



East Division Neighbourhood Watch Newsletter

Issue 7: Identity Theft December 2016

Welcome to this edition which focuses on identity theft. I hope you will find the contents useful.

Alex Harrington has now moved on and I have taken over the role of Volunteer and Neighbourhood Watch Liaison Officer for East Kent. I wish Alex well in her new post and thank her for her support and handover for my new role. For those of you that don't know me I am a retired Police officer of 30 years service. I was based at Ashford for most of my career and worked within the field of Neighbourhood Policing and Community Safety for most of this time. I am currently based at Ashford Police Station and my contact details are below. We have applied for the vacant post to cover Thanet and Canterbury to be made into a permanent, rather than a contract, post. We are awaiting a Force decision regarding this request. In the meantime I will be covering all of East Kent.

Thank you to our volunteer, Mrs Karen Uzzell- Childs, for completing the detail in this newsletter – we really appreciate her efforts.

I would like to take this opportunity to thank everyone for their assistance and support in 2016 and I look forward to working with you in 2017.

Season's Greetings,

Andrew Judd

NHW Liaison Officer, East Division

Office 01233 896151

Mobile 07980965236

andrew.judd2@kent.pnn.police.uk

Identity theft

- *Fraud & cybercrime cost the UK nearly £11bn in the past year*
- *That equates to approximately £210 per person over the age of 16 living in the UK, but represents only reported fraud and cybercrime to Action Fraud.*
- *Victims of online crime are losing an average of £523*
- *39% of people who said they'd been victims of online crime said they hadn't reported the incident – meaning that the overall amount of money lost by the UK could in fact be even more.*

Figures from Action Fraud October 2016

Identity theft occurs when a person or organisation acquires personal information about someone and uses it to their advantage, usually for financial gain. The information used could be someone's name, date of birth, current or previous addresses, National Insurance number, bank or credit card details or social media account. Often the information is used to commit fraud, such as obtaining loans, credit cards or a

mortgage. Someone may also be able to order goods and services in your name or obtain passports and driving licences with your personal details. Victims of identity fraud may not even be aware that they have had their identity stolen until they try to take out their own loans or mortgages and find that they have a very poor credit score or unexplained debts. They may also receive invoices for goods and services they had never ordered and demands for payment and/or summons from debt collection agencies.

Protect yourself against identity fraud using a few simple methods

“Be Vigilant”

- Don't throw away any letters, documents or forms with your name, address or financial details on them. Invest in a quality cross shredder to ensure documents are properly destroyed. Stockists include Staples and Argos.
- If you receive an unsolicited email or phone call from what appears to be your bank or building society asking for your security details, never reveal your password, login details or account numbers. Be aware that a bank will never ask for your PIN or for a whole security number or password. Put the phone down and visit the bank/building society in person.
- Check your statements carefully and report anything suspicious to your bank or financial service provider. Keep receipts and invoices to double-check purchases. If ordering on-line you should be able to review current and previous orders.
- Don't leave things like bills lying around for others to look at. File statements away carefully and shred any that are several years out of date.
- If you're expecting a bank or credit card statement and it doesn't arrive, contact your bank or credit card company. Also, find out what assurances and cover they offer if you are a victim of fraud.
- If you move house, ask Royal Mail to redirect your post for at least a year. Prices for redirecting mail in the UK start from £31.99 for three months and £59.99 for twelve months. For more details go to, www.royalmail.com Search for redirections and new addresses.
- Make a list of all the organisations that have your details, such as Banks, on-line shopping companies, utilities etc. and contact them as some post cannot be redelivered. This is often the case with electoral roll forms.
- Use credit reference agencies to check your credit rating and to find out if there has been any significant changes on your credit file that could indicate potential fraudulent activity: www.experian.co.uk; www.callcredit.co.uk; www.equifax.co.uk; www.clearscore.com; www.noddle.co.uk. Some of these agencies offer free services for checks, others may charge a fee for continual use. It is particularly helpful to check your personal credit file 2-3 months after you have moved house. Equifax is free for the first 30 days and then it's £14.95 per month. You can cancel at any time. With Experian you can check your Credit Score for free. If you would like to look at the factors affecting your score, you can check your Experian Credit Report, Score & more with a 30-day free trial of Credit Expert, a monthly fee of £14.99 applies thereafter and you can

cancel anytime.

Using Social Media responsibly

Many people use social media sites such as Facebook, Twitter, Snapchat and Instagram to stay in touch with family and friends or to post personal news and photos. These sites can provide a huge amount of information about individuals which criminals can use for identity fraud.

- Avoid posting personal details such as date of birth, home address, mother's maiden name, details of your workplace or school/college
- If you are away on holiday don't upload holiday photos until you are back home as this could indicate that your home is unoccupied
- Don't upload photos of your home which could give a potential burglar information about entry or show valuable possessions
- Check the security settings on your Facebook accounts, ideally it should be 'Friends only'
- Use secure passwords and usernames that don't include personal information
- If you are unsure about a post then ignore and/or delete it

Advertising items for sale

The criminal fraternity use a number of websites to assist them in their activities – such as Goggle Earth and Right Move, when your house is for sale. Ensure that if you post items for sale, including properties you make the property look lived in but bland (remove antique clocks from display for example).

Selling goods on Ebay: Fraud on eBay ranges from fake emails asking for your account details (often called phishing), to the sale of illegal and counterfeit goods. To avoid being taken in by a scam, make sure you read the information in eBay's safety centre and never reply to an email request for passwords or account details.

Gumtree provides examples of fraudulent advertisements and advice on avoiding scams, <https://www.gumtree.com>

What should you do if you've been a victim of identity fraud?

"Act quickly"

- Don't ignore the problem or think it has nothing to do with you. Even though you didn't order those goods or open that bank account, the bad debts will end up under your name and address
- If you believe you're a victim of identity fraud involving credit or debit cards or online banking you must report it to your bank as soon as possible. Your bank will then be responsible for investigating the issue. If money is stolen from your debit card, then the relevant piece of legislation is the Payment Services Regulations. It says you must be refunded immediately if you have had money taken from your account without your permission.
- You will be liable for any unauthorised withdrawals made before you tell your bank or building society, up to a maximum of £50

- If the money stolen is on credit, the Consumer Credit Act applies. This legislation states that for any unauthorised transactions the cardholder may be held liable for the first £50 spent if a card is lost or stolen. Again many banks and building societies will waive this.
- You should report all lost or stolen documents, such as passports, driving licences and credit or debit cards, to the relevant organisations. Driving licences and passports are of particular importance to criminal gangs as they can be used to gain access to financial services. If you're not sure which organisation to call, contact Action Fraud for advice.
- If you suspect your mail is being stolen or that a mail redirection has been fraudulently set up on your address contact the Royal Mail Customer Enquiry line on 03457 740 740. They are open Monday to Friday, 8am-6pm, Saturday 8am-1pm and Sunday 9am-2pm. Text Phone if you're hearing impaired, on 03456 000 606.
- Get a copy of your credit report. A credit report will show you any searches done by a lender, what date the search took place, what name and address it was done against and also for what type of application. It will also show what credit accounts are set up in your name. You can contact any one of these credit reference agencies and receive support in resolving credit report problems caused by identity fraud. • Callcredit • Equifax • Experian • ClearScore • Noddle.
- Look at your credit report closely. If you find entries from organisations you don't normally deal with, contact them immediately. Remember to keep a record of all your actions, including the people you've spoken to and when, and keep copies of all letters you send and receive. The credit reference agencies will contact lenders on your behalf where fraudulent applications have been made or fraudulent credit accounts opened in order to restore your credit history to its former state. Equifax Identity Watch Pro is available for £9.95 a month and alerts you within 24 hours if we find your personal data on websites used by fraudsters.
- Passwords - If you suspect someone has gained access to a password or pin number change it as soon as possible and do not write it down or use the same passwords for multiple accounts.

Credit and debit cards

- If your plastic cards are lost or stolen, cancel them immediately. Keep a note of the emergency numbers you should call to cancel them.
- When giving your card details or personal information over the phone, internet or in a shop, make sure other people cannot hear or see your personal information.
- Be wary of emails claiming to be from Banks or financial services, asking you to click on a link in the email and enter your information. This is a common scam used to steal money from people's accounts. Contact the companies yourself to query the problem and get more details. Check

From: CustomerSecurity@royalbank.com¹
Sent: Monday, July 20, 2009 7:54 PM
To: Rob.Smith@hotmail.com
Subject: Renew your Online Account with Royal Bank Immediately – Final reminder²

Royal Bank

Dear valued Royal Bank customer,³

It has come to our attention that you have not logged into your online banking account for some time⁴ now and, as a security measure, we must to suspend your online account.⁵ If you would like to continue to use the online banking facility⁶ offered by Royal Bank, please click the link below and renew your security details⁷ immediately. Failure to do so will result in your online account being suspended.⁸

Renew your security details immediately and continue to use our online banking facility:
<https://customerbankingrenewal.royalbank.com/>⁹

We are sorry for any inconvenience¹⁰ caused and hope you continue to use our online banking facility.

The Royal Bank Online Security Team¹¹

Link: <http://customerbankingrenewal.royalbank.com/>

your email addresses carefully and do not just click the reply button without checking the details.

An example of a fraudulent email

Contactless card fraud facts

According to Financial Fraud Action UK, in 2015, fraud on contactless cards and devices accounted for £2.8 million of losses compared to £7.75 billion in spending. Total card expenditure in 2015 was £856 billion, meaning contactless payments accounted for 0.9% of spending, but only 0.5% of fraud.

- At present contactless technology limits the value of purchases to a maximum of £30, so losses are smaller in comparison to a card being used in a shop if the thief also had the pin number. This amount is set to rise.
- A 2015 test by the consumer group Which? found that it was possible to steal details from contactless cards using an easy-to-buy card reader and free software. They were able to extract a card number and expiry date from 10 different contactless cards, but not the name or CVV code on the back. Typically, this would not be enough information to make a purchase online, but Which? were able to purchase goods from certain online retailers using the limited card information and a fake name and address.

How to protect against contactless card fraud – don't leave cards easily accessible in bags or pockets or lying about at home. Another technique involves lining your wallet or cardholder with tinfoil to block any signals from reaching your card. If the do-it-yourself approach does not appeal, there are products on the market containing metal inserts that do the same job. See Amazon for a range of products. If you are shopping at Bluewater don't forget to visit the Kent Police Bluewater Safety Shop as they sell wallet holders for a £1.

Stealing the identity of a deceased person

Criminals sometimes use the identities of the deceased to commit fraud, this is very distressing for those close to the deceased. The following websites offer deceased person mail preference services and provide further information on this issue: The Bereavement Register, www.thebereavementregister.org.uk, www.deceasedpreferenceservice.co.uk, www.mpsonline.org.uk/mpsr and credit reference agencies that we have already mentioned above. The credit reference agencies provide a free victims of fraud service, for anyone who has had their personal details used fraudulently. Importantly, the credit reference agencies liaise with each other, and the banks, to restore compromised personal credit records.

Are mobile banking apps safe?

Most internet banking providers invest heavily in the security of their mobile applications. These apps often have limitations on the amount of money they can transfer to minimise the risks. HSBC, for example, requires the user to set up an account using a unique code sent from the bank. The user must then create a user name and password. To stay safe follow these rules:

- Never leave your device unlocked
- Keep the apps on your phone regularly updated
- Try not to use unsecured wi-fi networks for banking, purchases or checking your emails
- Take care when downloading apps - if something looks too good to be true, it probably is
- Encrypt your phone

- Check the security settings in your device to ensure maximum protection

Ethical Hackers - a person who hacks into a computer network in order to test or evaluate its security, rather than with malicious or criminal intent. You can log onto the sites below to watch these clips from You Tube about what Ethical Hackers do:

<https://www.youtube.com> 'A day in the life of an Ethical Hacker'/ Why Ethical Hacking is so important in a 21st century economy' by Jennifer Arcuri at the TEDxLiverpool

For more information and advice on fraud and online security:

- Equifax Phone: 0800 121 4752 Web: www.equifax.co.uk/ask
- Callcredit Phone: 0870 060 1414 Email: vof@callcreditgroup.com
- Experian Phone: 0844 481 8000 Email: consumer.helpservice@uk.experian.com
- Experian Credit Expert Web: www.creditexpert.co.uk
- ClearScore Web: www.clearscore.com
- Noddle Web: www.noddle.co.uk
- Crimestoppers www.crimestoppers-uk.org
- Age UK Advice: 0800 169 2081 www.ageuk.org.uk
- OFCOM: 0300 123 3333 www.ofcom.org.uk
- www.thinkjessica.com
- Mailing Preference Service www.mpsonline.org.uk
- www.actionfraud.police.uk tel. 0300 123 2024
- www.hoax-slayer.com
- www.gov.uk/consumer-protection-rights
- www.frsb.org.uk (Fund Raising Standards Board) Tel. 0333 321 8803
- www.ico.org.uk (Information Commissioner's Office)
- www.fca.org.uk For financial advice on investments

- www.thebereavementregister.org.uk
- www.deceasedpreferenceservice.co.uk

Alexandra Harrington – East Division NHW Liaison Officer

PSV Karen Uzzell-Childs – Volunteer (researcher and compiler)

November 2016