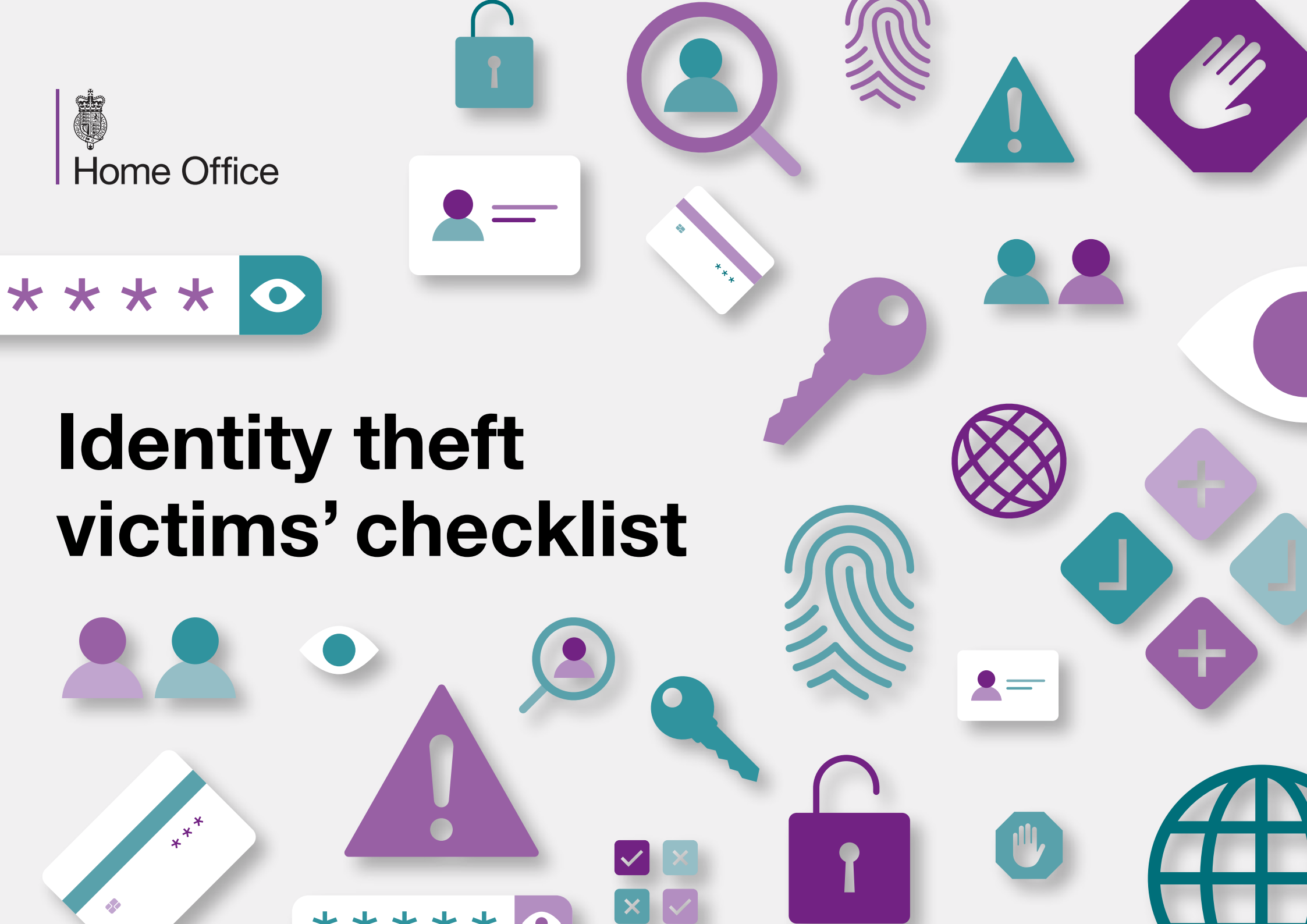
Home Office

Identity theft victims' checklist



Identity theft victims' checklist

Purpose: The purpose of the checklist is to provide victims and organisations with consistent helpful messaging and advice on what do when identity theft has occurred and how to prevent it from happening again.

The checklist is split into three parts:

1

A checklist dedicated to **victims** who have discovered they have been affected by ID theft.

2

A checklist that **organisations** can use when engaging with an individual affected by ID theft.

3

Advice on how to prevent revictimisation.

Checklist – victim journey

This checklist is for individuals who have discovered that their details have been used fraudulently and they are a victim of identity theft.

When you have been made aware that you may have been a victim of identity theft:

Take immediate measures to protect your accounts:

- Contact your banks and ask them to withhold pending transactions.
- Ask your bank about their process for claims.
- Contact any companies/ accounts that have been affected (e.g. credit card companies, store cards, phone and utility companies).
- Change your passwords and pins, including email addresses and social media accounts.
- Contact Action Fraud to tell them about the fraud that has taken place against you.

Contact relevant organisations to inform them that you have been a victim of identity theft:

- Use a credit referencing agency (e.g. Experian, Equifax and Transunion) to find out if any accounts have been opened without your consent and ask them to monitor your account.
- Check your personal documents:
  - if your drivers licence is lost or stolen contact DVLA
  - if your passport is lost, stolen or compromised contact HMPO
  - if your benefits have been affected contact DWP
  - if your company has been affected contact Companies House.

Additional steps to protect yourself:

- We recommend you use a credit checking service to ensure your details have not been used to open accounts you are unaware of.
- You may wish to sign up for further account protection such as Cifas Protective Registration (fee of £25 for two years).
- Contact Victim Support or Citizens Advice if you need further support, including emotional support.
- Take advice from the checklist on preventing revictimisation.
- Inform friends and family you have had your identity stolen.

Helpful links:

Help protect yourself from cyber criminals

Cifas – Protective Registration

Action Fraud

Checklist – organisation journey

This checklist is to help organisations share consistent advice and inform their customers of the support available, and to guide them in receiving the help they need to protect themselves in future.

Advice for when an individual has discovered that they have been a victim of identity theft

Advice to give to victim:

- Advise victim about immediate measures that can be put in place to protect their account. (e.g. withhold pending transactions, change passwords and pins and secure their wi-fi).
- Refer victim to Action Fraud.
- Assess victim vulnerability and provide support or signpost to a victim support service or Citizens Advice.
- Inform victim of the process for claims of bank/finance fraud process. Alternatively, advise victim of fraud reimbursement process for your organisation.
- Inform victim how to restore their accounts if they have been compromised.

Advise victim to take next steps:

- Contact credit referencing agency (e.g. Experian, Equifax and Transunion). Strongly encourage the opening of a credit checking service to ensure your details have not been used to open accounts you are unaware of.
- Contact creditors with whom they have an account (e.g. banks, credit card companies, store cards, phone and utility companies). If these accounts have not been affected, advise them that they should monitor their accounts to ensure they remain protected.
- Change passwords associated with accounts that could be compromised. Using a password manager can securely generate and store your passwords.
- Inform victim of identity protection services, (e.g. Cifas).
- (Include sector specific personalised messaging here that relates to your organisation.)

Helpful links:

Help protect yourself from cyber criminals

Cifas – Protective Registration

Action Fraud

Checklist – preventing revictimisation

This checklist will help victims of fraud protect themselves in the future and help to prevent revictimisation.

Advice to protect an individual from revictimisation

Steps to consider taking:

- You may wish to sign up to **Cifas Protective Registration**.
- You may wish to register with Companies House and sign up to their electronic filing, PROOF and monitor services.
- Contact HMPO, DVLA, GRO and DWP if the fraud involved stolen government documents or benefits.
- Check if this is fraudulent material by using Citizens Advice "check if something might be a scam".

Protecting personal information:

- Keep your personal information, credit cards, passwords and pin numbers in a safe place (preferably a lockable drawer or safe) and don't share these details with people or companies you don't know or trust.
- Never throw away bills, receipts, credit or debit card slips, bank statements or even unwanted post without destroying them first, ideally with a shredder.
- Always protect your post, especially if you live in a building where other people can easily access it. When you move house, redirect your mail from your old address to your new one for at least a year.
- Check all your statements and financial records as soon as they arrive and report any discrepancies straight away.
- Regularly obtain and monitor your credit report and check it for any discrepancies.
- Check security recommendations for your passwords and update accordingly, this is particularly important for email accounts.
- Data removal list – opt-out of data collection on websites and ask Google to remove personal information.

Stay safe online:

- Be wary of what information you publish online and who you make it visible to, pictures of your home, workplace or school, address, date of birth or full name. Also be wary of online quizzes which ask questions for the same answers as your security questions.
- Make sure your computer is protected from the threat of online attacks and check your privacy settings.
- Change your passwords regularly – a password management app can help with this.
- Think before responding to unexpected emails, social media requests and texts asking for personal information.
- Take a look at the NCSC cyber campaigns – **Cyber Aware**.

Helpful links:

Help protect yourself from cyber criminals

Action Fraud

Useful links

Action Fraud

Cyber crime – National Crime Agency

Protective Registration | Identity Protection Service | Cifas

Fraud – Victim Support

Citizens Advice