

PROTECTING CUSTOMERS AND STOPPING FRAUD



The Dedicated Card and Payment Crime Unit (DCPCU) set up

A specialist police unit, fully sponsored by the finance industry, which targets the organised crime groups behind card and payment crime. It has prevented an estimated £540 million in fraud.

The Fraud Intelligence Sharing System established

This highly-secure system enables the banking industry to share information on confirmed, attempted and suspected fraud with law enforcement agencies.



3-D Secure rolled out

The technology provides an additional layer of security when a customer makes a card payment on the internet.

Hanging up on phone scams

A phone system vulnerability exploited by fraudsters to trick victims into believing they are speaking to their bank is shut down following action by the finance industry, Metropolitan Police and telecoms providers.



Take Five to Stop Fraud launches

The national campaign offering advice to help consumers prevent financial fraud, Take Five urges people to stop and think whenever they get a call, text or email out of the blue asking for their personal information or money.

Government joins Take Five to Stop Fraud

The Home Office backs the second phase of Take Five, helping people confidently challenge requests for information by urging them to remember the phrase 'My money? My info? I don't think so.'



Mule Insights Tactical Solution introduced

New technology is brought in which tracks suspicious payments travelling between accounts, helping banks quickly follow and trace stolen money.



Multi-factor authentication

European rules come into force in September requiring payment providers to use multi-factor authentication – such as one-time passcodes or biometrics – for higher-value and higher-risk transactions.



2002

2006

The switch to Chip & PIN

UK card transactions fully switch to Chip & PIN authorisation, instead of a signature. In 2017 counterfeit card fraud losses were down 86 per cent since the 2008 peak. The same, secure Chip technology underpins contactless payments.



2008

2010



Financial Fraud Bureau (FFB) created

The fraud intelligence and data sharing hub, the FFB alerts the industry immediately to any known compromises of bank or card data and works with the police to identify organised crime groups.

2010

2015

Joint Money Laundering Intelligence Taskforce formed

A partnership between banks and the National Crime Agency aimed at tackling money laundering, by enabling banks to share information in a way that would not otherwise be possible.



2015

2016



Joint Fraud Taskforce begins

The finance industry joins with government and the police to crack down on fraud and tackle issues considered too difficult for a single organisation or sector to manage alone.

2016

2017

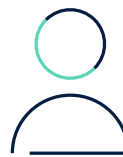
The Banking Protocol rolled out to every UK area

A ground-breaking rapid response scheme enabling bank branch staff to contact police if they suspect a customer is being scammed, with an immediate response to the branch. It has prevented almost £37 million of fraud and led to 336 arrests.



2017

2018



Best Practice Standards come into action

Ensuring those who have fallen victim to authorised push payment scams get the help they need, the new standards include access to staff trained in scam management 24 hours a day, 7 days a week to handle scam complaints.

2018

2018

Text spoofing blocker trialled

A new system aiming to block scam texts by allowing banks to register the sender IDs they use to send messages to customers. It's a collaboration between banks, mobile network operators and the messaging industry.



2019