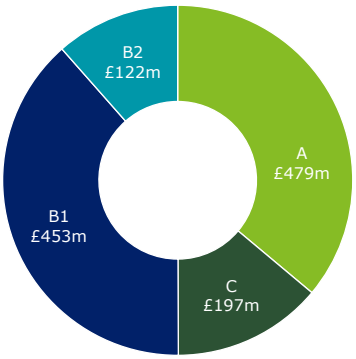
Retail Banking Fraud Sector Charter

Specific fraud risks in the Retail Banking Sector

Fraud loss by type (2020)



A. Authorised Push Payment Fraud (APP)	A criminal tricks their victim into sending money directly from their account to an account which the criminal controls. This covers 'Malicious payee' type fraud, such as investment and purchase scams, as well as 'Malicious redirection' type fraud, such as impersonation and invoice redirection scams. This is the banking industry's primary concern currently. (See actions 1 - 3), (5 - 7)
B. Unauthorised Card Fraud: CNP Other	Captures fraud committed using the information from payment cards issued in the UK. The most significant element of this relates to 'Card not present' (CNP) fraud whereby a criminal uses stolen card details to buy something on the internet, over the phone or through mail order. The adoption of Strong Customer Authentication is expected to significantly reduce the prevalence of this fraud type. (2, 3), (5 - 7)
C. Remote Banking Fraud	A criminal gains access to an individual's bank account through remote banking channels, typically through manipulation of the eventual victim and their device, and makes an unauthorised transaction within the account. (2, 3), (5 - 7)

Key fraud enabler

Money Mule activity	Customer accounts are utilised by criminals to receive and launder the proceeds of illegal activities. (4), (5 - 7)

Actions to tackle fraud risks in the retail banking sector

Action (1) – Driving cross sector fraud engagement to fight APP fraud – by building evidence base		**January 2022**
Objective: Develop evidence base to illustrate the points of origination for fraud suffered by banking customers.	**Action:** UK Finance will co-ordinate the banking sector to capture a consistent set of data points at the point of a fraud being reported or identified. This data will be used to produce analysis of fraud suffered in the banking sector that illustrates points of origination, which will be shared with the Home Office to assist with a cross-sector drive to combat fraud.	**Outcome:** Evidence base established to underpin cross sector engagement.
Action (2) – Develop a cross-sector data breach response plan to protect consumers from fraud		**December 2021**
Objective: Enhance coordination between law enforcement and private sector on data breach fraud prevention steps.	Data breaches can result in fraud through: • **Card Not Present** fraud using stolen bank details; and • **APP** and **Remote Banking fraud** through social engineering from stolen personal data **Action**: To complement existing guidance on mandatory reporting responsibilities, the government will explore the development of a set of actions that the loser of data, law enforcement and other relevant public and private sector bodies should undertake in the event of a data breach.	**Outcome**: Reduced fraud risk through implementation of playbook of standardised actions.
Action (3) – Leveraging technology to increase fraud detection and prevention controls		**June 2022**
Objective: Balancing the efficiency of the customer journey with fraud prevention.	**Action**: UK Finance will support the ongoing review of existing payments architecture, promoting changes that could most effectively be adopted by the sector to aide fraud prevention. The banking industry will also explore promoting better use of existing account features that could be better used to help protect customers.	**Outcome**: Increased use of account features that protect customers form fraud.
Action (4) – Take action to reduce the impact of Money Mules in facilitating fraud		**June 2022**
Objective: Increase effectiveness of deterrents for 'Money Mule' activity and apply consistently.	**Action**: The banking sector will develop a strategy by which it is able to consistently respond to and subsequently reduce levels of **Money Mule activity** across the sector. This will include support from government and law enforcement in increasing the effectiveness of deterrents for identified Money Mules.	**Outcome**: A co-ordinated public-private strategy that reduces the impact of Money Mule activity.
Action (5) - Explore opportunities to enhance fraud prevention and repatriation of funds to victims		**December 2021**
Objective: Banking sector, government and regulators work together to prevent fraud.	**Action**: The banking sector will work with a wide range of partners, including law enforcement, regulators, government and other sectors to identify and address vulnerabilities identified from a shared understanding of the threat. This will include identifying and assessing potential options for operational or policy changes to tackle vulnerabilities, with consideration of legislative and regulatory changes where appropriate and feasible. In addition, the Government will explore the mechanisms needed to (legislative or otherwise) to allow for more effective repatriation of stolen funds to the identified victim, and to enable unlocking of untraceable funds currently held in suspended accounts.	**Outcome**: A collaborative approach between regulators, the government and the banking sector towards fraud prevention.
Action (6) – Increase fraud awareness and change customer behaviours		**March 2022**
Objective: Plan and execute education campaigns to raise consumer awareness and reduce vulnerability.	**Action**: The banking sector will support law enforcement in driving a cross sector communication strategy that delivers a consistent message across several different sectors.	**Outcome**: Increased fraud awareness through cross sector communications strategy, changing customer behaviour to reduce fraud.
Action (7) – Victim Support		**June 2022**
Objective: Encourage victim reporting and improving consistency of victim treatment.	**Action**: The banking sector will work with victim support groups to ensure victims are correctly and consistently advised on where they obtain support in the event they are defrauded. The banking sector will also support the Joint Fraud Taskforce in developing a plan to enable better sharing of victim data across other applicable sectors.	**Outcome**: Consistent victim support to reduce re-victimisation.

Signatories

This voluntary charter is supported by UK Finance on behalf of its members:

- Allied Irish Bank (GB)
- Bank of Ireland UK PLC
- Barclays Bank Plc
- Capital One (Europe) plc
- Citigroup Global Markets Limited
- Clydesdale Bank plc
- Co-operative Bank plc
- Coventry Building Society
- Danske Bank
- Hampden & Co
- Handelsbanken plc
- HSBC Bank Plc
- Investec Bank Plc
- Lendable Operations Limited
- Lloyds Banking Group
- Metro Bank Plc
- Modulr ICB Limited
- Monzo Bank Limited
- Nationwide Building Society
- NatWest Group Plc
- Nedbank Private Wealth
- NewDay Cards Ltd
- Railsbank Technology Ltd
- Revolut Ltd
- Sainsbury's Bank plc
- Santander UK Plc
- Secure Trust Bank Plc
- Starling Bank Limited
- Tesco Personal Finance Plc
- TSB Bank
- Yorkshire Building Society