

Cluberly Fraud Awareness Guidance

Version: V1.2

Effective Date: 10/09/2025

Last Updated: 23/02/2026

1. Our Approach to Security

Your financial security is our top priority. When accessing your Cluberly account, we take steps to ensure it's really you.

- Login Details: You'll receive unique login credentials. Never share these with anyone.
- Memorable Questions: If you contact our support team, we may verify your identity using security questions.
- Information Requests: We will never ask for your password or PIN. If we need to contact you, we'll email you first.

2. How to Report Fraud

If you notice suspicious activity, contact us immediately:

- Report Fraud: 020 4623 8702
- Lost or Stolen Cards: 020 4623 8702
- Suspicious Emails/Phishing: abuse@cluberlyapp.com

You can also use the in-app chat to report concerns.

3. How to Protect Yourself from Fraud

Stay safe by following these tips. If in doubt, don't act. A genuine company will never pressure you to provide personal information.

4. Keep Your Contact Details Updated

Ensure your mobile number and email address are kept updated on the Cluberly App so that we can alert you to unusual activity.

5. Tips for Using Your Cluberly Account and Card Safely

When Accessing Your Account

- Use antivirus software and a firewall.
- Keep your device updated.
- Use secure networks.
- Use strong passwords.
- Never share passwords, PINs, or emoji login codes.

When Using the Mobile App

- Only install apps from recognised app stores.
- Check app ratings and reviews.
- Review app permissions carefully.
- Treat your phone like your wallet.

When Shopping Online or In-Store

- Research unfamiliar retailers before purchasing.
- Don't reply to unsolicited emails.
- Check for a secure connection (padlock symbol and https://).
- Always log out after use — closing the browser isn't enough.
- Keep your PIN safe and shield it when entering.
- Regularly check your statements.

6. Device Disposal

If donating, reselling, or recycling a device, fully remove all data and apps to prevent unauthorised access.