Digital wallet abuse

Extract from NCA Amber ALERT of September 2025 (Reference 0777 - NECC)

Overview

This alert aims to contribute to the understanding of the threat of digital wallet abuse and to assist the accountancy sector in playing its role in preventing digital wallet fraud.

Background

Digital wallet fraud is a rapidly growing financial crime where criminals add stolen bank card details to mobile wallet apps—such as Apple Pay or Google Pay—without the cardholder's knowledge. Once added, these wallets can be used to bypass standard banking fraud controls, enabling fraudulent purchases and cash-outs at scale.

Fraudsters exploit the verification process for linking a card to a digital wallet. This typically requires a one-time passcode (OTP), sent by the bank to the legitimate cardholder by SMS. Criminals use various lures (via phishing, malicious online advertisements, user-user social media content) and social engineering to deceive victims into revealing these OTPs, often without realising they have authorised the wallet registration. Once registered, many transactions using the digital wallet rely on the security of the phone handset that they are provisioned to, and do not require further cardholder authorisation and face fewer restrictions than physical card payments.

Key Threats and Trends

1. Scale and Sophistication

In 2024, UK Finance recorded over 2.5 million cases of remote purchase fraud, much of it linked to social engineering and digital wallet exploitation.

2. Criminal Process

Digital wallet fraud follows a multi-stage model:

- Victims are targeted through phishing sites or fake online retailers.
- Personal and banking details are collected, often via real-time monitoring.
- Victims are manipulated into providing OTPs.
- Stolen cards are added to criminal-controlled digital wallets and monetised. (Victims are often unaware their cards have been added to criminal-controlled wallets until monetisation).

3. Phishing-as-a-Service (PhaaS)

PhasS platforms built by developers based in China'; such as Darcula and Lucid, provide turnkey phishing kits and tutorials via Telegram, enabling non-expert criminals to conduct large-scale UK-targeted campaigns. These kits mimic trusted brands—Amazon, Royal Mail, UK Government— and now use generative AI to scale attacks more effectively. Some phishing kits now auto-generate realistic card images using AI, streamlining the OTP verification process for criminals.

4. Cash-Out Methods

- Online or in-store purchases: Typically, high-resale items or gift cards.
- Device resale: Phones preloaded with digital wallets are sold to other criminals.
- Near Field Communication (NFC) remote relay: Allows criminals to control contactless transactions remotely via an app, using "mules" to make purchases instore without revealing the fraud. Data is sent from the wallet-holding device to a mule's phone, which makes contactless payments at Point of Sale (PoS) terminals. This insulates criminals from detection.
- Fake businesses: Digital wallets are used to process low-value payments through fronts on platforms like Stripe or Zelle.

5. Deliberate Timing

Criminals sometimes delay use of the stolen cards—up to 90 days—after adding them to wallets, to avoid triggering fraud alerts. This lag is shortening but remains part of an evolving risk profile.

How accountancy firms can protect their clients from digital wallet abuse

All OTPs sent via SMS are vulnerable to interception through social engineering and SIM-swap attacks. The accountancy sector should be alert to clients who have revealed OTPs to third parties.

Industry engagement with UK retail banks has revealed those that have already moved away from SMS based OTPs report a near total eradication of digital wallet abuse. Firms and practitioners in the accountancy sector should consider promoting a move away from SMS based OTPs to their clients.

The accountancy sector should be alert to the distribution of phishing kits and point of sale platforms for laundering stolen funds. The banking industry and law enforcement are also increasingly partnering to tackle the abuse of the online advertising ecosystem.

Increasing public awareness and victim education around the risks of sharing OTPs and how digital wallets work may be effective in protecting the UK public. Highlighting campaigns led by the Cyber Defence Alliance, UK Finance, and Cifas will help protect clients. The Stop! Think Fraud campaign helps alert consumers to the most common phishing lures such as courier delivery fees or promises of government refunds, which have been linked to digital wallet abuse.

Suspicious Activity Reporting [SARs]

If you know or suspect ML or TF activity you should make a SAR and include the alert reference **0777-NECC** within the text *in addition* to the ongoing use of the Glossary of Terms, including XXJMLXX. Guidance on reporting is available at: www.nationalcrimeagency.gov.uk

Data Protection Considerations

Please consider your obligations under the relevant data protection regulations and where necessary remove any related personal data from your systems securely and within a satisfactory timeframe.

Disclaimer

The Accountancy AML Supervisors' Group (AASG) accept no responsibility for any loss, damage or expense arising in connection with the use of information in this alert. Any use will be taken to signify agreement to these conditions.

Protecting this document

This document uses the United Kingdom's Government Security Classification System (GSCS) and has been graded as OFFICIAL. There are no specific requirements for storage and it can be considered safe for wide distribution within your organisation and for use in staff training or awareness programmes. However, unless otherwise specified, this information is not intended for general public dissemination and should not be included on public facing websites, external mailing lists, social media or other outlets routinely used by you to deliver information to the public without the prior and specific permission of the NCA Alerts team. We therefore request that you risk manage any onward dissemination in a considered way. This document should be disposed of by cross-cut shredder, pulping or incineration.