Contents

3 About this guide

4 Introduction

5 What to do if you think you have responded to a scam

About this guide

This guide has been brought to you by the National Trading Standards Scams Team and the National Centre for Post Qualifying Social Work and Professional Practice at Bournemouth University, working in partnership with Lloyds Bank, Halifax and Bank of Scotland. Our teams have been leading research on scams and fraud across the UK. We work closely with people who have fallen victim to scams and we use their insights to help protect others. The advice in this guide is based on our knowledge and practical experience of what works.

PART ONE:
STOPPING CRIMINALS FROM REACHING YOU

Mail scams

If you receive scam mail, you may want to consider reducing the amount that reaches you. Ask a friend or relative to go through your post with you and help identify any scams. Remember that scam mail can come in many forms, including lotteries, prize draws, catalogues, and clairvoyant scams. You can reduce the amount of junk and scam mail you receive by following these tips:

- Become a **Scam Marshal** and send any scam mail you receive to the National Trading Standards Scams Team to help them investigate and stop the criminals behind scams. You will receive information to help you identify scams. Sign up online at ZZZ or write to 'FREEPOST NTSST MAIL MARSHAL'.
- Sign up to Royal Mail's paid-for **redirection service** to have your post delivered to a trusted friend or relative. Apply online at **www.royalmail.com**
- Sign up to the 0DLOLQ3UHIHUHQFH6HUYLFH036. Although the MPS does not stop scam mail, it will reduce the amount of direct marketing mail that you receive. The MPS is a free service. For more information and to register visit **www.mpsonline.org.uk** or call **0207 291 3310**.

Doorstep scams

To stay safe from doorstep scams, never trade with people on
willra2e with peopp (e)10 0.1 (en'tmbep (t)15((emet sur en(emember a cemembonle ont su9 80 (ouT*0.10.1 (e e on)]ght fr)2t suwr)22 fr)22 ()81 e.3He222tmbepa2

Internet scams

- Use a different, strong password for every online account in case one gets hacked. You can use a **password manager** to help you store your passwords securely – this means you'll only have to remember one strong master password.
- Enable **multifactor (or two-factor) authentication** on online accounts like your email. This is a safer way to log in and requires another source such as a mobile phone to authenticate that it is you logging on to your account.

What is a Lasting Power of Attorney (LPA)?

Types of Lasting Power of Attorney