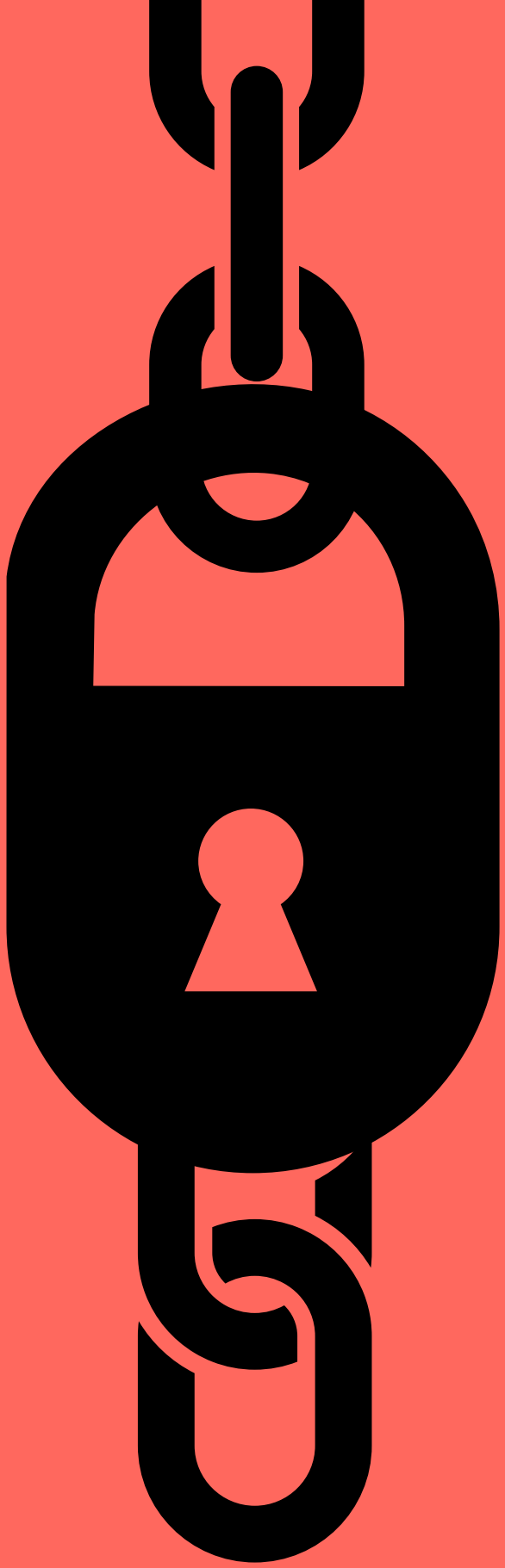

# FRAUD PROTECTION TOOLKIT

The ultimate guide on how to minimise the risk of fraud

THAMES VALLEY POLICE

www.thamesvalley.police.uk

# Introduction from Detective Inspector Duncan Wynn

**Central Fraud Unit**

Becoming a victim of fraud can be both frightening and overwhelming. It can leave you with worries about money, and may also evoke other feelings such as a loss of identity and direction, and not knowing which way to turn for help. It can prompt feeling powerless which can be amplified by worries about the possibility of future fraud and being unsure about how best to protect yourself. I am in no doubt that there is excellent fraud prevention advice already in existence, but much of it relies on the need for individuals to remember a series of information for any range of potential future situations where you may be on the other end of a communication with a fraudster.

My team and I place great emphasis on taking positive action to block the routes of communication often exploited by criminals (Also known as an 'enabler' or 'gateway' to fraud). This booklet will provide you with ways in which you can be a part of that positive action, empowering you to take steps to feel back in control, and also practical ways in which you can keep both your financial and emotional wellbeing safe. Please use this booklet in any way that works for you, for example if telephone calls are an area where you feel a little vulnerable, or where you'd like to increase your self-protection, then start with this. It may also help to keep this guide by the telephone, on the fridge or somewhere else handy so that it remains easily accessible to you. The more positive steps you take then the more you will feel more in control and make it harder for fraudsters to use those routes as a gateway to fraud.

Please remember that it is never your fault if you have been a victim of fraud. You are not to blame and there is no shame. Fraudsters will use techniques designed to make you feel distressed, vulnerable, lonely and isolated. This can lead you to unfairly place blame upon yourself.' You did not 'fall' for the fraud and full responsibly always lies with the criminals. You are not alone.

Emotional support is available from Victims First. Finally, please do share this booklet and the information in it with your family, friends, neighbours and communities because when we unite we stop the loneliness that fraudsters want to exploit, we refuse to allow the blame and shame, and we become much more powerful in the fight against fraud.

# How to Minimise Fraud Risk

**Have you been a victim of fraud?** → **NO** → This guidance, if followed, will still help to safeguard you from fraud.

↓

**YES** → Please report the incident to both your financial provider and Action Fraud.

↓

**Next**

↓

Please start with pages 4 and 5 in order to secure both your personal and financial information and page 6 for recovering monies lost to fraud.
Next – Let's take some action to give you more control over the contact routes and minimise fraud risk

↓

**How was contact made with you?**

|  |  |  |  |
|---|---|---|---|
| **Telephone** | **Mobile/ Social Media** | **Email/ Computer** | **Post/ Doorstep** |
| ↓ | ↓ | ↓ | ↓ |
| Page 7 | Page 8 | Pages 9-10 | Page 11 |

***the more contact routes you control, the more you can minimise the risk of fraud.***

# Personal Information

**Criminals will try to get hold of your personal information as it makes it possible for them to take out financial products like loans or credit cards and/or services in your name, leaving you liable for the cost.**

- Treat your personal information like your house or car keys and never hand it over to strangers, recent acquaintances or anyone asking for your details where it's not strictly necessary.
- Always be mindful about what personal information you share online such as through any social media accounts.
- Only give out your personal information after very careful consideration. It's ok to reject, refuse or ignore any requests whilst you think it through.

**Minimise fraud risk and control your personal information by:**

- [ ] Check if identity fraud has been committed by checking all 4 UK credit reference agencies (Equifax, TransUnion, Crediva and Experian). For a fee all 4 reports can be checked at once at Check my File.
- [ ] Protect against identity fraud and from criminals using your personal details to apply for products and services in the future by applying for CIFAS Protective Registration which costs £25 for 2 years.
- [ ] Find out what to do if identity fraud is confirmed as being committed.
- [ ] Notify any relevant organisations where originals or copies (including photos) of documents/identification may have been provided (DVLA, HM Passport Office).

# Safeguard your Finances

**Criminals will try different tactics to get at your finances.**
**Warning signs for fraud include:**

- Asking you to withdraw money or transfer money to a different account.
- Asking you to reveal your full banking password or PIN.
- Asking you to reveal your OTP (one time password).
- Asking you to purchase jewellery/expensive items or iTunes vouchers for an investigation.
- Sending a courier to collect money, cards or personal items.
- Asking you to provide cash so it can be checked for fingerprints.

! **The Police or your bank will never ask you to do any of these things.**

- Treat your bank cards, PINs and login details like your house or car keys and never hand them over to strangers or recent aquaintances.
- Keep all your financial information such as bank details, PINs and banking passwords safe.

**Minimise fraud risk and control access to your financial information by:**

- [ ] Report the fraud to your bank so cards and account numbers can be changed and a refund can be discussed if applicable.
- [ ] Ensure that Action Fraud have been informed (Action Fraud do not investigate).
- [ ] Consider how a co-signatory on your account may reduce the scope for fraud.
- [ ] Consider how appointing a lasting power of attorney gives you more control over what happens to you and your finances in the event of an accident or illness.

# Recovering Monies Lost to Fraud

**Please note that any decision to refund any monies lost to fraud lies entirely with the bank/financial institution concerned. Action Fraud or Police form no part of the decision making process.**

Fraudsters will often pose as being able to recover monies lost to fraud for an upfront fee which is known as Recovery Fraud, so please ensure that steps are taken to verify any route you may choose to pursue.

The Financial Conduct Authority also has information on Financial Investments.

**Minimise fraud risk and control access to your financial information by:**

- [ ] If money was transferred via bank transfer please refer to What to do if you're the victim of a bank transfer (APP) scam - Which?
- [ ] If payment took place via credit card please refer to Section 75 of the Consumer Credit Act - Which?
- [ ] If payment was made via a debit card, check to see if you can claim for a refund under a voluntary scheme called Chargeback using this letter template .Debit card payments and purchases are not covered by section 75 of the Consumer Credit Act.
- [ ] If the payment was made via an online payment platform such as PayPal, Apple Pay or Google Pay check to see if you can make a claim under their dispute resolution process. Terms and conditions will apply.
- [ ] If a purchase took place via an online marketplace check to see if you are covered under any buyer protection scheme. Please see eBay UK - Buyer Protection Guide ,What is Buyer Protection? - Shpock and Buyer Protection (vinted.co.uk).
- [ ] Contact Citizens Advice to discuss how it may be possible to get your money back.
- [ ] Consider making a court claim or using mediation services Make a court claim for money - GOV.UK (www.gov.uk) (A claim to the small claims court may be done directly or via a solicitor).
- [ ] Consider using a Financial Advisor or Claims Management Company regulated by the Financial Conduct Authority (Check the Financial Services Register to ensure they are regulated. It is also possible to check to see if an individual or company is already known to the FCA for being unregulated Unauthorised firms and individuals | FCA).

# Contact via Telephone

**Criminals will use the telephone most often to contact potential victims. Warnings signs for fraud include:**

- Threatening to arrest you if you do not do something such as withdraw cash or transfer money to pay a ‘fine’ or ‘fee’.
- A recorded message asks you to call a number to ‘claim a prize’.

! **No genuine organisation/institution would ever use threats like this.**

**Minimise fraud risk and control this contact route by:**

- [ ] Contact your service provider to discuss what call blocking solutions may be available.
- [ ] Request your service provider makes any landline numbers ex-directory.
- [ ] Discuss changing your telephone number with your service provider.
- [ ] Consider purchasing a handset with caller display so withheld/unrecognised numbers can be ignored.
- [ ] Register with the Telephone Preference Service to stop unsolicited and marketing calls (Applies to mobile too).
- [ ] If scam/nuisance calls still persist then consider purchasing an external call blocker. Trading Standards recommends trueCall.
- [ ] Report Nuisance calls to ICO - Information Commissioners Office who collate information for potential enforcement action.

# Contact via Mobile Phone /Social Media and Messaging Services

**Criminals can make SMS messages and phone calls appear genuine.**

- Never click on link provided in SMS messages or provide personal information, before taking steps to verify the source of the message.
- Visit Mobile phone fraud | Action Fraud for further information on keeping safe.
- Discover Date Safe Tips from the Online Dating Association to ensure a safe online dating experience.
- Learn more about Staying Safe from Romance Fraud in our e booklet.

**Minimise fraud risk and control this contact route by:**

### Calls

- [ ] Block any unwanted numbers via your handset.
- [ ] Some handsets will enable specific numbers to be blocked. A service provider will be able to advise how to do this.
- [ ] Register with the Telephone Preference Service to stop unsolicited and marketing calls.
- [ ] Report spam calls by texting 'CALL' plus the number that called you to 7726. This will alert your service provider to investigate the number and potentially block it, if it's found to be a nuisance.

### SMS/Text Messages

- [ ] Spam texts can be forwarded for free to "7726" which is run by Ofcom (This spells "Spam" on the telephone key pad).

### Social Media and Messaging Services

- [ ] Secure e mail accounts and ensure social media privacy and security settings are set to manage your digital footprint.
- [ ] Block unwanted contact/messages. For information about doing this on specific platforms, follow these links - Facebook, Twitter, Instagram, YouTube, Snapchat, WhatsApp, Discord, Hangouts, TikTok, LinkedIn.
- [ ] Make use of the reporting facilities on each platform to report unwanted contact or untoward behaviour - Facebook, Twitter, Instagram, YouTube, Snapchat, WhatsApp, Discord, Hangouts, TikTok, LinkedIn.

# Contact via Email and Websites

**Fraudsters will frequently spoof email addresses and websites.**

This means that an email address can be made to look as if it is from a genuine organisation when in reality it is from a web based address (Gmail, Hotmail, Yahoo, etc.). Just because an e mail or website looks recognisable, it doesn't mean it's the genuine one.

- Check there's a 'closed padlock' icon in the browser's address bar when paying for your items. Although the padlock icon doesn't guarantee that the retailer itself is legitimate/reputable (and that their website is secure). It does mean your connection is secure.
- Always take extra steps to be certain before proceeding and never provide copies or photographs of personal documents to a stranger online or in response to a request out of the blue.

**Minimise fraud risk and control this contact route by:**

- [ ] Open the full email or hover your mouse over the display email to check the display and sender e mail address correspond. A mismatch is a good indicator of an email that should be treated as spam.
- [ ] Avoid clicking on links in that you haven't checked out first. Report any suspicious e mails to the Suspicious Email Reporting Service by forwarding them to report@phishing.gov.uk
- [ ] Searching on the correct exact full website address can reduce the risk of ending up on a fraudulent website. Remember that the top results in search engines are sold as advertising space so the top result is not always the authentic website.
- [ ] Determine if a website is likely to be legitimate or a fraud by using by using the Check a website facility from Get Safe Online.
- [ ] Please see the "Computer" section *(page 10)* for additional advice on how to secure your online presence.

# Contact via Computer or Tablet

**The anonymity of the internet allows criminals to be whoever they want to be online. Just because someone says it's true, it doesn't mean that it is. If it sounds too good to be true then it probably is, however, it doesn't have to sound amazing to be a fraud.**

- Use a Google or TinEye reverse image search to double check a situation.
- Be sure to follow Key Cyber Protect Advice from the National Cyber Security Centre.

**Minimise fraud risk and control this contact route by:**

- [ ] Use a strong and different password for your email using 3 random words: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
- [ ] Turn on 2-Step Verification (2SV) for your email: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email
- [ ] Save passwords in your browser: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
- [ ] Backing up your data: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data
- [ ] Install the latest software and app updates: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates
- [ ] Advice for those concerned a device has been infected: www.ncsc.gov.uk/guidance/hacked-device-action-to-take
- [ ] Find out how you can use social media safely. www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely
- [ ] How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you: www.ncsc.gov.uk/collection/phishing-scams
- [ ] Report any suspicious e mails to the Suspicious Email Reporting Service by forwarding them to report@phishing.gov.uk

# Contact via Post to Home Address

**Criminals also try tactics to scam you by sending you fraudulent mail. Fraud warning signs can include:**

- Mail that pressures you to respond by telling you that you need to 'act fast' or that 'an urgent response is required', particularly if this is in order to receive a pay-out or a prize.
- Find out more about different types of postal scams at Think Jessica.

**Minimise fraud risk and control this contact route by:**

## Post

- [ ] Opt out of the Open Voters Register which is available to anyone who wants to buy a copy.
- [ ] Remove your details from mailing lists by registering with the Mailing Preference Service.
- [ ] It is possible to stop getting junk mail by following this guidance from The Citizens Advice Bureau.
- [ ] Report any scam mail you receive to Royal Mail.
- [ ] Set up a Royal Mail Postal Redirection to your new address when moving to ensure your mail moves with you.
- [ ] Royal Mail can redirect mail in special circumstances where a power of attorney, deputyship or other similar legal authority exists.
- [ ] Set up a HM Land Registry - Property Alert for any registered property that could be at risk of fraud.
- [ ] Consider asking a relative or trusted friend to help you check and screen the post.

# Contact via the Doorstep at Home Address

**You may also get doorstep callers offering their services or products for sale. This can also include people posing as bank officials or couriers claiming to need to collect bank cards, cash or jewellery.**

**Tactics may involve:**

- You are asked or pressured to hand over money at the door.
- You are asked or pressured to hand over bank cards, financial information, PINs, or withdraw cash.

**The below tips will help you feel better equipped to deal with any unexpected doorstep callers:**

- Say 'No' to doorstep callers. Many people worry about appearing rude if they say no to doorstep callers. It is always ok to say no thank you.
- Taking time to think and talk to someone you trust outside the situation, when you are asked to do something.
- Never sign on the spot if you are seeking trades persons– shop around. Get at least three written quotes to make sure you're not being ripped off.

**Minimise fraud risk and control access to your financial information by:**

## Doorstep

- [ ] Install a "no cold calling" sign. If a doorstep caller still knocks then it's a good indication of when not to engage with someone.
- [ ] Discuss if a neighbour may help you screen visitors and install a sign directing doorstep visitors to this neighbour.
- [ ] Consider a CCTV camera in your porch (with a warning sign) or purchasing a smart/ Ring doorbell (local Trading Standards are able to advise further in this area).
- [ ] Consider registering with the free support service offered by energy suppliers and network operators. The Priority Services Register is able to set up an identification and password scheme to help you identify if a doorstep caller is genuine.

# Fraud Minimisation Checklist :

**Minimise becoming a victim of fraud. The below checklist may help you keep track of any actions'**

- **Safeguarding personal information** **(see page 4)**
- **Safeguarding your finances** **(see page 5)**
- **Safeguarding the telephone** **(See page 7)**
- **Safeguarding mobile phones/social media** **(see page 8)**
- **Safeguarding the computer or tablet** **(see page 10)**
- **Safeguarding the post** **(see page 11)**
- **Safeguarding the doorstep** **(see page 12)**



# Useful Website Addresses

**Thames Valley Police fraud advice:** www.thamesvalley.police.uk/advice/advice-and-information/fa/fraud

**Victims First :** www.victims-first.org.uk/crime-info/guidance-and-support/fraud/

**Action Fraud A-Z:** www.actionfraud.police.uk/a-z-of-fraud

**National Cyber Security Centre:** www.ncsc.gov.uk

**National Trading Standards:** www.nationaltradingstandards.uk

**Friends Against Scams:** www.friendsagainstscams.org.uk

**Age UK scams and fraud advice:** www.ageuk.org.uk/information-advice/money-legal/scams-fraud

**Take Five to Stop Fraud:** www.takefive-stopfraud.org.uk/advice/general-advice

**Don't Be Fooled money mules advice:** www.moneymules.co.uk

**Citizens Advice:** www.citizensadvice.org.uk/consumer/scams/reporting-a-scam

THAMES VALLEY POLICE

VICTIMS FIRST

Care | Empower | Recover

ActionFraud

National Fraud & Cyber Crime Reporting Centre

0300 123 2040

Designed by Corporate Communications CC5809_V4_08/22