

<b>For Information</b>	
<b>Public</b>	<b>Public</b>
<b>Report to:</b>	<b>Joint Audit and Scrutiny Panel (JASP)</b>
<b>Date of Meeting:</b>	<b>24<sup>th</sup> July 2018</b>
<b>Report of:</b>	<b>Chief Constable</b>
<b>Report Author:</b>	<b>Detective Chief Inspector Young</b>
<b>E-mail:</b>	
<b>Other Contacts:</b>	
<b>Agenda Item:</b>	<b>8</b>

\*If Non Public, please state under which category number from the guidance in the space provided.

## **Tackling Fraud – Nottinghamshire Police**

### **1. Purpose of the Report**

1.1 The purpose of this report is to provide an overview of Nottinghamshire Police's:

- Current investigative response to fraud, including strategic principles
- Identification and management of vulnerability
- Collaborative and preventative working arrangements

### **2. Recommendations**

2.1 It is recommended that the meeting notes the content of this report.

### **3. Reasons for Recommendations**

3.1 To ensure that members are aware and updated on the Force's strategy in relation to tackling fraud.

### **4. Summary of Key Points**

#### **4.1 Contextual Summary**

4.1.1 Nationally, fraud offences make up around half of all reported crimes and this statistic is replicated within Nottinghamshire. It is also significantly under-reported as a crime category leading to a high probability of unaccounted for demand and an associated victim base that have not engaged meaningfully with the authorities. Within Nottinghamshire Police, fraud offences are the responsibility of a dedicated unit managed under Organised Crime and regarded as a specialist function. This includes capability for the management and investigation of specialist offences, such as election fraud or bribery and corruption. Advances in technology and the level of sophistication in criminal modus operandi have contributed to the rise and complexity surrounding fraud investigations. There is a clear and defined link between technology and fraud (cyber-enabled offending) that has caused a necessary mind-set shift from

pursue based activities to ones that are focussed on prevention and protection.

4.1.2 Fraud affects all parts of society whether as individuals or as part of the business community. Some victims may be more susceptible, for example the casual approach of the young in sharing online personal data or the vulnerability of elderly people who are more easily exploited through 'grooming' style techniques. Similarly, businesses that are unable or reluctant to invest in protective technologies and training face a greater risk of exposure to fraud with an increasing consequence of fatal economic damage to their business.

#### 4.2 **Resource & Investigative Structure**

4.2.1 The Fraud Unit operates within the Organised Crime Department, under the Crime & Operational Support Command.

#### 4.3 **Acceptance Criteria**

4.3.1 The aim of Nottinghamshire Police is to deliver a proportionate investigative response to all reported fraud offences and to prioritise those cases that impact most heavily on the vulnerability of the victim and the threat, risk or harm to citizens of Nottinghamshire.

4.3.2 To support this principle, fraud investigators are empowered to apply criteria for the purpose of determining the type of response that each reported crime will warrant, appropriately prioritising those where vulnerability and risk are most apparent. This takes the form of a structured guidance document (Acceptance Criteria) that informs the decision making process. All fraud offences are managed through the unit, ensuring that the criteria are applied consistently and fairly.

#### 4.4 **Sources of Referral**

##### 4.4.1 **National Fraud Investigation Bureau Disseminations**

These are cases that have been referred to Action Fraud, assessed as containing viable investigative leads by the National Fraud Investigation Bureau (NFIB) and distributed to Police Forces via a dedicated email address. Upon receipt, they are registered on NICHE and auto-allocated to the Fraud Unit.

Determination for allocation is governed by NFIB criteria, as shown below:

1. The police force covering the location of the fraudulent operation e.g. suspects address/company office

2. The police force with the greatest number of individual usages on a card or account
3. The police area where the first offence was committed
4. The police force where the victim resides
5. If impossible to determine from 1 to 4 above, the NFIB will determine.

Individual disseminations can include multiple victims and suspects. The dissemination is sent under a single reference number, but may include numerous victim reports.

As the disseminations are frequently sent on the basis of the suspect location, it is common for each force to investigate allegations where they have victims located in other force areas, and with no victims located within the investigating force area.

#### **4.4.2 NFIB Referrals Featuring Vulnerability**

If the NFIB disseminate an investigation to an area that does not include the home address of a vulnerable victim, they may generate a control room incident requesting that the home force for the victim attend and conduct a safeguarding assessment.

#### **4.4.3 Calls for Service**

These are cases that are reported to Nottinghamshire Police directly and require a local attendance in accordance with force attendance grading criteria. Additionally, all Calls for Service will also require onward referral to Action Fraud.

The flow chart at **Appendix A** details the considerations applied by Control Room staff when determining whether a reported incident of fraud requires attendance by a Nottinghamshire Police resource. Where the flow chart indicates that attendance is not required, the Control Room should advise the caller to report the allegation to Action Fraud via the online portal or by telephone. Under these circumstances, a Nottinghamshire Police incident would not be created.

Any referral to Action Fraud creates an National Fraud Reporting Centre (NFRC) reference which is a crime number. These are held by the City of London Police, not the Home Force and are completely compliant with crime recording protocols.

#### **4.4.4 SAR Referrals**

Suspicious Activity Reports (SAR) are generated through the financial services industry and reach Police Forces in report form. They are confidential disclosures between the Financial Services Industry and Law Enforcement and therefore not disclosable to involved parties, whether as victims or suspects.

Nottinghamshire Police expect to receive in excess of 300 reports each month and these are managed by the Financial Investigation Unit that is co-located with Fraud. A process is in place that reviews each report, with appropriate action taken where suspicion of criminality or vulnerability is identified. Examples of suspicious activities

could include foreign money transfers or large cash withdrawals that could be indicative of organised crime or some form of exploitation. Some such cases will be referred to the Fraud Unit for consideration of further investigation or safeguarding measures.

Nottinghamshire Police has received 2728 SAR reports in the first half of 2018 and employs three Financial Intelligence Officers within the Financial Investigation Unit to proactively examine all SARs.

Nottinghamshire are one of only a handful of forces to do this, recognising that in this way we can truly identify and deal with vulnerable victims, identify investigative opportunities and develop intelligence that supports current operations.

SARs are the only mechanism by which financial institutions are able to share intelligence with law enforcement and have proved to be of particular value in identifying victims of investment fraud, romance fraud, advance fee fraud and recovery fraud; many of whom are categorised as, yet often fail to see themselves as vulnerable victims.

In addition to SARs, the FIOs also receive Defence Against Money Laundering (DAML) requests from financial institutions seeking consent to conduct onward transactions where concerns have been identified. The NCA send SARs directly to the Force where they have identified vulnerability or criminality.

Nottinghamshire Police FIOs have identified 65 vulnerable victims over and above those disseminated by the NCA. As noted, these victims do not typically identify as victims of fraud and therefore will not report themselves to the police.

Whilst each force develops its own policy in relation to how SAR intelligence is used, Nottinghamshire police are recognised as good practice and currently chair the East Midlands Regional Financial Investigation Working Group. In this capacity, Nottinghamshire has secured a seat on the National Financial Investigations Working Group and as such we are able to promote best practice in proactively supporting vulnerable victims of financial crime and using financial intelligence to its fullest potential.

#### 4.5 **Prevention and Collaboration**

Established practices exist within Nottinghamshire Police that focus specifically on preventative strategies that aim to:

- Prevent re-victimisation
- Intervene where vulnerability is identified
- Communicate protective messaging

#### 4.5.1 Banking Protocol

The Banking Protocol is a partnership between financial institutions, the police and other agencies. The primary objectives of the Protocol are:

- The identification of individuals who are coerced/deceived into attending their local bank to withdraw or transfer funds to pass on to criminals
- The prevention of that fraud taking place
- The provision of victim support to reduce the individual's future susceptibility to fraud
- Where possible, arrest of the suspect

In practice, these incidents relate to occasions where employees at financial institutions believe that a customer, present at the branch may be subject to a fraud. Other factors include the presence of a suspect in the vicinity and the necessity to safeguard their customer's funds by preventing cash withdrawal or transfers. If these concerns are met, the member of staff will contact the police via 999 quoting '**Banking Protocol.**' which will prompt the immediate despatch of officers to the location. Successful interventions have resulted in the arrest of numerous suspects for rogue trader type offences, identified victims of fraud and prevented the loss of over £280k.

In the last 12 months there have been six arrests and £282,210 prevented losses from attempted fraud in Notts as a result of 94 protocol activations. The Banking Protocol shows how close cooperation between the industry and law enforcement helps protect victims, crack down on fraudsters and provides a joined-up approach, which in itself is crucial to stay one step ahead of fraudsters. Excellent working relations with local banks have enabled Nottinghamshire Police to very quickly intervene and prevent vulnerable people from being financially exploited.

#### 4.5.2 Op Signature

Nottinghamshire have sought and applied best practice (developed by Sussex Police) through implementation of a process whereby individuals at risk of financial abuse are identified and supported through the delivery of 'Protect' advice and other measures that are commensurate to their assessed level of financial vulnerability (**see Appendix B & C for examples**). These assessments are undertaken in relation to Calls for Service, Banking Protocol incidents, NFIB disseminations, Suspicious Activity Reports, referrals from partner agencies and monthly Action Fraud Victim Data. All assessments are completed by utilising a number of financial vulnerability considerations, which include age, mental capacity, disability, the impact of the fraud both financially/emotionally, any future risk to the victim and other safeguarding issues. To manage demand effectively, a tiered response is applied:

- High risk – Personal visit from a Fraud Protect Officer
- Medium Risk – Protection advice letter/email
- Low Risk – No further action

Fraud Protect visits will be conducted by a combination of two Fraud Protect Assistants and a cadre of trained PCSOs across the NPTs. They will be centrally tasked by the Op Signature team with outcomes recorded on NICHE. The number of visits the victim receives is case-dependent and will continue until the risk of financial vulnerability has been mitigated.

This process is designed to complement the Force's existing work around overall vulnerability, with safeguarding considerations built into the initial fraud Protect visit actions and assessment. Public Protection Notices are submitted where appropriate.

Whilst Op Signature is clearly in its infancy, analysis of the initial and available data is demonstrating that circa 60 high and medium cases are identified per month, and by way of example, losses to victims have totalled in excess of £1Million (£1,042,187.00).

#### **4.5.3 Multi-Agency Approach**

Opportunities are taken to identify vulnerability and spread safety/prevention messages by working collaboratively with other agencies and charitable organisations. The following initiatives involve partnership working:

- Delivery of awareness training to care home operators and staff in relation to financial vulnerability and abuse. The training has already resulted in a marked increase in co-operation and reporting from care homes, reaching over 200 delegates.
- Nottinghamshire Fire and Rescue Service (NFRS) – agreement to work with the Fraud Protect Team from July 2018. The aspiration is that NFRS will train their crews to identify financial vulnerability/abuse. They will have access to the Operation Signature team for the purpose of making referrals and have additionally agreed to train Fraud/Cyber Champions within their own teams to deliver Protect messages.
- Get Safe On-line provide materials for social media, campaigns and leafleting whilst supporting bespoke events.
- Working with educational establishments throughout Nottinghamshire to deliver Protect messages to students. In 2017 the Protect Officer attended 'Fresher' events.
- County & City Trading Standards - Working together to avoid duplication of action and refer to each other where appropriate.
- Nottinghamshire Police issue alerts via social media utilising Facebook, Twitter and Neighbourhood Alerts.

#### **4.5.4 Further collaboration opportunities, currently under development**

- A meeting was scheduled for 10<sup>th</sup> July to progress engagement with the Action Fraud National Economic Crime Victim Care Unit.
- Catch22 - Agreement reached to jointly provide consistent advice to service users
- Chamber of Commerce & Federation of Small Businesses - Links to Nottinghamshire businesses via this relationship with an agreement from the Protect team to complete presentations and support events.
- Although there is no current referral process in place due to capacity, agreement had previously been reached with Age UK and the Rural Community Action Network that they would assist in delivering Protect advice.

#### **4.6 Conclusion**

4.6.1 This report demonstrates that fraud is multi-faceted, technical and requires collaborative effort to achieve the right outcomes on behalf of the most vulnerable victims. Our approach to tackling fraud will be considered as part of the Force Annual Departmental Assessment.

4.6.2 The clear focus has become on how fraud can be prevented and victim's protected as a result of the volume of offences and also as a result of jurisdictional limitations, such as offenders operating from abroad.

4.6.3 Investment in specialist training that keeps pace with technical developments in offending are key to providing an effective response to pursue serious offenders, whilst more generalised training is required to enhance the skillset of frontline officers who can more widely support preventative and protective messaging and identify vulnerability at first point of contact. Adapting to changes in offending, reporting and vulnerability are essential to maintaining and developing the service provided.

### **5. Financial Implications and Budget Provision**

5.1 There are no financial implications arising from this report.

### **6. Human Resources Implications**

6.1 There are no HR implications arising from this report.

### **7. Equality Implications**

7.1 There are no equality implications arising from this report.

## **8. Risk Management**

8.1 Any risks are highlighted within the body of the report.

## **9. Policy Implications and links to the Police and Crime Plan Priorities**

9.1 The Force's approach to tackling fraud is intrinsically linked with the Police and Crime Plan priorities, specifically 'Protecting People from Harm' and 'Helping and Supporting Victims.'

## **10. Changes in Legislation or other Legal Considerations**

10.1 There are no changes in legislation in relation to this report.

## **11. Details of outcome of consultation**

11.1 There has been no additional consultation in relation to this report.

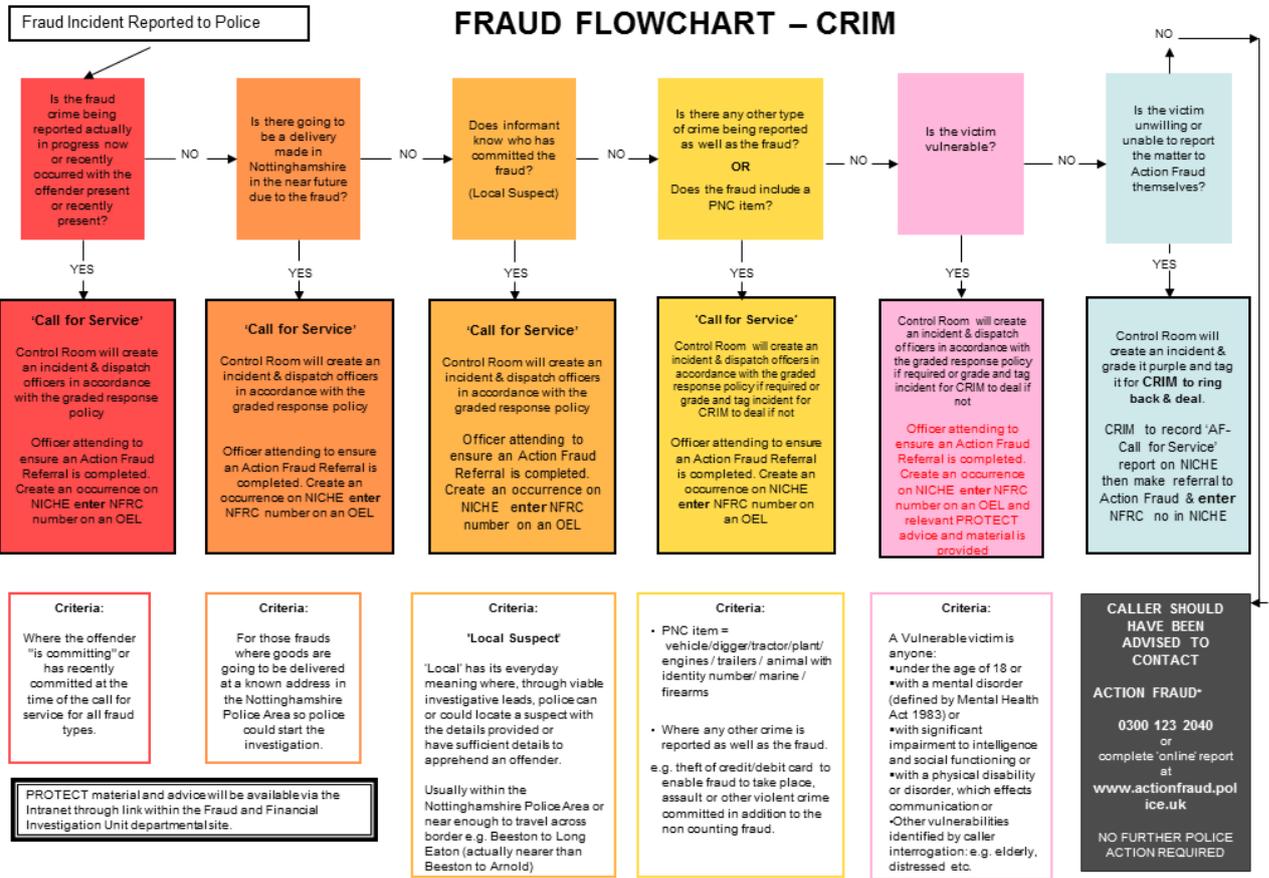
## **12. Appendices**

12.1 Appendix A – Fraud flowchart CRIM.

12.2 Appendix B – BAN Romance Fraud.

12.3 Appendix C – Advice doc.

# Appendix A



## Appendix B

# BAN Romance Fraud:

## **B**eware of:

- **Anyone asking personal details:** On you/your background & nothing on themselves
- **The Sob Story:** Someone telling you how much they want to visit, but need a loan to pay for: Tickets/Visas or for medical expenses for desperately ill family members/children, discharge fees from their current job or for essential goods. There's also the too good to be true business deal to be aware of, if only they had some extra up-front money to pay into this!
- **Repayment:** Any reference to Gold/ Gems/Diamonds as a repayment, allowing you to check a pretend bank balance online to show you a fake bank balance. Don't become a money mule- The fraudster could send you a cheque and request you to transfer the funds over to them. However by doing this you could be committing a criminal offence of money laundering
- **Vague communication:** Around personal interests, they may repeat things or seem disconnected, dodge questions or make excuses for not meeting or speaking on the telephone.
- **Don't let time cloud your judgment:** Fraudsters use time to play their fake stories on you, make you believe the relationship is real, gain trust and all with one goal in mind, to financially exploit you, even if this is 1-2 years down the line.
- **Declarations of love:** This can be within a matter of weeks, days or hours, so be cautious! You need to know someone to come to love them. Instant messages of love could be someone trying to get right into your life for all the wrong reasons.
- **Opening email attachments:** **Don't** - Especially from someone you have only just met
- **Video Call:** Excuses to why the person can't do a video calls. With internet cafés and technology that surrounds the world; there's never an excuse to prevent face to face communication where ever you are.
- **Profiles:**
  1. **Profile Name:** Different user name to that of the person you are speaking with. For example: User name – 'Davidin2u' and first message received states 'Hello how are you, my name is Kelvin
  2. **Profiles that tug on heart strings:** Living on an oil rig, are in the military or left military work or widowed. Other indicators: They make reference to gold or gems to sell as repayment and/or have odd spelling and grammar
  3. **Profile Location:** Discrepancies - Location states is in Malaysia but their profile states they're looking for a relation in Germany

## **A**lways:

- **Use only reputable dating sites and their own messaging service:** Ensure sites used are part of the [Online Dating Association](#) (ODA). Fraudsters want to quickly switch to social media or to texting to avoid the sites own scam protection from detecting their grooming tactics and to hide their requests for money.
- **Keep safe:** Do not share pictures or information about yourself or others that can give someone a hold over you. Your private life should stay private until you know that person, have met face to face and can start to trust them. Often victims can be socially engineered through social media accounts like Facebook, to protect yourself, ensure you have all applicable security settings set to private preventing strangers from finding out everything about you, your interests, your history, conversations, friends and groups you have.
- **Speak openly about your dating:** Use trusted friends or family (don't let embarrassment scare you). If you're involved emotionally it's hard staying objective. Alert them if a contact starts

to feel strange, especially if the subject of money gets raised. If their advice is to back off, LISTEN! They have no emotional involvement and can provide the correct level of judgement with your best interests at heart.

- **Account Security:** Be careful when accessing your account. Public or shared computers can be used to view or record your password or personal information. Keep your internet security software up to date.
- **Stop communicating if pressured over anything:** For personal or financial information or who seems to be trying to trick you into providing it or tell you to keep your relationship a secret. Never agree to this. This is a ploy to stop you telling your family and friends who have the opportunity to see this for what it really is.
- **Profiles:**
  1. **User Names:** Choose a username that doesn't let everyone know who you are by not including your surname or anything that can identify you (eg. Place of work, family names or address).
  2. **Remember:** Overtly sexual, provocative or controversial usernames could attract the wrong kind of attention.
  3. **Keep Contact Details Private:** Stay in control when it comes to how and when you share information. Don't include your contact information such as your email address, home address, or phone number in your profile or initial communications. Take things slowly and share more information when you feel comfortable doing so (especially after regular face to face contact). It is impossible to get back information once you have given it away and this can be used against you later on.

## Never:

- **Give Away Personal Information:** Revealing your full name, date of birth and home address. Giving this away may lead to your identity being stolen. If not advertised the Fraudster will try using other conversational tactics to try obtaining this information from you (eg. Whens your birthday? How old are you? This will give them your full date of birth)
- **Send or Agree to Receive Money** – The Fraudster will try anything in attempt to get your bank details. Never do this no matter how much you trust them or believe their story, don't forget if they're genuine they wouldn't ask you for any money. If you do send money, they'll continue to come back for more until you have nothing left.
- **Assume Fraudsters are Illiterate:** You are unlikely to see through the scam in an instant as you'd predict. Fraud/Scamming is a pretty sick line of business but it is a business for them. They practice tugging at heartstrings, show tenderness and love, but can generally be needy and tell victims what they want to hear and can relate to.
- **Leave the dating site:** Never move off the dating site to communicate as this prevents the site from protecting you and identifying fraud.

## Appendix C

### Advice (Recommended where applicable) - Part 1



**PREVENT:** No matter how realistic the story is or who they claim to be representing (even police), don't engage in conversations, or respond directly to an email or text. Contact the organisation using a number you know to be genuine, like the number from a bill or off the back of your bank card as this ensures the line is disconnected first. Never agree to send/receive money or give away your bank details/pin number to anyone who has contacted you.

Avoid giving away too many personal details online. Revealing your full name, date of birth and home address may lead to your identity being stolen.



Never give personal details to people who have contacted you or engage in any conversation with them. The below support will assist you in blocking and preventing unwanted calls:

- Change Telephone Numbers:** Contact phone provider and request them to change your telephone number.
- Stop International Calls:** You can limit calls calling you to UK calls only. If international numbers aren't required you can contact your network provider to stop these numbers from calling you.
- Telephone Preference Service (TPS):** Free opt-out service for individuals who do not want to receive unsolicited calls. Tel: **0845 070 0707** or visit: **www.tpsonline.org.uk**.
- True Caller:** For mobile phones you can download the **True Caller** app from any smart phone app store. Register your details and this will significantly reduce these cold callers coming through.
- Call Blocker phones:** BT4000 Advanced Nuisance Call Blocker (details provided on attached sheet) is an example of what nuisance call blocking aids are available on the market.
- Network Provider:** BT, Sky & TalkTalk provide free services to reduce unwanted calls (this is separate to the TPS service).
- Citizens Advice/Trading Standards:** If none of the call reducing options work Tel: **0345 404 0506** or call the police on **101** at any time. Trading Standards respond immediately where any Rogue Trader is present and give advice/support to all affected by rogue traders.



The below support will assist you with: Arranging mail re-direction if required by next of kin/family member, prevent and stop scam mail. Going forward do not to open any more scam mail and if you have an outdoor letter box please consider an indoor one to prevent theft of your mail/details:

- Mailing Preference Service (MPS):** Free register for individuals who do not want to receive unsolicited contacts by post. Tel: **0845 703 4599** (MPS registration line) or visit: [www.mpsonline.org.uk](http://www.mpsonline.org.uk).
- Royal Mail:** Can report scam mail by posting directly to **FREEPOST SCAM MAIL** and/or Tel: **0345 611 3413** or Email: [scam.mail@royalmail.com](mailto:scam.mail@royalmail.com).
- Think Jessica:** Protects elderly & vulnerable people from scams both postal & telephone. Can arrange for trading standards to pay a visit. Email: [advice@thinkjessica.com](mailto:advice@thinkjessica.com) or visit <http://www.thinkjessica.com>.

## Advice (Recommended where applicable) - Part 2



Don't buy from the door step, genuine companies or charities will not knock on your door. Display a no cold calling sticker outside your door and always report suspicious activity immediately.

- Citizens Advice/Trading Standards:** Call when anyone has tried to sell to you on your door step immediately. Tel **0345 404 0506** or police on **101** at any time. Trading Standards respond immediately where any Rogue Trader is present and give advice/support to all affected by rogue traders.
- Checktrade:** For trading standards approved local traders and services. Tel: **0333 0146 190** or visit: [www.checktrade.com](http://www.checktrade.com). There are other trader lists that are available, and operate within the area, but trading standards in Nottinghamshire only check the traders on this list.



Tech support won't call you. Don't ever allow remote control to your computer or device as fraudsters use this tactic to gain access to your bank accounts and transfer themselves all of your money.

- Email:** Be careful with any unexpected emails, practically where the senders unknown. Don't open any attachments or click on any links sent.
- Change E-mail account if required:** To do this, generate a new account with your chosen provider. We recommend updating sites with new information for promotional offers, transaction invoicing and delivery information etc.

- Software:** Ensure all Antivirus/firewall, Malware protection; device APP updates and IOS software are all regularly updated. This will allow all the latest bug fixes to be installed and malicious software to be removed.
- Passwords:** Don't use generic passwords. Try and mix letters, numbers and symbols into your password and have more than one word within this. Using phrases can help and avoid any family or pets names. Visit: <https://howsecureismypassword.net/> to test how secure your password is.
- Device & Web:** Closing unused page/internet tabs and turning off computers when not in use as this leaves your device more vulnerable. Check in your URL (address tab) to ensure the padlock display is visible: 

**General Fraud Prevention Advice:** 

The below sites will give really valuable prevention advice:

- Get Safe Online:** <https://www.getsafeonline.org>
- Scam Smart:** <https://www.fca.org.uk/scamsmart>
- Action fraud:** Fraud and Cybercrime reporting centre. Please don't re-report this incident as already reported. Action Fraud provides fraud prevention advice and alerts on emerging tactics used by criminals. Visit: <https://www.actionfraud.police.uk/> for further fraud protection advice.

## Advice (Recommended where applicable) - Part 3



**Financial Considerations:** 

- A power of attorney to next of kin:** Age UK can assist with this or visit: <https://www.gov.uk/power-of-attorney>
- Contact your bank/CreditCard company:** If account details have been used or compromised.
- Contact local Western Union/MoneyGram:** Let them know about the fraud and request they block future transactions (the bank may be able to do this).
- Credit Reference Agency:** A credit score is a tool used by lenders to help determine whether you qualify for a particular credit card, loan, mortgage or service. You can regularly monitor your credit file activity or report any fraud to a credit reference agency. You can do this using any of the 3 agencies:

**Experian, Equifax, CallCredit.**

With any 3 of the agencies you can ask for a 'Notice of Creation'. This will put a password on your credit file over all 3 credit reference agencies. This prevents anyone from accessing your credit report as you will need your password to access it.

- **Call Credit:** Offer a free service. Visit: <http://www.callcredit.co.uk/default.aspx> or Tel: **0330 024 7574**. With these you can add a 'Notice of Creation' by emailing [consumer@callcreditgroup.com](mailto:consumer@callcreditgroup.com) and providing them with your full name, address and date of birth
- **Experian:** Tel: 0344 481 0800 or visit: <http://www.experian.co.uk/>
- **Equifax:** Visit: <https://www.equifax.co.uk/>

- CIFAS:** Please call **CIFAS** directly and request they add you to their CIFAS database, this will cost £20.00. Please see the below information to help you:  
**CIFAS** - Is a non-profit membership association, a dedicated Fraud Prevention Service within the UK to prevent against fraud through credit and is used by all banks, loan/finance companies, retail credit, insurance, with savings and investments, telecommunications, factoring, and share dealing.

Members share information about identified frauds in the fight to prevent further fraud. CIFAS is unique and is the world's first not for profit fraud prevention data sharing scheme.

If you have been the victim of identity theft or a scam, please report this to your financial services provider. Call **0330 100 0180** to be added to **CIFAS**.

Following specification by the Home Office under the Serious Crime Act 2007, public authorities are able to join CIFAS and share information reciprocally to prevent fraud. For more information visit <http://www.cifas.org.uk>

- ID Material Compromised:**
- **Passport:** Passport photo or copy of passport sent – Tel: **0300 222 0000**
  - **Driving licence:** If this is compromised recommend contacting insurance company to advise should they be receive any claims of the victim crashing in to them
  - **National Insurance number:** Contact the Inland Revenue to advise of the compromise. Tel: **0300 200 3500** (Mon - Fri: 8am to 8pm and Sat: 8am to 4pm)

## Advice (Recommended where applicable) - Part 4



### Financial Advice/Support Services:



- Money Advice Service:** Provides information and guidance on money management. Tel: 0300 500 5000 or [www.moneyadvice.service.org.uk](http://www.moneyadvice.service.org.uk)
- Citizens Advice:** Free legal advice in some parts of England. Free general support, advice and guidance. Call **0344 411 1444** or visit [www.citizensadvice.org.uk](http://www.citizensadvice.org.uk)
- Welfare Rights:** Provides free advice and help with claiming correct or emergency benefits, tax credits and advice on managing debt. Visit: [www.nottinghamcity.gov.uk/welfare/rights](http://www.nottinghamcity.gov.uk/welfare/rights)

### Wellbeing and Care Support:



- Age UK:** Advice and information, smoke alarms or improved security for people in later life, Tel: **0800 169 65 65** 8am to 7pm every day. Visit [www.ageuk.org.uk](http://www.ageuk.org.uk)
- Fire Service:** If fire alarm assistance is needed you can do a fire-service referral: <https://www.notts-fire.gov.uk/home-safety-check>. If anyone was to take this action on your behalf consent will need to be given.
- Catch 22 - Nottinghamshire Victim Care:** When affected by fraud/crime - Visit: [www.nottsvictimcare.org.uk](http://www.nottsvictimcare.org.uk) or Tel: **0800 304 7575** or **0115 934 2605** (Mon –Fri - 8am-8pm and Saturdays 9am-5pm) or email: [admin@nottsvictimcare.org.uk](mailto:admin@nottsvictimcare.org.uk)
- The Silver Line:** Open all day every day they are a free and confidential helpline who offer advice and friendship through their helpline and services. Tel 0800 4708090 or visit [www.thesilverline.org.uk](http://www.thesilverline.org.uk)
- Samaritans:** Whatever you're going through, call free 24 hours a day by calling from any phone on **116 123**.  
You can call 24 hours a day. If you need a response immediately, it's best to call on the phone and is FREE to call.
- Metropolitan Connect Line Metropolitan Connect:** Provides free practical advice, connections to services and short term support (up to 3 months) to maintain independence. Tel: **0115 939 5406** or E-mail: [connect@metropolitan.org.uk](mailto:connect@metropolitan.org.uk). See below for further detail on these services:
  1. **Improved physical, emotional or mental health and wellbeing** - Rediscovering skills and interests, exercise groups, preventing falls, keeping active, finding carers, help to manage long term health conditions including dementia
  2. **Maintaining independence** - Support to find local services, opportunities and resources to help improve self-confidence and give people more control
  3. **Managing money** - Support to budget effectively and manage income and expenditure
  4. **A safe and secure home** - Advice and support on anything from repairs and gardening to home security; aids and adaptations to looking at the options for moving home
  5. **Getting involved in the local community** - Support finding local activities, clubs, groups and leisure facilities
  6. **Befriending and social activities** - Getting in touch with old friends and meeting new ones

## Advice (Recommended where applicable) - Part 5



- How to delete personal information from 192.com and other areas online:**  
-   

By scraping through public databases like the electoral roll, websites such as 192.com are able to collate your address, home phone number and more details all in one place. For a small fee, anyone can then discover a large amount of information about you that you may have considered relatively private.

So, if you'd rather people didn't know how much you paid for your current property or other personal details, read on to find out what 192.com knows about you and how to delete your information from the internet.

### **What does 192.com know about me?**

Anyone can register for an account with 192.com and by doing so you'll be able to obtain several key details about a person's identity. By paying extra for one of the site's 'Background Reports' it claims to be able to provide (among other things) your:

- **Full Address**
- **Age Guide**
- **Telephone Numbers**
- **Alive or Dead Status**
- **Neighbours**
- **Company Financials 2002-2013**
- **County Court Judgments**

How to remove your personal details from the web in three key steps:

#### **1. Make your phone number ex-directory:**

To avoid having your phone number listed on websites, you need to contact your phone company to have yourself made ex-directory. This also means your number and address won't appear in local telephone directories. For BT call free by calling: 0800 800 150 (between 8.30am and 5pm, Monday to Friday).

#### **2. Get taken off the electoral register:**

The electoral register is where sites like 192.com garner the majority of your personal details. To erase yourself from its published incarnation, you'll have to contact your local council or tick the relevant box on the annual voter registration form. This will also stop directory services accessing the information in future.

#### **3. Submit a takedown request to 192.com:**

Information already collected and published by 192.com will remain live until you request it be taken down. In the case of 192.com, you need to fill out its record removal form (<http://statics.192.com/rel-4b1442/downloads/C01.pdf>) by printing it and then emailing or posting it back to the company on:

##### **Email:**

[feedback@192.com](mailto:feedback@192.com)

##### **Address:**

Customer Services, 192.com, Unit 8-10 Quayside Lodge, William Morris Way, London, SW6 2UZ

# C01: Record Removal Form



To remove your details please complete the form and return by either:

**Email:** [feedback@192.com](mailto:feedback@192.com)

**Post:** The C01 Requests Administrator,  
192.com Ltd, Unit 8 Quayside Lodge,  
William Morris Way, London, SW6 2UZ

192.com is the UK's leading people finding website.  
The personally identifiable information found on 192.com has been  
obtained from various public sources including the edited Electoral  
Register and the Telephone Directory

On receipt of this form we have 21 days to remove your record  
under the Data Protection Act 1998.  
However we do aim to remove all records within 7 days.

## Details to be removed

We can only remove your record if the information given on this form matches the details we have on 192.com

### PRIMARY ADDRESS

SURNAME:

FULL ADDRESS:

POSTCODE:

### PREVIOUS OR ALTERNATIVE ADDRESSES

FULL ADDRESS:

POSTCODE:

FULL ADDRESS:

POSTCODE:

SIGNED:

DATE: \_\_\_/\_\_\_/\_\_\_

## 192.com and search engines

When we remove a record from 192.com this does not automatically remove the link as shown on Google and other search engines. Once your record is removed, if anyone clicks on the link on Google the page they are taken to will not show your record.

## Unwanted marketing calls and posts

192.com is not used for direct marketing and removing yourself from 192.com will not stop you from receiving unwanted marketing calls or post.  
To stop receiving unwanted direct marketing please visit [www.tpsonline.org.uk](http://www.tpsonline.org.uk) or [www.mpsonline.org.uk](http://www.mpsonline.org.uk)