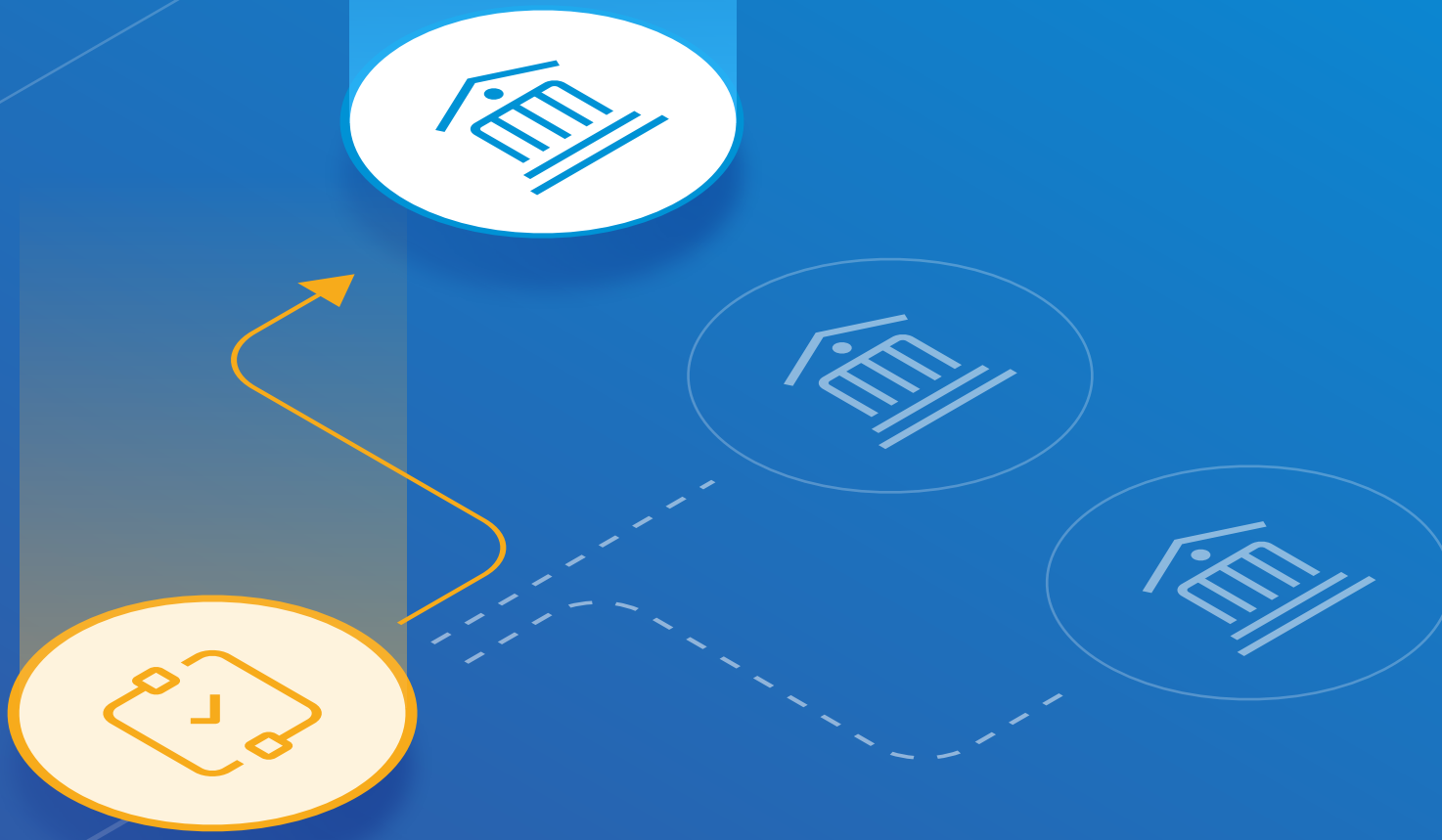
RESEARCH REPORT



The future of ecommerce payments

Why open banking will challenge card dominance

TRUELAYER

Table of contents

Tap this logo to return to this page

Foreword from TrueLayer

One of the key motivations behind open banking has been to enable the growth of alternative payment methods to cards. This report demonstrates that the policy drivers, the industry development and the innovation have all worked together to deliver that alternative in the form of open banking payments.

The simplicity of the open banking payment chain, made possible by API technology, is key to the cost savings, reduced fraud and improved conversion for merchants. It also increases convenience for consumers, who increasingly want to make and receive all payments instantly and seamlessly.

The development of capabilities for instant refunds, such as TrueLayer's own PayDirect, will enable open banking to be used successfully in ecommerce.

At the same time, the growth of ecommerce is beginning to show merchants' reliance on card payments creates problems of its own.

Card schemes and the chargeback approach, which is the target of increasing fraud and which suffers from slow resolution, will only further impact merchants if they are unable to add new payment methods to their checkout as ecommerce payments continue to grow.

Strong customer authentication (SCA), while seamlessly integrated into open banking payments, is also creating issues for merchants who collect card payments, as SCA is retro-fitted onto an existing and ageing infrastructure.

So while ecommerce merchants will continue to feel the pain of collecting card payments, open banking payments are truly ready for launch.

TrueLayer is excited to see many merchants across ecommerce and other industries develop new payment experiences using open banking. We believe open banking payments will become the default way to collect money online in the coming years.

Francesco Simoneschi
CEO & Co-founder

Executive summary

This research report examines the development of open banking payments (payment initiation services) since PSD2 (2015) and looks at the most important reasons why this payment method is becoming a competitive alternative to card payments.

The report finds that:

- Open banking has led to the emergence of new payment providers with the potential to challenge the dominance of card networks.
- The growth of open banking payments has been encouraged by the decline of cash in retail transactions (which fell by 35% between 2019 and 2020[1]); the expansion of ecommerce; and an increased focus from policymakers on the persistently high costs of card acceptance.
- Greater competition between open banking payments and card payments is likely to bring significant benefits to merchants and consumers. These benefits include:
  - lower merchant fees for accepting electronic payments
  - reduced risk of unauthorised payments and fraud, thanks to embedded strong customer authentication (SCA) and pre-populated payment details
  - increased convenience for consumers (and conversion rates for merchants) as a result of shorter payment journeys
- Non-card payment providers in other countries with similarities to open banking payment providers have achieved high take-up rates, strong popularity with consumers, low fees and low fraud rates. These providers include:
  - bank schemes such as iDEAL (Netherlands) and Swish (Sweden)
  - third-party providers such as SOFORT (Germany)
- Open banking provides digital payments for a digital age. It reduces the number of parties to transactions, increasing efficiency and speed, which should translate into customer satisfaction.

1
Source: UK Finance, UK Payment Markets Summary 2021, p. 4.

Methodology

TrueLayer commissioned an independent research consultancy with experience in payments and open banking to create this report.

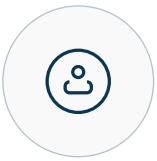
The report draws on existing research into open banking in the UK and the EU, recent documents produced by the regulators and government, and a series of interviews with stakeholders and experts to evaluate specific policy issues and other aspects of open banking payments. Stakeholder input was gathered anonymously to encourage candour.

Input came from across the ecosystem:

Consumers — UK and EU representatives

Banks — International banks and industry bodies

Merchants — Large merchants and advisory firms



Other parties — Scheme operators and independent experts

Chapter 1:
The rapid growth of open banking payments

Key points

Open banking offers a new way to collect payments and has been expanding rapidly since UK and EU regulations created frameworks for its operation from 2015.

This growth has been encouraged by:

- the decline of cash and growth of electronic payments
- ecommerce taking a growing share of retail purchases
- the high costs to merchants of accepting card payments

Open banking has sometimes been hampered by slow progress on rolling out necessary infrastructure and ensuring its reliability, but both of these are now improving.

What is open banking?

Open banking refers to a series of policy interventions and market developments since 2014, which have sought to increase competition in UK and EU payments. The UK led the way with the Competition and Markets Authority's (CMA) 2014–2016 retail banking market investigation. This investigation led to an order requiring the UK's nine largest banks (known as the CMA9) to enable consumers and businesses to access their personal and SME current accounts via third party providers (TPPs)[2]. The CMA also required the CMA9 to create an Open Banking Implementation Entity (OBIE) charged with setting common standards for TPP access via APIs[3] and enforcing the delivery of its market order.[4]

2
Competition and Markets Authority, The Retail Banking Market Investigation Order 2017.

3
API stands for 'application programming interface'. APIs allow third-party providers to access consumer account and payment data with the consumer's consent.

In the case of Open Banking in the UK, the OBIE sets API standards for third-party account access that the CMA9 must implement.

4
Competition and Markets Authority, The Retail Banking Market Investigation Order 2017, pp. 19–20.

The EU took a similar approach in 2015 with the Revised Payment Services Directive (PSD2), which introduced various open-access obligations on EU banks. Like the CMA's retail banking market order, PSD2 sought to boost competition and increase the range of payments functionality available to EU consumers and businesses using their payment accounts. It codified two types of open banking services: account information services (AIS) and payment initiation services (PIS). PIS are referred to as open banking payments throughout this report.

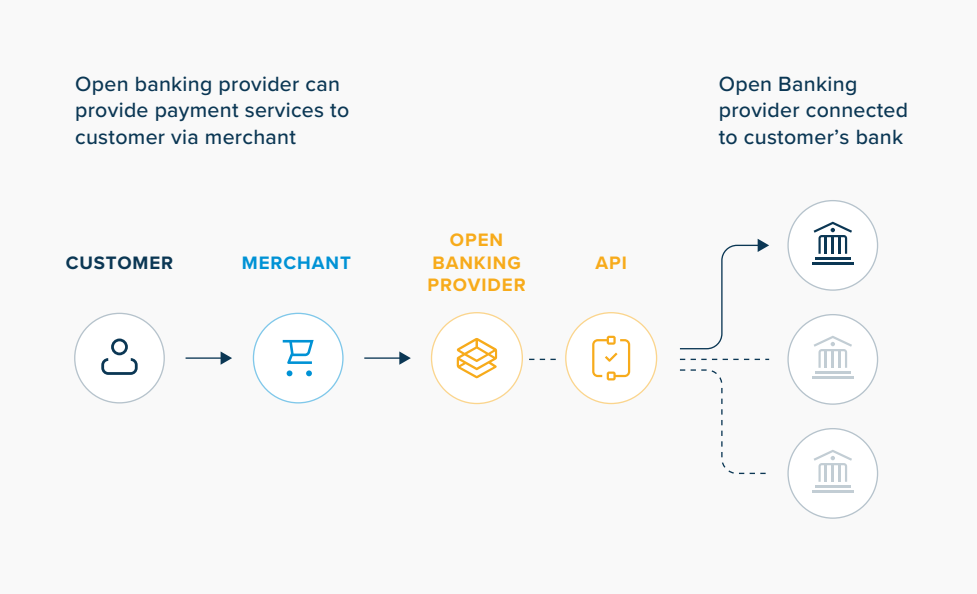
Open banking APIs power new financial service networks

Open banking has been implemented largely through application programming interfaces (APIs). APIs are a technology which connects different IT systems together so that they can exchange data. One system can 'call' or request data from the other system using an API, and receive that data in a standard format.

Under PSD2 and the UK CMA order, banks and other payment account providers have opened up access to payment accounts by building APIs that third party open banking providers can connect to. In order to provide its services, a TPP will connect to all the banks that its own customers use. This will allow it to serve the largest number of customers with open banking services. This creates new networks and platforms that, for example, can be used instead of existing card networks.

Fig. 1

Open banking networks



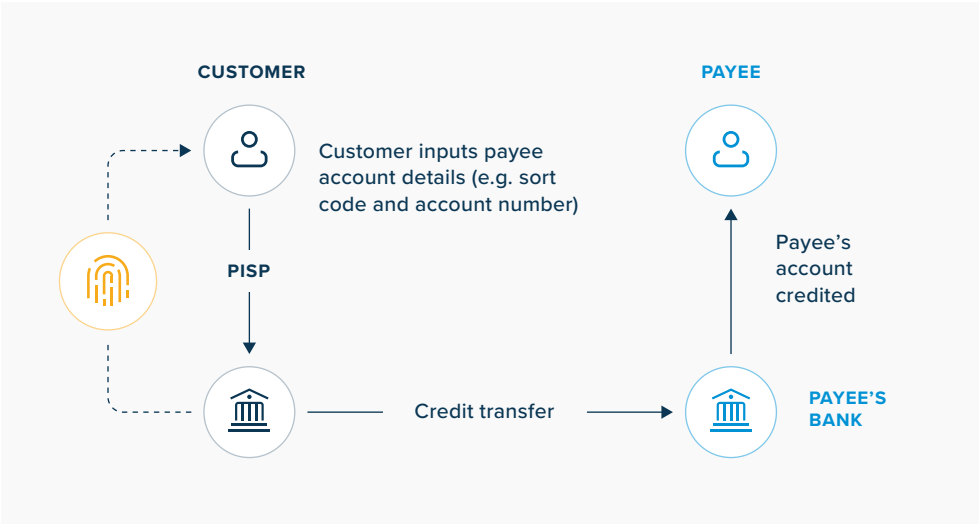
What are open banking payments?

Open banking payments involve a third party provider accessing a consumer's bank account to initiate the transfer of funds on their behalf and with their consent and authentication. There are two main types of use case for open banking payments, worth noting separately because the consumer journey is different in each case:

- **Peer-to-peer payments**: an open banking provider enables a consumer to transfer funds to an account of their choosing, either belonging to themselves ('me-to-me' payments) or to someone else. The consumer can either enter the recipient's account details directly into the open banking payment app or select an existing account from a stored list on the app. This type of open banking payment is generally used for transfers between accounts rather than purchases.

Fig. 2

Open banking payment where consumer inputs recipient details

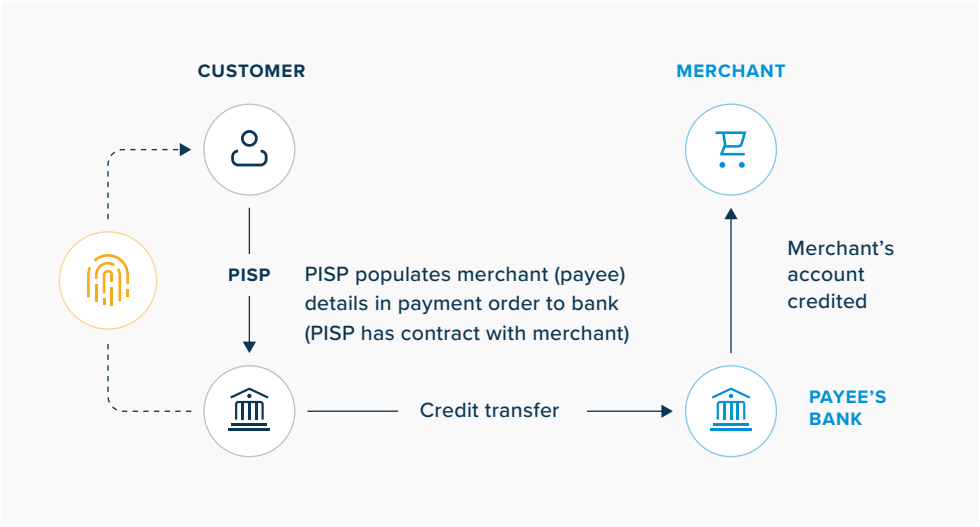


- **Payments to businesses**: some providers of open banking payments enable consumers to pay businesses from their bank account, instead of using a card or another payment method. This form of open banking payment is increasingly widespread in ecommerce and may soon expand into point-of-sale (POS) transactions. The open banking provider has a contractual relationship with the business to enable it to receive open banking payments. When the consumer chooses open banking as the payment method at checkout, the open banking provider initiates the payment from the consumer's account to the business account. The open banking payment provider is responsible for populating the business payee details in the payment order to the bank, rather than the

customer. This prevents misdirected payments from occurring.[5] Misdirected payments have long been an issue, with the UK Financial Ombudsman signalling its concerns back in 2014.[6]

Fig. 3

Open banking payment to merchant: open banking provider populates the merchant's account details



Growth of open banking payments

The number of open banking providers in the UK and EU has grown steadily in recent years, rising from just over 100 in early 2019 to nearly 500 in Q1 2021.[7] As of Q1 2021, just over half of these providers (252) were authorised to provide open banking payments. The UK has the highest number of open banking providers, followed by Germany. As of July 2021, there were 98 open banking payment providers in the UK (see figure 4).

Table 1

Total open banking registrations by country

Source: Vocalink Open Banking Tracker.

	Q1 2021	Q1 2020
UK	205	129
Germany	35	35
Sweden	34	24
Netherlands	23	10
France	23	15
Rest of EU	154	66

Fig. 4

Open Banking payment providers on the UK FCA register as of July 2021

Source: FCA Account Information & Payment Initiation Service Providers

1. Afterbanks Ltd
2. Aj Bell Management Limited
3. Appfleet Ltd
4. Authoripay Emoney Ltd
5. Access Systems (uk) Limited
6. Acquired Limited
7. Allpay Limited
8. Alpha Fx Limited
9. American Express Payment Services Ltd
10. American Express Services Europe Limited
11. Ardohr Limited
12. Automated Payment Transfer Limited
13. Banked Ltd
14. Billx Ltd
15. Bottomline Payment Services Limited
16. Bud Financial Limited
17. By Miles Payment Services Limited
18. Crezco Limited
19. Cashfac Plc
20. Caxton Fx Ltd
21. Cheddar Payments Limited
22. Chip Financial Ltd
23. Citadel Commerce Uk Limited
24. Citizen Uk Holding Limited
25. Coupay Limited
26. Creditladder Ltd
27. Currency Uk Limited
28. Currensea Limited
29. Curve Os Limited
30. Ecospend Technologies Limited
31. Equire Limited
32. Expensedoc Ltd
33. Fire Financial Services Limited
34. Fluidly Limited
35. Fumopay Ltd
36. Faizpay Ltd
37. Finexer Ltd
38. Flagstone Investment Management Limited
39. Fondy Ltd
40. Fractal Labs Ltd
41. Global Private Solutions Ltd
42. Gocardless Ltd
43. Google Payment Limited
44. Hope Macy Ltd
45. Ipagoo Llp
46. Isx Financial Uk Ltd
47. Income Group Limited
48. Indigo Michael Limited
49. Insignis Asset Management Limited
50. Kikapay Limited
51. Kashet Ltd
52. Ksher Wikaas Uk Ltd
53. Mbna Limited
54. Mmob Ltd
55. Monese Ltd
56. Mia Pago Ltd
57. Modulr Fs Limited
58. Moneyhub Financial Technology Ltd
59. Naudapay Limited
60. Obn Global Limited
61. Obconnect Limited
62. Osu Ltd
63. Paysend Plc
64. Paydog Ltd
65. Paylink Solutions Limited
66. Paymentwall Ltd
67. Paymentz Ltd
68. Pelican Payment Services Ltd
69. Plaid Financial Ltd.
70. Pollen Technologies Limited
71. Promptly Paid Ltd
72. Reflow Zone Limited
73. Revolut Ltd
74. Roqqett Ltd
75. Safeconnect Ltd
76. Safened-fourthline Limited
77. Sty.com Ltd
78. Sync.money Uk Ltd
79. Saturn Technologies Ltd
80. Sentenial Limited
81. Skrill Limited
82. Soldo Financial Services Ltd
83. Stripe Payments Uk Limited
84. The Smart Request Company Ltd
85. Thirdfort Limited
86. Tide Platform Limited
87. Token.io Ltd
88. Trilo Group Limited
89. Truelayer Limited
90. Vibe Pay Limited
91. Volt Technologies Limited
92. Vyne Technologies Limited
93. Wealthkernel Limited
94. Wise Payments Limited
95. Worldpay Ap Ltd
96. Yoello Limited
97. Yolt Technology Services Limited
98. Zeux Limited

(From previous page)

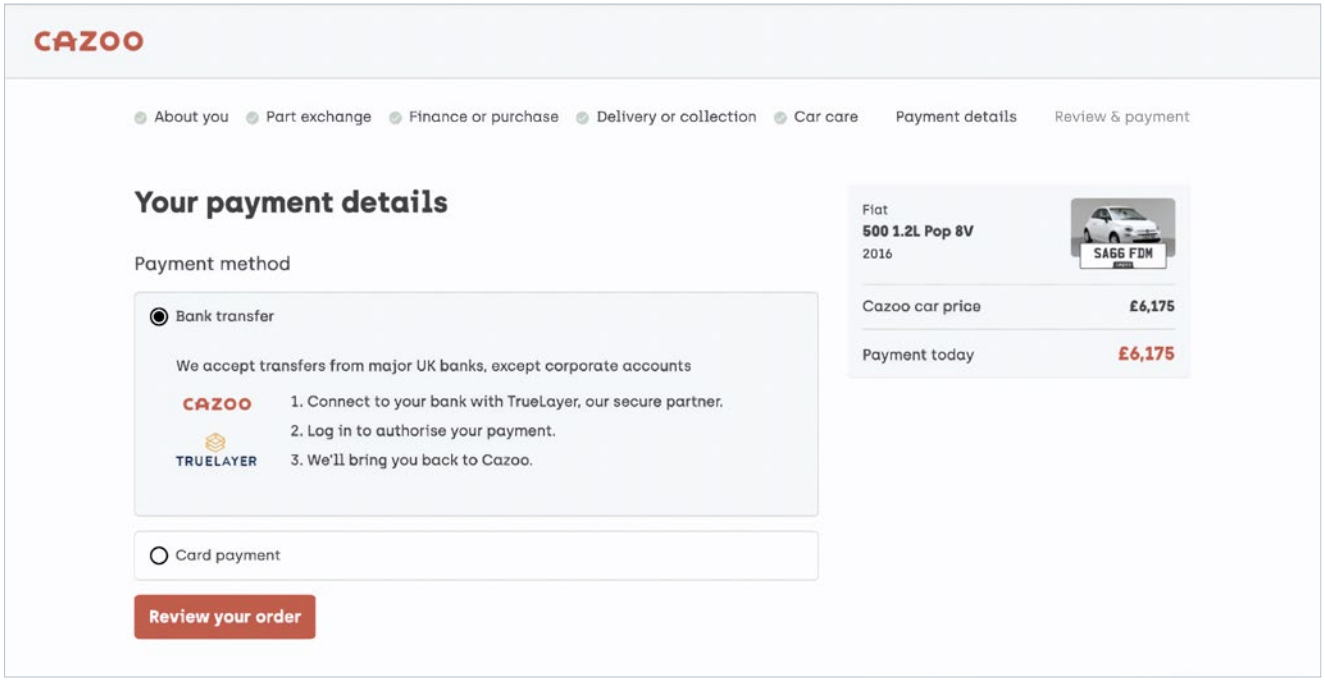
5 A misdirected payment occurs when a customer is sending a bank transfer and mistypes the recipient's bank account details e.g. sort code/ account number, or IBAN in the EU.

6 The Guardian, 'Banks told to respond faster over misdirected payments, 24 April 2014.

7 Vocalink, Q1 2021 Open Banking tracker.

Open banking payments were slower to develop than other open banking services - such as account information services - in the early years after PSD2 came into force, but both the number of providers and the range of use cases is now expanding (see table 2). Use cases to date have involved a mix of peer-to-peer payments and payments to businesses, such as transfers to investment providers. Several providers already allow merchant payments for a range of ecommerce purchases, with more set to do so in 2021 and beyond. For example, the online car retailer Cazoo recently enabled open banking payments, powered by TrueLayer (see figure 5 below).

Fig. 5 | **Online checkout featuring card and open banking payment options**



Source: Cazoo

This acceleration in the growth of open banking payments can be explained by a number of trends reinforced by the COVID-19 pandemic, as well as the removal of friction that had made it unattractive to launch these payment solutions earlier.

Table 2

Noteworthy open banking payment providers and relevant use cases

Name	Use case(s)
Adyen	Open banking payments for flight bookings (offered in partnership with KLM)
GoCardless	Recurring and one-off payments focused on SMEs
IATA Pay	Bank transfer payments for flight bookings (currently available with Emirates in Germany and the UK)
TrueLayer	Open banking payments for investment, gaming, trading and ecommerce
Trustly	Open banking payments, typically for ecommerce, financial services and igaming
Yapily	Peer-to-peer payments and bulk payments
Yolt	YoltPay, peer-to-peer transfers can be set-up by a YoltPay user on the Yolt app

Trends favouring the growth of open banking payments

Three distinct trends in retail payments have created an opportunity for open banking payments:

1. Cash has declined as electronic payments have grown.
2. Ecommerce's share of retail purchases has increased, highlighting the need for smooth customer journeys and boosting alternatives to card payments.
3. Regulators have pressed forward with reforms, concerned that the costs of accepting card payments remain high, even after the introduction of the EU's Interchange Fee Regulation (IFR).[8]

8

The IFR, discussed in more detail in chapter 2, capped interchange fees for consumer credit and debit cards in the EU from 2016. See Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions. (Link)

Table 3

Trends favouring the growth of open banking payments

Trend	Description	Significance for open banking payments
Decline of cash / growth of electronic payments	Cash accounted for more than 50% of retail payment volume in 2010 but less than 20% in 2020.	The decline of cash has made cards more dominant and consumers more comfortable with electronic payments, creating an opportunity for competing alternatives.
Growth of ecommerce in retail sales	Internet sales have grown from less than 5% of all sales in 2006 to around 30% in 2020.	More merchants are participating in, and making a growing share of their sales through ecommerce channels. Here, open banking payment providers offer a lower-cost alternative to cards that is also less vulnerable to fraud.
Policy concerns and interventions to lower the cost of card acceptance	Even after the Interchange Fee Regulation, the cost to merchants of accepting card payments remains high. Since 2018, merchants have also been banned from recouping these costs through surcharging.	Open banking payments would put downward pressure on card fees by increasing competition with cards, which still dominate electronic payments.

Growth of electronic payments

Electronic payments have steadily increased their share of all UK payments by volume and value since 2000. Even before the COVID-19 pandemic, cash use for transactions had been declining at a rapid rate, which accelerated over 2020 with a drop of 35% from 2019.[9] Debit and credit cards currently account for 60% of UK POS retail payments and 50% of ecommerce payments.[10]

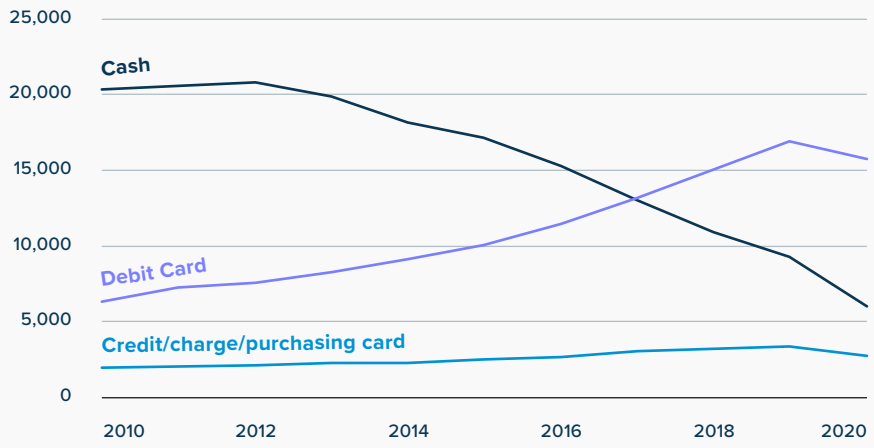
9 UK Finance, UK Payment Markets Summary 2021, p. 2.

10 Worldpay, The Global Payments Report 2020, pp. 128–129.

Fig. 6

Payment volume (millions) in the UK, 2010 to 2020

Source: UK Finance, UK Payment Markets Summary 2021, p.1.

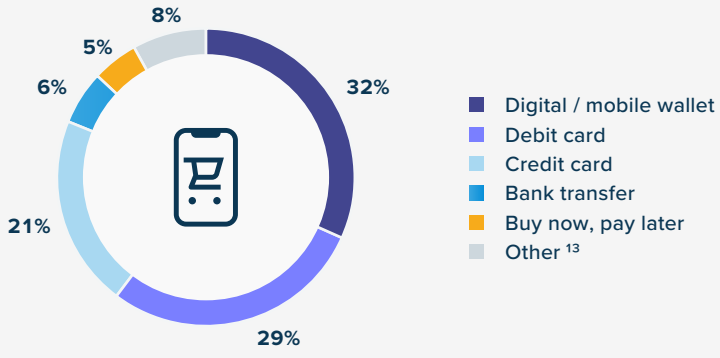


The spread of smartphones has enabled new payments functionality such as mobile wallets (e.g. ApplePay, GooglePay). These can be more convenient and secure than physical cards, as they are already subject to strong customer authentication (SCA, see pp. 19–23) and payments made with them are tokenised.[11] Mobile and digital wallets, often but not always used for card payments, are now the most popular payment method in ecommerce and increasingly popular for POS payments[12].

Fig. 7

UK ecommerce mix by payment method, 2020

Source: FIS Worldpay Global Payments Report 2021, p.129.



11

Tokenisation in payments is the process of replacing sensitive card or account data with a randomly generated transaction identifier. Tokenisation provides additional protection for sensitive data.

12

Worldpay, The Global Payments Report 2020, pp. 128–129.

13

'Other' includes cash on delivery, charge and deferred debit card, prepay, Direct Debit and prepaid card.

With customers more comfortable making electronic payments instead of using cash, adoption of open banking payments becomes easier. The growth of electronic payments has also highlighted card acceptance costs for merchants and made them more receptive to lower-cost alternatives.

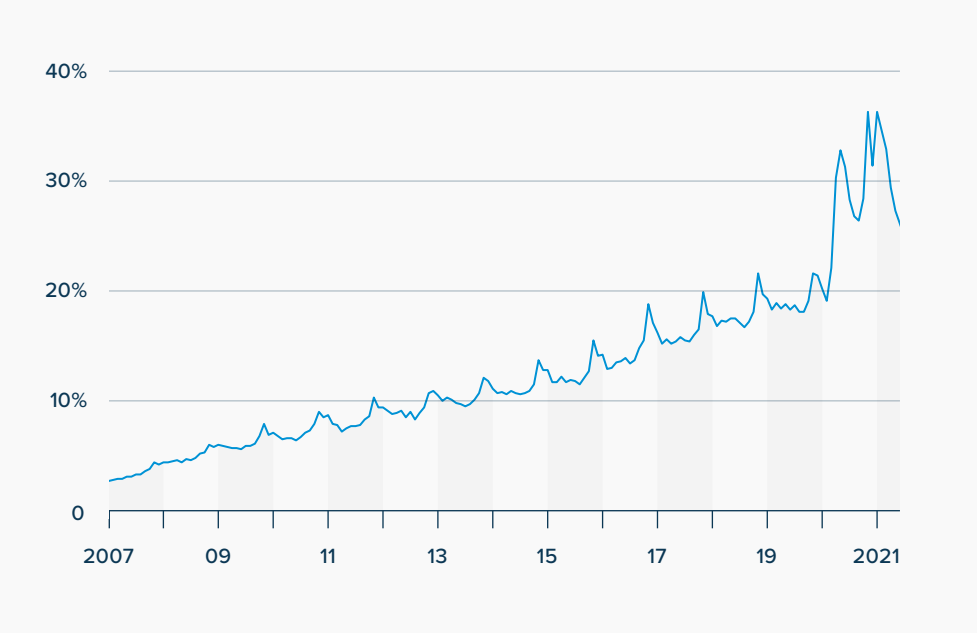
Growth of ecommerce

The share of internet sales in total UK retail sales has steadily increased since 2006, and it accelerated significantly with the onset of the COVID-19 pandemic. The growth of ecommerce has boosted existing electronic payment methods and led to new options such as 'buy now, pay later' (BNPL), although BNPL tends to be costlier to merchants than cards.

Fig. 8

Internet sales as a percentage of all UK retail sales, 2006–2021

Source: Office for National Statistics, 2021.



Ecommerce payments have lower barriers to entry than POS payments because they don't require merchants to upgrade their physical infrastructure (such as card acquiring terminals) in order to accept new payment methods. Instead, alternative options such as open banking payments, BNPL and digital wallet payments can be integrated into the ecommerce customer journey relatively easily. Different payment options are displayed transparently at the online checkout, reducing friction and expanding choice for consumers.

45% OF ALL RETAIL FRAUD IS CARD FRAUD

Payment innovations first applied to ecommerce tend to spill over into POS payments later on. For example, several challengers that started and grew in ecommerce (from acquirer Stripe, to BNPL firm Klarna) have later expanded into payments at physical shops.

From the perspective of merchants, while each additional customer may be served at low cost, ecommerce poses new challenges. Ecommerce purchases are riskier for merchants, as they are associated with higher decline and fraud rates, both of which can considerably dent merchant margins.[14] Card-not-present fraud in ecommerce is now the single-largest category of card fraud in the UK, which itself accounts for 45% of all retail financial fraud.[15] Open banking payments can help to reduce some of these merchant risks, as explored in more detail in the next chapter.

Regulatory drive towards new payment mechanisms

Another push in favour of open banking payments has come from regulators, who are concerned about the persistently high cost of card payments, especially for smaller merchants. They have sought to promote competition by allowing third-party access to payment accounts.

The high cost of accepting card payments

Interchange fees, the largest component of the merchant service charge (MSC) that merchants must pay to accept card payments, were capped in the UK and the EU by the 2015 Interchange Fee Regulation (IFR). While this cap did effectively lower interchange costs for merchants, a subsequent study of the UK card payment market found that savings from the cap were only partially passed through to

14

Callum Godwin, 'The dark side of ecommerce: fraud and lost customers', 4 June 2020. https://cmspi.com/nam/blogs/the-dark-side-of-ecommerce/

15

UK Finance, Fraud: the facts 2021, pp. 16 and 18.

merchants, while other components of the MSC such as scheme fees increased.[16] UK SMEs with turnover under £50 million, for example, have seen their total card acceptance costs stay the same or increase even as the IFR caps caused the interchange fee component to decline.[17]

In the UK, the Payment Systems Regulator (PSR) is reviewing the card acquiring market and has published a set of proposed measures to improve outcomes for merchants.[18] In the EU, there are several independent initiatives aimed at boosting competition, including the European Payments Initiative (EPI), which seeks to create a new scheme to rival Visa and Mastercard in cross-border payments, and the forthcoming review of PSD2, which is due to launch in late 2021.

Increasing third-party access

In addition to intervening directly in card payment markets, regulators in the UK and the EU have sought to promote competition by facilitating alternatives to cards. This has involved measures to ease access to customer bank accounts by third-party providers (TPPs), including open banking payment providers, as well as measures to open up the interbank payments infrastructure to non-banks, including payment firms.

The European Commission is consulting on the creation of pan-European instant payments solutions.[18] These measures are based on the idea that greater TPP participation will increase choice for consumers and strengthen incentives to create user-friendly options in interbank payments.

16

Payment Systems Regulator, Market review into the supply of card-acquiring services: Interim report (September 2020), p. 61; Annex 4: Scheme fees, p. 22.

17

Payment Systems Regulator, Market review into the supply of card-acquiring services: Interim report, p. 61.

18

Payment Systems Regulator, Market review into the supply of card-acquiring services: Interim report, pp. 11–12.

After a slow start, open banking payments are growing fast

In the UK as elsewhere, payment solutions were initially slower to develop than other open banking services (account information services), but they are now growing quickly.

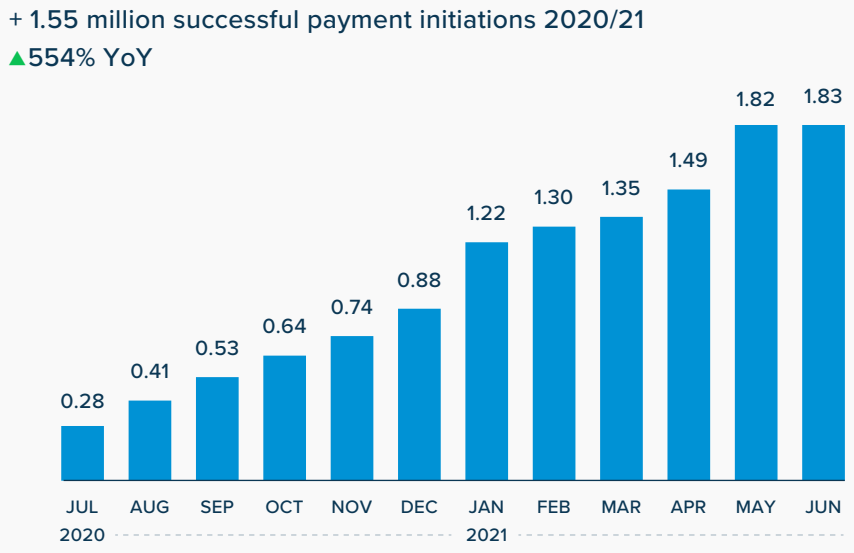
The growth of open banking payments has hugely accelerated in the last year. Successful payments made using open banking providers have increased from 280,000 in July 2020, to 1.83 million in June 2021.

We can expect this number to increase as open banking payments become more widely available. Already, there are over 3 million open banking users in the UK[20], equating to 5% of the population. On its current growth trajectory, 60% of the population will be open banking users by September 2023. The growth of successful open banking payments should follow suit.

Fig. 9

The number of successful payment initiations made by third party providers using account providers' (ASPSPs) Open Banking APIs.

Source: OBIE. Successful payment initiations are based on data submitted by banks to Open Banking since July 2020. Since July 2020, 19 UK banking brands have submitted this data.



19 Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU, 24 September 2020.

20 European Commission, Consultation strategy for the initiative on instant payments in the EU.

60% **OF THE UK POPULATION WILL BE OPEN BANKING USERS BY SEPTEMBER 2023**

The initial slow growth of open banking payments was linked to:

- bank API availability
- bank API performance
- friction in the consumer journey caused by bank authentication steps

API availability at the CMA9 took longer to deliver than the OBIE had planned. Both the OBIE and the CMA repeatedly took banks to task for dragging their feet on API delivery. There was also fragmentation in the type of access banks were required to provide to third party providers. While the CMA9 were required to deliver APIs according to the CMA order and the OBIE's standards, smaller banks – together accounting for around 15–20% of deposit accounts – could choose whether or not to provide APIs, or to offer less efficient access channels (modified customer interfaces). In reality, many non-CMA9 banks did provide APIs, and third party providers have been increasing coverage of these banks consistently.

To address access issues at the banks who chose to provide non-API access methods, the FCA recently proposed to require all but the smallest banks and electronic money providers to offer dedicated APIs. This extension will take at least another 18 months to come into effect.[21]

API performance was also less-than-optimal initially because bank APIs were slow to respond and often unavailable. Slow API speeds discouraged open banking take-up and made open banking providers reluctant to develop use cases, particularly payments-related ones, until bank APIs were more reliable. API performance has since improved, with average response speeds dropping from 2,500 milliseconds in mid-2018 to 550 milliseconds by March 2021. API availability has also improved, increasing from an average of 96–97% in 2018 and 2019 to 98–99% in 2020 and 2021.[22]

21

Financial Conduct Authority, Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money – Our Approach' and the Perimeter Guidance Manual, consultation paper (January 2021), pp. 11–12.

22

Open Banking Implementation Entity, Open Banking APIs performance, March 2021.

Chapter 2:

How merchants and consumers will benefit from open banking payments

Key points

Without alternatives to card payments, many merchants currently face:

- persistently high fees for accepting electronic payments
- high rates of card-not-present fraud and purchase abandonment in ecommerce

Consumer payment journeys are often longer and less convenient for cards when buying goods and services online than at the point-of-sale.

Greater competition from open banking payments could bring about:

- lower fees for merchants
- greater payments security, benefiting merchants and consumers
- increased convenience for consumers

Fig. 10 | Key consumer and other benefits of open banking payments

Lower fees for merchants

For card payments, merchant service charges (MSCs) average 1.9% for UK merchants with turnover less than £380,000, and ~1% for those with turnover between £380,000 and £1 million. These turnover groups together represent 97.8% of all UK merchants. The MSC is the most significant – but not the only fee – that merchants pay for accepting card payments. Other card fees include authorisation fees, card terminal hire fees, PCI compliance fees and chargeback fees. Chargeback fees, discussed in greater detail in chapter 4, have become of particular concern to merchants in ecommerce.

Table 4

Representative cost of card acceptance in the UK, by fee category

Source: CardSwitcher.co.uk, 'What are payment processing fees?', 18 January 2020; Rob Binns, 'PCI compliance guide 2021: everything you need to know', ExpertMarket.com, 8 April 2021.

Fee name	Description	Cost
Merchant service charge (MSC)	Standard fee on every card transaction. Consists of an interchange fee, a scheme fee and an acquirer fee.	1–1.9%
Authorisation fee	Additional fee on every card authorisation	1–3p per transaction
Card terminal hire	Monthly rental fee for a card terminal to accept point-of-sale payments	£14–24 per month
PCI compliance fee	Fee to ensure compliance with personal data protection standards and regulation	£2.50–5.50 per month
Chargeback fee	Contingent fee payable every time a consumer requests that a payment be reversed	£15–25

In its interim report on the UK card acquiring market, the PSR found that MSCs had not noticeably changed since 2014, before the Interchange Fee Regulation (IFR) came into force.[23] The European Commission's report on the IFR, published in July 2020, found that MSCs had declined following the IFR's introduction, but unlike the PSR it did not break down these findings by merchant turnover.[24] The Commission report also found that the decline in interchange fees had been partly offset by an

23 Payment Systems Regulator, Market review into the supply of card-acquiring services: Interim report, p. 48.

24 European Commission, Report on the application of Regulation (EU) 2015/751 on interchange fees for card-based payment transactions (July 2020), p. 5.

increase in scheme fees for regulated cards and interchange fees for commercial cards, which are not subject to the same caps.

In addition, from 2018, UK and EU merchants are no longer allowed to add a surcharge at checkout to reflect the increased cost of processing different forms of payment, so they must either limit customer payment options, raise prices for everyone or absorb the incremental cost if costlier payment methods are used. The surcharging ban has increased margin pressure on merchants and encouraged them to seek out less expensive payment methods.

Open banking payments are one such option, as they can offer lower and more predictable merchant processing fees than card acquirers do. For example, TrueLayer's average fee is less than 1% of transaction value, while Trustly's standard fee is 1.5%[25]. Open banking payments also do not involve additional fees such as authorisation fees, card terminal fees, chargeback fees or fees for PCI compliance. They can therefore bring direct cost savings to a large number of merchants and place competitive pressure on costlier electronic payment methods. This is especially true for the ecommerce sector, where the use of cash as an alternative to cards is highly impractical or impossible.

Table 5

Taxonomy of retail payment methods (representative merchant with turnover <£1 million)

	Cards	Buy now, pay later	Cash	Open banking payments
Merchant service charge	~1–1.9%	~4–6%	N/A	~1–1.5%
Contingent charges[26]	£15+	£6–36	N/A	N/A
Other costs	N/A	N/A	~0.2%[27]	N/A

Source: PSR card-acquiring market review interim report (for card MSCs), FCA Woolard Review (for BNPL fees), European Commission study on interchange 'merchant indifference test' (for cost of processing cash).

25 Trustly (link)

26 'Contingent charges' refers to chargeback fees in the case of cards and fees for late payment in the case of BNPL products.

27 This figure is based on the 'merchant indifference test', which seeks to find the level of MSC at which merchants are indifferent between accepting cards or cash. The figure is therefore a measure of the cost of accepting and processing cash.

Greater payments security

Consumers using open banking payments must authorise every payment with their bank using strong customer authentication (SCA). SCA means that a consumer must provide at least **two** separate types of identification from three categories, in order to prove who they are:

KNOWLEDGE

Something they know, like a password or PIN

POSSESSION

Something they own, like a phone or payment card

INHERENCE

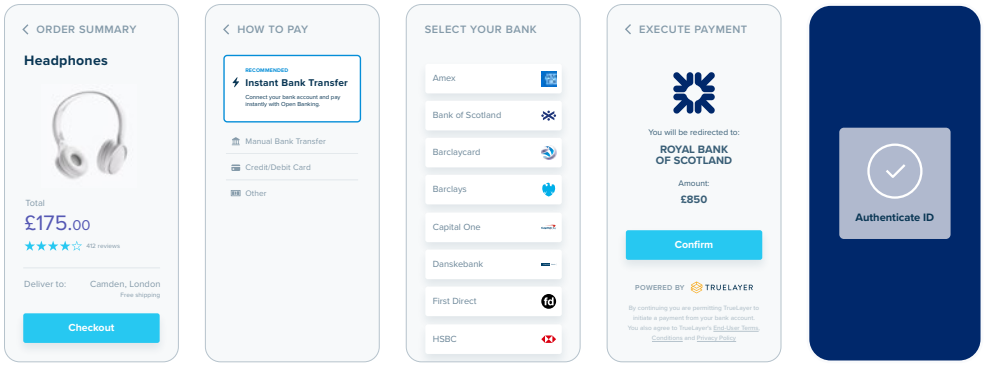
Something they are, referring to biometrics like fingerprint or facial recognition

In the UK and most of the EU, SCA has been implemented for open banking in the form of 'redirection', where consumers are sent from the open banking app to their bank in order to provide the required credentials.[28] Redirection uses secure APIs and ensures that banking credentials do not leave the banking domain.

Fig. 11

Open banking ecommerce payment with redirection

Source: Truelayer



28

In Germany, the embedded approach has been supported by banks, which requires customers to give their banking credentials to an authorised open banking provider, which then transmits these credentials securely to the bank.

Open banking payment providers have had SCA in place since 2018, whereas some banks have been slower to implement SCA for card payments. The Financial Conduct Authority recently delayed SCA compliance for card-based ecommerce payments until March 2022, citing 'disruption to customers and merchants'[29].

> **"Safety and security is the top of the tree, something consumers expect and assume. If you fail there, consumer trust breaks down."**
>
> – Merchant representative

Open banking payments also reduce the need for risky information-sharing among parties to a transaction compared with cards. Card payments typically require unique customer credentials, such as the long card number and CVV, to be shared with retailers or their payment service providers. If stolen, these can be used to make unauthorised transactions. This is not the case with open banking payments, where consumers provide their credentials directly in the bank's domain.

2.8m CASES OF UNAUTHORISED CARD FRAUD IN 2020 VALUED AT **£574M**

Because they enable SCA and remove the need for consumers to share sensitive information, open banking payments can be more secure than cards. This is relevant because card fraud accounts for 45% of all financial fraud in the UK, with 2.8 million cases of unauthorised card fraud in 2020, valued at £574m.[30] As the share of open banking payments in all retail purchases increases, instances of fraud would be expected to also increase, but the security features of open banking payments could help to reduce the incidence of fraud per transaction.

29

Financial Conduct Authority, 'Deadline extension for Strong Customer Authentication', 20 May 2021.

30

UK Finance, 'Fraud – the facts 2021', p. 20

Finally, open banking payments used in ecommerce offer security benefits relative to manual bank transfers. Manual bank transfers involve entering the merchant's sort code and account number. This increases the risk of misdirected payments, where the consumer makes a mistake entering payment details, and authorised push payment (APP) scams, where customers are tricked into sending money to a fraudster masking as a legitimate payee. According to the OBIE, 64% of APP fraud cases and 13% of financial losses are in an ecommerce context.[31]

As noted in Chapter 1, figure 2, With open banking payments in ecommerce, open banking providers handle the payment instruction to the consumer's bank, including pre-populating the merchant or businesses sort code and account number (IBAN for EU payments), eliminating the risk of payment errors and significantly reducing the risk of APP scams.

Increased convenience for consumers

Some of the features mentioned above help to make open banking ecommerce payments more convenient for consumers, by enabling a faster checkout process that requires less effort from them. For example, by pre-populating the merchant's payment details, open banking providers reduce the steps of a transaction down to simply redirecting a consumer to their bank to authenticate the transaction (e.g. with a thumbprint). This speeds up transactions and helps to reduce purchase abandonment.

> **"I hope that, in the near future, we will be able to pay in shops with a convenient alternative. Right now, the options are limited to cash and cards."**
>
> – Consumer representative

31

Open Banking Implementation Entity, 'Open banking standards relating to Confirmation of Payee and Contingent Reimbursement Model Code', July 2021, p. 8.

SCA: cards vs. open banking payments

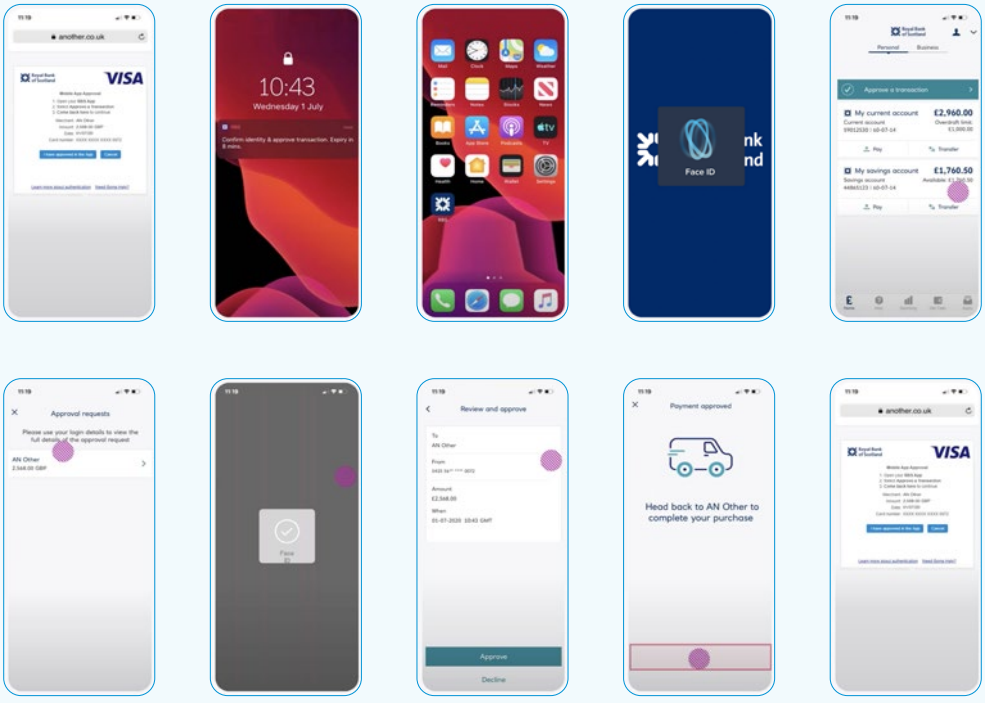
While SCA can significantly reduce fraud risk, especially for online transactions, it can also introduce significant additional friction for consumers, leading them to abandon purchases they would otherwise have made. A 2021 study found that as many as 14% of browser-based card transactions, and a quarter of app-based ones, were discouraged by SCA.[32] Another recent study looking at EU markets found that a mix of friction and lack of preparedness from banks could lead to up to €108 billion in lost online sales over 2021.[33]

One merchant advocate interviewed for this report cited the introduction of SCA for card payments as a key driver of purchase abandonment, given that it typically involves the elements of possession (a card or device) and knowledge (a PIN or 3D-secure password). Verification takes longer in this case than under other forms of SCA, and some consumers may not be able to authenticate, for example because they do not remember their password.

Fig. 12 | **Illustration of SCA card payment journey**

Cards with SCA

Source: NatWest, 2020.

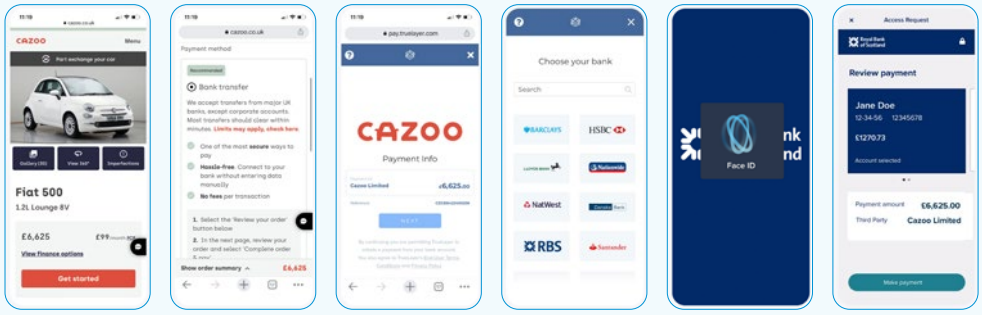


Concerns about purchase abandonment have partly motivated regulatory delays to the full rollout of SCA for cards in the UK. In the EU, EuroCommerce and Ecommerce Europe recently wrote to the European Banking Authority to highlight problems with SCA for card payments and the direct cost impact of SCA implementation for merchants in the form of higher scheme fees.[34]

Open banking payments appear to have adapted more successfully to incorporating SCA in the consumer journey. Studies of the impact of SCA on purchase abandonment find it to be smaller in EU countries where bank transfer apps are popular, because consumers tend to already be familiar with SCA.[35] In the UK, the open banking payments journey was significantly improved by the OBIE's September 2018 customer experience guidelines, which set out the steps for open banking payments in order to reduce friction for consumers.[36] As a result, existing open banking SCA journeys are significantly shorter than the SCA journeys for some card payments. Figure 13 illustrates the SCA steps in an open banking journey compared with a card-based payment for a customer who banks with NatWest.

Fig. 13 | **Illustration of SCA in open banking**

Open banking with SCA



32

Fi911, 'Strong Customer Authentication: the state of SCA adoption in 2021', p. 9.

33

CMSPI, 'SCA Economic Impact Assessment' (September 2020).

34

EuroCommerce and Ecommerce Europe, 'Re: Measuring the impact of Strong Customer Authentication in Europe', letter to the European Banking Authority, 30 April 2021.

35

CMSPI, 'SCA Economic Impact Assessment', p. 14.

36

OBIE, Open Banking Customer Experience Guidelines, Version 1.0 (September 2018).

In addition to strong customer authentication, several other forms of protection apply to open banking payments:

- PSD2 ensures that consumers are **refunded by their payment provider** if the provider makes a mistake with the payment. This applies to all types of electronic payment, including open banking payments.

- PSD2 also ensure that **consumers are refunded for unauthorised transactions**, with limited loss-sharing by the consumer in some cases. When a payment is made through an open banking provider, it is the consumer's bank who is responsible for processing the refund in the first instance.[37]

- **Confirmation of Payee** protects consumers from misdirecting payments in cases where the consumer is inputting the recipient's details. It also helps to prevent manipulation fraud, where scammers trick customers into sending funds to the wrong account.

- In addition, providers of open banking merchant payments mitigate the risk of this harm by **pre-populating the merchant's payment details**, avoiding the risk of consumer error or fraudulent acts.

- The **Contingent Reimbursement Model Code** helps to protect consumers against fraudulent acts, by ensuring banks place risk warnings within the payment journey to discourage consumers from sending funds to scammers. With open banking payments, these risk warnings are presented to consumers when they are redirected to their bank to provide authentication. The OBIE recently published standards governing these warnings and the merchant's account verification for open banking payments.[38]

- **Statutory protections, retailer protections, dispute resolution schemes and non-profit advice** services allow consumers to seek redress when there is a fault with the goods or services purchased.

Some open banking payment providers enable speedy reimbursement of consumers by providing merchants with instant refund functionality.

37

Financial Conduct Authority, 'Account information and payment initiation services', 19 March 2021.

38

Open Banking Standards Relating to Confirmation of Payee and Contingent Reimbursement Model Code

Chapter 3:

What we can learn from non-card payment methods in Europe

Key points

Non-card payments have gained wide adoption in EU jurisdictions. Some arrangements are schemes owned and operated by domestic banks, as in the case of iDEAL in the Netherlands and Swish in Sweden. Others are run by third-party providers and operated before PSD2 came into force, such as SOFORT (now owned by Klarna) in Germany. Non-card payment providers have achieved:

- high rates of consumer adoption in ecommerce transactions
- low merchant fees, below those charged for card payments
- low rates of fraud

These providers are generally well-liked by merchants and consumers. Their experience shows that non-card methods of payment can become the norm if market conditions are right.

However, unlike these payment methods, open banking has the potential to be truly pan-European, giving it the scope and scale to challenge the dominance of cards.

Non-card payments elsewhere in Europe

While open banking payment providers are relatively new ecosystem participants, other forms of non-card electronic payments were already popular in some EU countries before PSD2 came into force. Some of these are schemes owned and operated by domestic banks, while others are run by third-party providers that launched before API-enabled access to accounts became the norm.

Table 6

Selected EU mobile payment systems

Name	Country	Structure/type	Ecommerce market share	Merchant fee/tx
iDEAL	Netherlands	Bank scheme	~60-70%	~€0.25
SOFORT [39]	Germany	Third party provider	~20–30%	0.9%+ €0.25
Swish	Sweden	Bank scheme	32% (2019)	SEK2 (~€0.2)

Bank scheme model

Before PSD2 created a formal procedure for consumers to grant third parties access to their accounts, alternative payment methods to cards in the EU were often run jointly by banks. This is the case with iDEAL in the Netherlands and Swish in Sweden, which are each owned by the largest banks in those countries.

The bank scheme model has the advantage of relying on trusted participants to facilitate online transactions at a lower cost than using card rails. Each bank has a direct relationship with either the merchant or the consumer. An independent expert interviewed for this report cited trust between banks and the ability to 'sort things out between themselves' as a factor behind consumer satisfaction with these payment systems. Ongoing cooperation between banks and the existence of a long-term relationship with consumers appear to have enabled their growth while keeping both fees and fraud rates low.

However, relying only on the bank scheme model presents a number of drawbacks. First, bank scheme options may pose competition concerns if they entrench the dominance of banks in the payments ecosystem. The motivation for open banking was to increase competition and innovation by giving third parties the ability to access account data and payments functionality with consent. This was based on the belief that banks were not sufficiently innovative and consumers were unlikely or unable to switch.

While bank schemes can make consumers better off by expanding the payments functionality available to them, they may not help to erode banks' market power.

39

SOFORT is active in 12 EU markets in addition to Germany, its main market. Merchant fees are illustrative and may vary.

CASE STUDY

Swish is a Swedish mobile payments service launched in December 2012. While initially focused on peer-to-peer transfers, Swish use cases have steadily expanded, first to ad hoc payments to small businesses and charities (2014), and later to ecommerce (2017) and POS payments (2018).[40]

As cash use for retail transactions declined in Sweden (faster than in any other EU country), take-up of Swish has grown rapidly. Around 80% of the Swedish adult population used Swish in 2019, the same percentage who owned a smart-phone.

As of 2020, 22% of ecommerce purchases in Sweden were made by bank transfer, higher than the share of debit (19%) and credit cards (11%) and surpassed only by BNPL (23%).[41] Around 70% of Swish transactions are for amounts below 300 krona (~£25/€30).[42]

Past experience of cooperation between Swedish banks helped the growth of Swish, as it ensured sufficient investment in common infrastructure to take advantage of network externalities and promoted consumer trust in the new payment system.[43] Two factors incentivised Swedish banks to promote Swish: the opportunity to offer it as an added benefit from holding a bank account, and the potential to eventually phase out the costly infrastructure around cash.

Swish has gained impressive market share in Sweden, with a user base of 7.9 million, ~60 million monthly transactions and ~13,500 merchants accepting Swish payments as of April 2021 (up from ~8,000 in April 2020).[44] Retail payments represent ~20% of Swish transactions by volume and ~16% by value. The value of merchant payments made on Swish was over 55 billion krona (~£4.7 billion/€5.5 billion) in 2020, double the 2019 figure.[45]

40

Craig Beaumont, Tommaso Mancini-Griffoli, Maria Soledad Martinez Peria, Florian Misch, and Björn Segendorf, 'The diffusion of payment innovations: insights from the stellar rise of Swish' (November 2019), p. 4.

41

Worldpay, Global Payments Report 2021, pp. 118–119.

42

Beaumont et al. 'The diffusion of payment innovations', p. 5.

43

Björn Segendorfand anna-Lena Wretman, 'The Swedish payment market in transformation', Sveriges Riksbank Economic Review 2015:3, pp. 52 and 59–60.

44

Swish statistics, April 2021, p. 16.

45

Swish statistics, 2012–2020, p. 15.

Such competition concerns were recently raised in connection with plans by Irish banks to launch a mobile payments scheme.[46]

Second, bank schemes require a degree of trust and coordination between banks that may not be present in all jurisdictions. Even if banks join together to develop alternatives to card payments, consumer adoption will be low if the functionality is limited. This appears to have been the case with Paym, a mobile payment system developed by UK banks. Since its launch in April 2014, Paym has attracted just 5.8 million users (~11% of the adult population) and processed £1.9 billion worth of payments, less than 0.1% of all consumer payments over that period.[47]

Third-party model

Germany-based SOFORT (now owned by Swedish BNPL provider Klarna) was a successful early non-bank payment provider focused on ecommerce payments. It used 'screen scraping' – the practice of collecting and exporting screen display data from one application to another – to assess whether a consumer had sufficient funds in their bank account to pay a merchant and decide accordingly whether to authorise the transaction.

Because of its use of screen scraping, SOFORT drew criticism from competitors that it compromised user data and competed unfairly with bank-owned schemes such as Giropay. In response, some German banks introduced restrictions in their terms and conditions regarding third-party use of online banking credentials. However, the German competition authority ruled such restrictions illegal in 2016, stating that they had:

> 'significantly impeded... the use of non-bank and innovative payment solutions for the purchase of goods or services [on] the Internet. The providers of these payment solutions have developed an offer of services which provides a lower-priced alternative to the payment solutions already established in the market and have responded to the needs of online customers and sellers for a cheap and fast payment option.' [48]

46

See M/21/004 – AIB/BoI/PTSB – Synch Payments JV (8 April 2021) for the banks' submission notifying the Irish Competition and Consumer Protection Commission. See Electronic Money Association, 'Re: Synch Payments JV between Allied Irish Banks, Bank of Ireland, Permanent TSB and KBC Bank Ireland' (28 April 2021), for other market participants' concerns

47

Paym, 'FAQs'.

48

Bundeskartellamt, 'Restriction of online payment services by German banking industry in violation of competition law', 5 July 2016.

The German ruling helped to lay the groundwork for PSD2 implementation, which created new opportunities for third-party participation in payments via bank transfer. By mandating explicit customer consent to conduct different types of operations and requiring third party providers to connect with banks via dedicated APIs (with screen scraping as a residual option), PSD2 has helped to address the privacy and data protection challenges that banks had raised against SOFORT.

Non-card options are well liked by consumers and have low fraud rates

Several of those interviewed for this report stated that the three non-card payment systems discussed above are well-liked by consumers and merchants. Low fees are especially appealing to merchants, while consumers value the familiarity and convenience of the consumer journey. In the case of iDEAL and SOFORT, consumers also have a strong perception of security from the fact that – as with open banking payments – transactions on these systems are authenticated via their bank accounts using SCA.

iDEAL, SOFORT and Swish appear to have lower fraud rates than cards. When asked what might explain this performance, stakeholders pointed to the use of SCA and the consumer's bank login details in the case of iDEAL and SOFORT. For Swish, the high prevalence of peer-to-peer payments to known individuals and organisations may contribute to a relatively low fraud rate.

Chapter 4:
Digital payments for a digital age

Key points

- Open banking provides digital payments for a digital age. In ecommerce, open banking can reduce the number of parties to transactions, increasing efficiency, speed and consumer satisfaction.
- In contrast, card scheme arrangements and chargeback processes suffer from high costs, high rates of friendly fraud and slow and uncertain consumer processes.

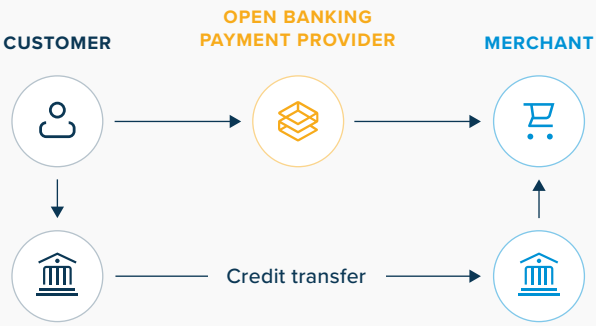
Open banking simplifies the payments chain

The cost savings to merchants of using open banking payments (outlined in chapter 2) can be attributed to the simplicity of the open banking payments chain which is made possible because open banking payment providers send instructions directly to the payer's bank via APIs. There is no need for funds to travel through any other parties. In this sense, open banking 'digitises' payments, and brings internet style connectivity to financial services. In an open banking payment, aside from the banks, there are just three actors involved:

- the customer
- the open banking payment provider
- the merchant

Fig. 14

Open banking actors

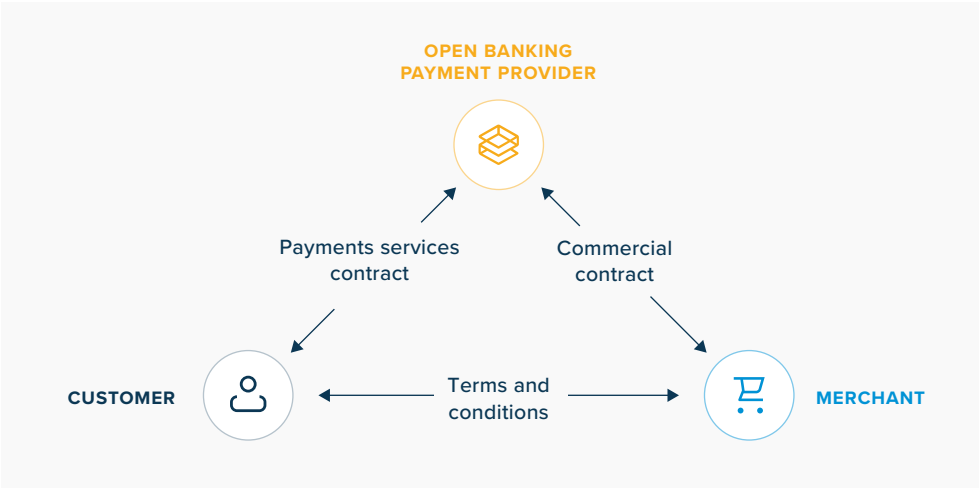


There are also direct relationships between all three actors:

- The open banking payment provider and the customer have a payment services contract governed by the Payment Services Regulations/PSD2.
- The merchant and the customer have an arrangement governed by the merchant's terms and conditions (and certain laws, such as the Consumer Rights Act).
- The open banking payment provider and the merchant have a commercial agreement, to enable the merchant to accept payments from customers using the open banking payment service.

Fig. 15

Direct relationships between open banking actors



This simple model is well suited to payments in the digital age. Open banking providers can integrate seamlessly with merchant checkouts, without the need for payment gateways, acquirers or schemes.

The consumer benefits because if something goes wrong, only three parties, all with direct relationships, are involved in the resolution. This means there is no need to rely on arbitration methods such as chargebacks (see p37).

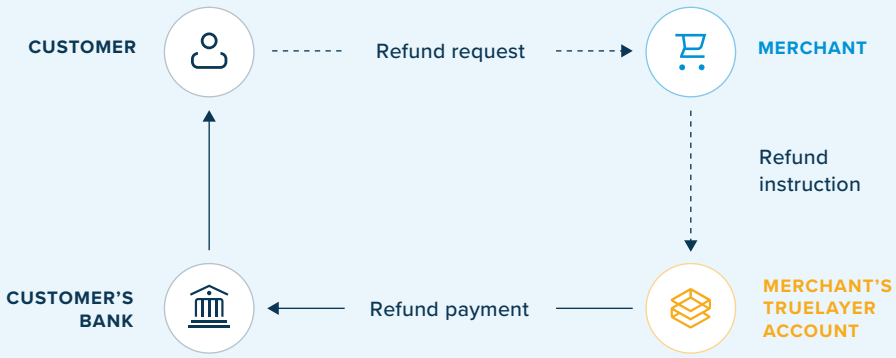
The payment method also has built in security because of the need for the customer to strongly authenticate each payment with their bank and because payee details are populated by the open banking payment provider. This eliminates the risk of unauthorised payments and the need for expensive PCI compliance.

Provider solutions to facilitate refunds:

PayDirect

TrueLayer recently launched PayDirect, which enables merchants to initiate an instant payment to the consumer the moment they receive a refund request. This can remove friction and delays from the refund process, reducing its cost to merchants and inconvenience for consumers.

Fig. 16 | **How PayDirect facilitates refunds**



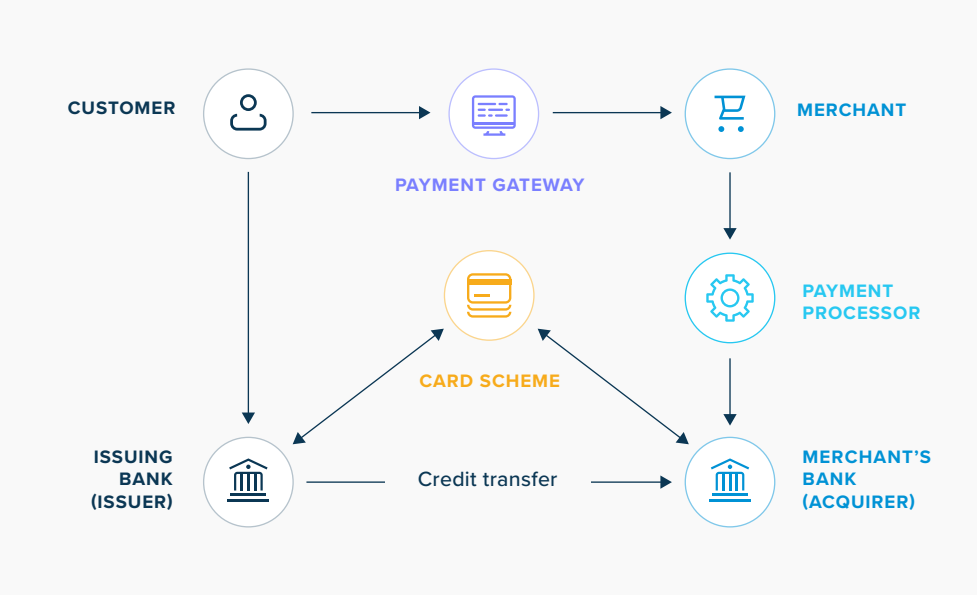
> "High-value transactions require greater certainty around the timing of the refund. Getting your money back instantly, as opposed to seven days later, makes a big difference."
>
> – Banking expert

Complex multi-party card schemes

In contrast, when a customer makes a card payment, up to five businesses are involved, not including the banks. The customer, payment gateway, merchant, payment processor, and card scheme. There are also accompanying businesses that support in terms of security, fraud and dispute management.

Fig. 17

Complex multi-party card scheme



Chargebacks

Chargeback rules within card schemes were introduced as a means of fixing onboarding incentives and dispute resolution between participants in complex multi-party schemes. Chargebacks were designed to promote card take-up when cards were a new payment method, by reassuring consumers, incentivising acquirers to onboard reputable merchants and encouraging merchants to provide refunds where appropriate.[49] In practice, though, chargebacks suffer from several drawbacks.

49

Chargebacks911, '[What is a chargeback?]',

High costs

Scheme liability rules are costly to administer and run, as they entail resource, and time-intensive investigation into claims and generate uncertainty until these are resolved. In the case of chargebacks, schemes charge steep fees for processing, ranging from £15 to upwards of £150 per chargeback, depending on the scheme and the type of dispute. Because card issuers hold back the disputed transaction amount while a dispute is being resolved and this process can take up to 120 days, even chargebacks resolved in the merchant's favour can increase its cost of doing business.

There are other adverse consequences for merchants if they become frequent targets of chargebacks. Issuers and schemes run monitoring programmes for chargeback-heavy merchants, and those which show persistently high chargeback ratios may have their card-acquiring contracts ended. While these measures can be effective at penalising merchants who unreasonably reject legitimate consumer claims, they can also hurt other merchants facing illegitimate or fraudulent claims. In order to reduce uncertainty for merchants, acquirers have developed additional services. Some acquirers bundle chargeback fees into their regular acquiring fees (Square), or they offer merchants 'chargeback protection', a form of insurance, at a cost of ~0.4% of transaction value (Stripe). These services raise merchants' fixed cost of card acceptance, even for the 'good' merchants whose consumers do not raise disputes. Moreover, this insurance is not comprehensive, as it usually covers only certain types of disputes (mostly card-not-present fraud) up to a limit (€20,000 or £20,000 in Stripe's case; $250 for Square).[50]

> **"It doesn't feel like the existing system really discourages fraud. Merchants are constantly looking for alternatives [to cards]."**
>
> – Merchant advocate

50

See e.g. Stripe Chargeback Protection overview.

Friendly fraud: a growing problem of consumer abuse

Chargeback schemes can create incentives for so-called 'friendly fraud', the abuse of purchase protection by unscrupulous or careless consumers. Friendly fraud usually involves attempts to reverse legitimate transactions while keeping the goods purchased, either deliberately or by mistake. With centralised liability rules, the scheme owners enforcing the rules may not have adequate incentives to establish who is at fault and may instead take claims at face value, leaving merchants to bear the cost of dubious chargebacks.

One source quoting US figures estimated the share of chargebacks that could be friendly fraud at 86%.[51] This form of fraud is difficult to detect and prevent, and other sources quote lower figures. An expert stakeholder interviewed for this report added that friendly fraud is especially prominent in the US market because of the prevalence of chip-and-signature cards, which are more vulnerable to counterfeit fraud than chip-and-PIN cards. Even with no fraudulent intent, consumer surveys find that a majority of them will file a chargeback out of convenience instead of relying on the merchant's returns policy in the first instance, as they should and as the PSR expects.[52]

Given the risk of fraud and high cost of chargebacks to merchants, both acquirers (such as Worldpay's Dispute Defender and Square's Protect service) and independent providers (such as Chargebacks911) have launched dispute management services, promising to help merchants to fight spurious chargeback claims.

A slow and uncertain process for consumers

Merchants' struggle with chargeback fraud does not necessarily mean that the chargeback dispute resolution process is always easy to navigate for consumers who raise legitimate issues. There are anecdotal reports of unsuccessful chargeback claims and ones in which the consumer had to wait for weeks to receive reimbursement.[53] Furthermore, while chargebacks may also cover purchases made at retailers that have gone out of business, there is a 120-day time limit on claims, so consumers filing disputes related to insolvent merchants could find they have no protection if insolvency happens long after a purchase was made.

51

Chargebacks911, '13 scary chargeback facts', 20 October 2020.

52

Payment Systems Regulator, Consumer protection in interbank payments – call for views (February 2021), p. 34.0.

53

Financial Ombudsman Service. 'Riley couldn't get her bank to do a chargeback when her holiday was cancelled', case study.

Seamless payments for every checkout, powered by open banking

Let your customers pay in a few clicks and offer instant refunds.
No cards, no chargebacks, and reduced fraud.

Businesses building with TrueLayer:

CAZOO Revolut nutmeg TR^DING 212

Ready to get started?

Talk to one of our ecommerce experts at truelayer.com/ecommerce

TRUELAYER