National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Monthly Fraud Threat Update

January 2017

Key Judgements:

Impact on Individuals:

- Phishing email and texts purporting to be from HMRC installing ransomware and setting up accounts and contracts in victims' names
- Suspects exploiting victims unfamiliar with activating their computer antivirus software

Impact on Enterprise:

- Retail company refunding clearance price goods to suspect at full price

Cross Cutting Themes:

- Victims having motor insurance policies taken out fraudulently, using their personal details
- Victims receiving parking charge notifications in their names
- A third party seller instructing online customers to make payments to Italian IBANs

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 of 1st December – 31st December 2016. We welcome your feedback so that we can shape future reports to your needs.

Banking & Corporate Fraud

Retail company Refunds

The suspect has purchased pallets of mixed goods from a retail company's clearance trade business at low prices and has then returned them to various stores obtaining refunds for them at full price, thereby illegitimately making a profit. The retail company has reported this as a fraud. The refunds have been traced to two credit cards, neither of which have previously been reported to have been used illegally.

Cyber

Her Majesty's Revenue and Customs (HMRC) Virus

Victims have received phishing emails and texts purporting to be from HMRC concerning the victims' tax rebates. Victims have downloaded a word document attached to an email and inadvertently downloaded files from a hacked website which installs ransomware. When victims click on the link in the HMRC spoofed texts they are redirected to a registration page requesting personal details. The emails and texts appear genuine and the victims who have provided their personal details have consequently had direct debits, mobile phone contacts and new bank accounts set up using their personal information. HMRC have advised on their website that this is a fraud and stressed that they would never contact people using these methods.

Identity Crime

Motor Vehicle Insurance Fraud

Victims are getting letters to their address informing them that they have insured themselves on various motor vehicles. The trend appears to be rising with increasing reports. It is possible that an organised criminal group is involved as the fraud would be too much for one individual to coordinate.

Parking Charge

Victims have been receiving letters from individuals purporting to be the police and parking authorities informing them they have been spotted parking illegally and are due to pay a fine. This includes victims receiving penalty notices for hired vehicles contracted in their names.

Investment Fraud

Wine Investment Fraud and Recovery

There were seven reports in December linked to wine investments and wine recovery. Six of these reports stated that contact had been made by the fraudsters within the last two months. The Investment Fraud Team is anticipating that this might become a commodity sold by boiler rooms again. Recovery Room fraud is a method where criminals contact victims of previous frauds, often by cold calling, and claim to be able to recover previously lost funds for an upfront, advance fee. When Recovery Room fraudsters contact victims of wine investment fraud they will usually claim to be a legal professional such as an insolvency practitioner or a representative of another investment firm whose client wishes to purchase the victim's wine. 'Release' fees and various taxes will be requested by the fraudsters before the victim receives their money.

Mass Marketing Fraud

New Antivirus Activation – Computer Software Service Fraud

Victims who have purchased brand new computers have found they have been unable to activate their antivirus software subscription and have followed a website link and have subsequently been contacted by phone by fraudsters asking for payment to install the antivirus. This modus operandi has also been used when victims have attempted to renew their antivirus subscription.

At present the reports are still low in volume and there is no correlation in the victims' locations that would suggest an issue with a single outlet. However the reports do suggest that fraudsters are targeting and exploiting victims that are potentially unfamiliar with activating or renewing antivirus software.

Money Laundering

Italian International Bank Account Numbers (IBANs) Online Shopping & Auction

During December, Italian IBANs were the most reported IBANs, after the UK. This was due to a third party seller, on an online shopping platform, who has been altering the process of ordering goods through the online shopping platform and removing the accompanying protections that are in place. The typical modus operandi involves the victims identifying goods advertised on the online shopping platform and then being informed on the website to contact the third party seller in order to check stock. On doing this the victims are then asked to make a payment to an Italian IBAN to purchase the goods. The bank transfers were made to an Italian bank with three different account names.

Glossary of Terms

Phishing	Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by illegally impersonating a trustworthy entity in an electronic communication.
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.

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:	G:\OPERATIONAL\Fraud_Intel\Desk_Screening_Reports\Monthly Threat Update\17-01
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, 105429p
Review By:	Senior Analyst, 88071e