National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Monthly Fraud Threat Update

September - November 2016

Key Judgements:

Impact on Individuals:

- Vishing calls
- Account takeovers
- Binary Options
- Trading Software
- Job application fraud
- Dating Fraud Victim Loan
- Smart Phone – 'Lost Mode' Hack
- Armada Collective: DDoS & Extortion Hacking Group

Impact on Enterprise:

- Distribution Fraud

Cross Cutting Themes:

- Online Shopping – contact outside of the platform
- Online Shopping – Undelivered Items
- Delivery of Empty Boxes
- Social Media Hacking
- NHS Tax Reclaim
- HMRC Text Hack
- Increase in bank transfers to Italy and Germany

Introduction

This monthly threat update will provide an overview of the trends affecting individuals and enterprise as reported to Action Fraud. This report incorporates an assessment of information received during the period 1st August – 31st October 2016. We welcome your feedback so that we can shape future reports to your needs.

Banking & Corporate Fraud

Account Takeovers (August 2016)

Bank customers have been contacted by fraudsters via text message. The message asked the customers to dial 0345 956 9685 in order to reset their telephone banking details as there had been a technical issue with their account, which had caused their account to be blocked. If the customers dial that number and follow the instructions, their details are captured by the fraudsters. Subsequently this enables the fraudsters to call the bank pretending to be the genuine customer and carry out transactions.

Distribution Fraud (October 2016)

A UK supply business is contacted via email by the fraudster purporting to be from an establishment/company requesting a quote for goods to be provided on a credit basis. If this is approved the order is made and items are subsequently delivered to serviced offices or warehouses all over the UK from where they would be dispatched elsewhere; sometimes to privately rented storage locations as reports have also been received from companies that have been storing items for the fraudsters and have not been paid.

Suspects will use email addresses very similar to that of a legitimate establishment's address, just adding a digit, or an 'm' instead of 'nn'. In addition, any mobile telephone numbers given are likely to be VOIP (often starting with 070) and therefore hard to trace.

Investment Fraud

Binary Options (August 2016)

Binary Options fraud continues to be a problem, with one victim losing over £520,000 this month. No money is ever recovered and it is believed that the trades never take place. The fraudulent companies purport to be based in the UK (mainly London), however it is believed that they have no physical presence here.

In one report the victim was advised by staff at the binary options company what to say to bank staff in order to secure a loan (i.e. how much they earned/what the money was for) that was then transferred to the suspect company.

Trading Software (September 2016)

Suspects persuade the victim to purchase trading software for a small fee, in the form of a DVD which installs programmes on a desktop purporting to be linked to the London stock market. The promotional campaign offers a quick win within a 6 or 12 month period and if the victim encounters a loss, they are promised a full refund for their total outlay, paid via bank transfer. Victims find that they do not win and they cannot re-claim the money promised. This is a similar method to binary options fraud.

Mass Marketing Fraud

Job Application Fraud (August 2016)

The NFIB has received reports relating to job application fraud. This is the re-emergence of a trend noted in April 2016. Victims are contacted and told that they have a job and that they need to pay a fee for related vetting / training for their employment. The victim pays the fee and the job does not exist. The NFIB issued an alert for this in May 2016.

Dating Fraud Victim Loan (September 2016)

The suspect(s) uses their relationship with the victim to obtain their personal and financial details and then applies for a loan in the victim's name. The suspect then uses a variety of stories to convince the victim that the money which has appeared in their bank account has come from the suspect and it needs to be transferred to the account of a UK based company (mainly involved in recycling textiles and pharmaceuticals).

Vishing Calls (October 2016)

The NFIB has seen reports where victims receive a call purporting to be from a media broadcasting company stating that a refund was due to the victim, possibly linked to their 'viewing card'. The victim later receives a call purporting to be from their bank saying that there has been unusual activity on their account and asks for sensitive details. This 'verification call' from the bank may be repeated to obtain more details. Ultimately the aim of the suspect appears to be convincing the victim to transfer their money to a temporary 'safe' account that the suspect nominates.

Volume Fraud

Social Media Hacking (August 2016)

The NFIB have identified reports where fraudsters are targeting social media account users, by hacking their accounts then messaging the social media account user's friends, asking them to accept a PayPal credit on their behalf. Those who agree to accept the credit are then asked to transfer the amount to another account controlled by the suspect. Later the credit is disputed as goods were not delivered and refunded by PayPal, leaving the account holder with a financial loss.

NHS Tax Reclaim (September 2016)

The suspects advertised to NHS staff stating that they can claim a tax rebate from HMRC, which is a legitimate claim. The victims pass over all of their identity documents and give permission for the company to request the rebate on their behalf. The company claims the rebate from HMRC and receive the entire amount, purporting to only take a fee before passing the remaining amount to the victim. This does not happen and the company keeps the entirety of the tax rebate.

Online Shopping – Contact Outside of the Platform (October 2016)

Victims order through an online shopping platform, only for the order to be cancelled by the suspect company and a spoofed email is sent requesting an international bank transfer to Italy and Germany. It was also identified that victims have been asked to purchase goods by paying with Gift cards. The ordered items are not delivered.

Online Shopping – Undelivered Items (October 2016)

Victims attempting to purchase goods online pay through normal services and then receive notification of delivery. The delivery has been signed for by an unknown individual. In many instances the victim has reported that they were in at the time of delivery but did not receive any knock on the door or the victim had other items delivered but some were missing and had been signed for by an unknown individual. Online shopping companies have requested that the victims report the instances to police but have refused to provide refunds as the goods had been signed for.

Delivery of Empty Boxes (October 2016)

The victims order an item online or have an item ordered for them by the suspect. The victim ordering an item will receive a box with items which is not what they ordered. In one instance, the victim was ordering a TV and received a catalogue. For a seller, the suspect purchases the item and then purports that there was something wrong with the item and requests a refund. The item is sent back to the seller but the item returned is not what was ordered. In many instances the victim who has received an empty box or incorrect items does not receive a replacement.

Cyber

Smart Phone 'Lost Mode' Hack (August 2016)

The NFIB has seen an increase in reports that smart phone users are being locked out of their handsets, which are being remotely placed in 'Lost Mode'. A ransom requests appears, usually displayed in Russian, and provides Gmail addresses to contact about the ransom (usually the equivalent of £15 - £40).

Armada Collective: DDoS & Extortion Hacking Group (September 2016)

A number of reports have been received whereby victims have been sent emails stating that if they do not pay a fee (normally 1btc / £454 begin with and rising to 20btc's / £10,000) their business will be targeted with a DDoS attack. Open source information suggests that no business has actually been taken offline by the Armada Collective – instead it appears they use the threat of the DDoS attack as a type of protection racket with victims paying the extortion fee. Copycat extortionists are believed to be emailing businesses claiming to be the Armada Collective in addition to this.

HMRC Text Hack (September 2016)

Victims receive a text message stating they are due a tax rebate – the text contains a link to a website requesting personal banking information. Some victims receive a pre-recorded voice call from someone claiming to be from HMRC asking them to call back. It is not known if the texts and pre-recorded messages are linked.

Money Laundering

The Rise of Financial Technology (FinTech) Companies (September 2016)

The rise of FinTech companies and the implementation of the Payment Account Directive (PAD) will have an impact on economic crime as a whole.

In order to boost competition within the UK, the financial services regulator has relaxed rules and cut red tape for new financial institutions, making it easier to become a bank. Whilst it has taken some time for applications to be approved by the 'New Bank Start-up Unit', new financial institutions are now entering the market. They are all trying to compete and take market share away from the well-established financial services that currently exist, by exploiting new technologies and appealing to a new generation of mobile customers that never enter a physical branch.

Payment Account Directive (PAD)

The PAD was implemented in the UK on 18th September 2016. The aim was to improve transparency and comparability of fee information for payment accounts (including current accounts), help people to switch accounts and ensure every EU resident has access to a basic bank account.

The PAD has also enabled the opening of UK basic bank accounts without needing a UK residency, leaving financial services without the ability to perform sufficient identification, verification, Know Your Customer (KYC) and Anti-Money Laundering (AML) checks. The PAD has also removed the ability to close an account on the 'suspicion' of financial crime. It states that only one basic bank account can be opened, but there is nothing in place to monitor or manage this. The opening of UK bank accounts from a country in European Economic Area without sufficient due diligence could result in an increase in fraudsters or money launderers using these accounts for criminal purposes.

Glossary of Terms

Ransomware	This is a form of malware that attacks your computer, locking you out and demanding payment in the form of a 'fine' to have it unlocked. The warning page distributed by the fraudsters, typically uses logos from both the Metropolitan Police and the Police Central Crime e-Crime Unit (PCEU) to make it look more like an official warning notice.
Spoofing	Fraudsters typically clone the telephone number of the organisation they want to impersonate and then make it appear on the victim's caller ID display when they telephone them on a landline. The fraudsters will then gain the person's trust by highlighting the number to them, claiming that this is proof of their identity, before trying to defraud them in various ways.
DDoS Attack	Distributed Denial of Service (DDoC) attack is where multiple compromised or infected systems flood a targeted system – usually a system of web services. This is often to bring down an organisation's website.
DDoS with Extortion	The same as the above, however the suspect will normally email the victim to advise that an attack in about to begin and to prevent the attack the victim needs to pay a sum of money.

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998.

The cover sheets must not be detached from the report to which they refer.

Protective Marking:	**NOT PROTECTIVELY MARKED**
FOIA Exemption:	NO
Suitable for Publication Scheme:	NO
Version:	FINAL
Storage File Location:	
Purpose:	Provide an overview of key themes affecting individuals and enterprise. The information contained within this report has been based upon content within Action Fraud reports which have not been verified as true and accurate accounts.
Owner:	NFIB
Author:	Analyst
Review By:	Senior Analyst, 88071e