety of his family was in jeopardy.

As a result of this information, the control room contacted the National Fraud Intelligence Bureau's (NFIB) cyber prevention and disruptions team.

The victim, who had operated a successful agricultural business for a number of years, had a strong client base and had no need to have a website for his business. The NFIB identified that fraudsters operating from abroad had researched the victim's business and found it to be without a website.

Fake website

Knowing this, fraudsters from abroad constructed a fake website using information suspected to be gathered from Company's House, to put together a convincing website under the name of the victim's agricultural business.

The fraudsters then used the fake website to dupe a number of people, who believed they were dealing with a legitimate company selling agricultural machinery. Unsuspecting victims parted with large amounts of money purchasing what they believed was legitimate machinery.

The fraudsters provided the address of the real company so the goods could be collected. People who believed they had bought a piece of machinery via the internet were then arriving at the real company's premises to collect the goods only to be told there was no record of them buying the machinery.

This situation clearly caused a lot of stress and anxiety for both parties, as both were being scammed – the fraudsters took the money off the unsuspecting victims and created severe reputational risk for the business owner.

Victims gave reports to Action Fraud which were then passed to the NFIB for assessment. Enquiries suggested that the criminals were working abroad with the assumption that they would be free from law enforcement if they weren't resident in the UK.

The NFIB took a multi pronged approach by sending details of fraudulent telephone numbers to the relevant telephone providers and action was taken by them to block the telephone and fax numbers of these fraudsters.

Details of fraudulent bank accounts suspected of being used to launder funds were passed to the appropriate banking institution. A website suspension request was sent to the registrar for immediate termination of services relating to the fraudulent website. The website was removed from the internet in July however the content of the website was activated again by the criminals a short period later following the initial suspension request. A similar domain name was again used by the criminals. NFIB were soon on the case again approaching another registrar and requesting immediate action and termination of the website, the website proved difficult to remove so contact was also made with Google requesting that the domain name was removed from their search engine, another tactic adopted by NFIB to restrict access by unsuspecting victims.

Following extensive efforts with the website providers, eventually the website was removed from the internet. The process was repeated for a third time when the website reappeared; again the NFIB was successful in removing the domain name, putting it out of reach from the criminal and unsuspecting victims.

The victim in this case thanked the NFIB for its efforts to disrupt the website despite the persistence of the fraudsters.

eNewsletter

Contacts

Director of the NFIB:
Det Supt Peter O'Doherty: 020 7601 6806
peter.odoherty@cityoflondon.police.uk

Crime Management:
DCI Matthew Bradford: 020 7601 6894
matthew.bradford@cityoflondon.police.uk

Business Development:
DCI Andy Fyfe: 020 7601 6996
andy.fyfe@cityoflondon.police.uk

Action Fraud:
Pauline Smith: 020 7601 6802
pauline.smith@cityoflondon.police.uk

Editorial:
Merryn Hockaday: 020 7164 8272
merryn.hockaday@cityoflondon.police.uk

Over 29 million Twitter users reached by Christmas campaign

The NFIB and Action Fraud 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 crime.

DCI Matthew Bradford
Crime Management and Development

The new structure of the NFIB's crime and development team has now been embedded into the department. The introduction of focus desks which are aligned to crime types means the information developed by crime reviewers, analysts and researchers is in the right place to build understanding and create crime packages which will maximise action by law enforcement.

Our cyber team are fully engaged with the National Cyber Crime Unit and the regional cyber teams together with our contribution to the Cyber Information Sharing Partnership.

The cyber prevention and disruption team's aim is to disrupt the key enablers used in fraud and to close the gap between reported fraud and cyber fraud, using the crime packages that are viable for investigation. They're working with partners to share data from the Know Fraud database, sharing this information will maximise opportunities to reduce crime and prevent fraud.

Finally, our volume team have worked with the Rugby World Cup organisers to combat the unauthorised selling of tournament tickets for next year's World Cup.

DCI Andy Fyfe
Business Development

Working with the City of London Procurement & IT teams, as well as advisors PricewaterhouseCoopers (PwC), the Business Development Team has recently published its formal invitation to tender for the upgrade of the Know Fraud system and Action Fraud reporting service. We are anticipating formal bids from a number of suppliers and those bids will be assessed over the next two-to-three months.

We have sent our stakeholders a revised version of our information sharing protocol for review. The aim of this is to encourage our data sharing partners to sign up to a singular, consistent information-sharing protocol. This will simplify and help to expedite the process of sharing information, which will help to prevent fraud, in a more efficient and effective way.

We're currently engaging with the Independent Advisory Group (IAG) for City of London Police, asking them to act as 'critical friends' of our Action Fraud service. With tens of thousands of reports made to Action Fraud every month, it's vital we get our service right for victims; any objective feedback is very useful to us to help make improvements if the need is identified.

Stephen Proffitt
Deputy Head of Action Fraud

Action Fraud has had some excellent digital success in the last quarter; the website has experienced some of its highest traffic since its inception in 2010. In November 248,773 people visited the website and 51,588 were returning visitors. It's brilliant that so many people are visiting the site to either report fraud and cyber crime or to find prevention advice.

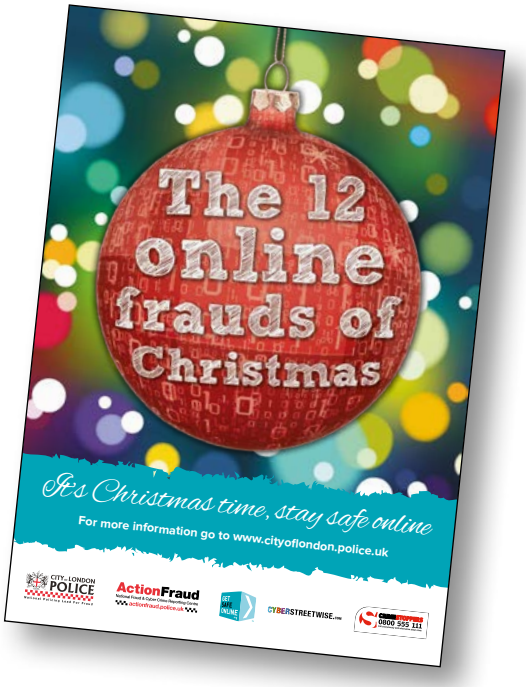
Further to this success, Action Fraud with the City of London Police, launched a national Christmas campaign to raise awareness of online fraud. Leaflets, posters and a social media campaign were produced detailing 12 different types of online fraud that people can typically fall victim to at Christmas time. On Twitter, over 5,000 tweets were sent using the #12frauds hashtag and 29.8 million saw the campaign messages.

The national campaign was rolled out by 38 local police forces and a number of partners, and this stimulated large amounts of regional media coverage, helping to further ingrain the message, that people should be aware of the risks of buying online and the need to report to Action Fraud.

73,804 disruptions and suspensions in the following areas:

- **33,045** telephone
- **20,313** bank accounts
- **447** websites

Data collected: April-September 2014



Action Fraud Alerts go further

Action Fraud and the NFIB have forged a partnership with VisaV, the company which has developed the innovative Neighbourhood Alerts service and which works with 14 police forces and numerous other public sector organisations nationwide.

This system will enable Action Fraud to send fraud and cyber crime prevention advice and alerts using NFIB intelligence on new and emerging threats to approximately 2.5 million people nationwide. These alerts will be propagated via VisaV's growing database of 50,000 Neighbourhood Watch coordinators and another 230,000 individuals.

The impact of this collaboration cannot be underestimated. The NFIB is aware of many new and existing crime types and modus operandi but is sometimes frustrated by its inability to warn the public, especially those people who do not have confidence in accessing the internet or email or who may be hard to reach for other reasons.

Our newly coined 'Action Fraud Alerts' will connect with people in the way which suits them best ; by text message, voicemail , email, or via the 50,000 Neighbourhood Watch coordinators who will be empowered to deliver our messages face-to-face at community meetings across the UK.

The alerts are able to be targeted by the sender and this means that the correct message is sent to the relevant demographic in the correct part of the country, ensuring that people only receive content which is relevant to them.

Micro-site

The accompanying micro-site which will host our Alerts will complement the existing Action Fraud website by providing a library of short, direct preventative alerts and will help us to understand the impact of our messages through direct feedback from recipients and it's able to show a myriad of data – the most important being whether or not the message has been read by the recipient and within what timeframe.

Once the system is up-and-running, we would be happy to take advice from partners on the kind of fraud prevention messages they would like us to be conveying to the public.

Moving forward, VisaV (www.visav.net) hope to expand their service across more UK forces and are signing up thousands of new message recipients each month. As this progresses, our messages will be delivered to more and more people at the right time and through the right method. Keep an eye on our website, www.actionfraud.police.uk for information on how you can sign up to receive real time Action Fraud alerts.

Falling victim to ticket fraud

Earlier this month Action Fraud spoke with a victim of ticket fraud. Amongst others, this 28-year-old woman had fallen victim to a ticketing scam orchestrated by the now convicted Lee Maher.

The woman who was desperate to get tickets to watch the singer Beyoncé found some tickets were available on Gumtree. She was convinced that the tickets were genuine and the fraudster said that he was selling them at cost price as he was desperate to get rid of them. He told her that she could pay £65 upfront and then pay for the second ticket when she received the tickets in the post.

When she didn't receive her tickets, she made a report to Action Fraud who had already received a number of reports. With the reports, the NFIB were able to build an intelligence picture and disseminate a package of information including the three bank accounts used by the fraudster – this was sent to Leicestershire Police who were able to investigate Maher.

He was arrested in August 2013 and was subsequently charged with 13 offences of fraud. In September 2013 Maher pleaded guilty and was imprisoned for 16 months for the 13 offences a further 97 reports were also taken into consideration.

The 28-year-old victim said: "The main advice is if it looks too good to be true then it is. Don't ever transfer money because it's basically the same as giving them cash."

Luckily she still got to see the concert as she was able to buy tickets elsewhere.

This case study reflects the end-to-end process, from its start at the Action Fraud reporting centre all the way through to the point where it is investigated by a local force – where in this case the fraudster was imprisoned.