Open Banking World Series

Edition 2: UK Consumer Report

Consumers looking for better payment choice

October 2020

NUAPAY

Nuapay, powered by Sentenial

Contents

Introduction

UK Open Banking launched to much fanfare in January 2018. But initial adoption and use by consumers remained low. Early services had challenges: poor user experience, inconsistent and unreliable service from the banks, and lack of consumer understanding all meant challenges for both consumers and third party service providers in delivering the much spoken about value of Open Banking.

Specifically in payments, the ramp up has been even slower. Despite strong demand and interest from merchants, the reliability needed to support payments was not available, and many merchants were concerned about the low potential customer adoption. In January 2020, two years after UK Open Banking went "live" there were only 385,000 API calls.

In 2020 though, Open Banking looks like it has turned the corner, with some significant developments across the industry.

Firstly, the consumer experience has now been supercharged. All major UK banks now offer an "In-App" mobile authentication journey, meaning consumer can authenticate and pay using the biometrics on their mobile device. API reliability has also improved. In July 2020, the major banks provided 99.25% availability, with 99.12% of all API calls successful, meaning consumers can now use the services with confidence.

Secondly, a number of notable merchants are now going live with Open Banking payment solutions, particularly in the financial services sector. These "halo" type merchants are leveraging the power of Open Banking payments to enable their customers to pay in a fast and frictionless manner. With the consumer brand and trust they have, they are able to quickly drive use and adoption of the payment option within their customer base.

And lastly, use of Open Banking has started to become more wide spread amongst consumers. UK Open Banking Implementation Entity (OBIE) announced that Open Banking had hit the 2 million users mark in September 2020, and payment API calls having grown by more than 300% from January 2020 according to the OBIE statistics.

But despite these developments, consumer awareness of Open Banking remains low. Uptake (or lack thereof) by consumers is perceived by merchants as one of the biggest barriers to the successful integration of Open Banking into a merchant's checkout options. The current growth in the Open Banking ecosystem is being driven by a handful of successful payment use cases. The question remains as to when and what will trigger the broader adoption of Open Banking payments by consumers.

This report, based on a survey of over 2,000 UK consumers in September 2020, explores consumer perceptions on payment methods, and outlines willingness to adopt Open Banking payments in various use cases and situations.

About the research

The research was conducted by Censuswide, with 2,028 consumers in the UK surveyed. The fieldwork took place between 09.09.2020 - 11.09.2020. Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles.

Open Banking Implementation Entity, API Statistics, https://www.openbanking.org.uk/providers/account-providers/api-performance/

1. Consumers demand better security in their payment methods

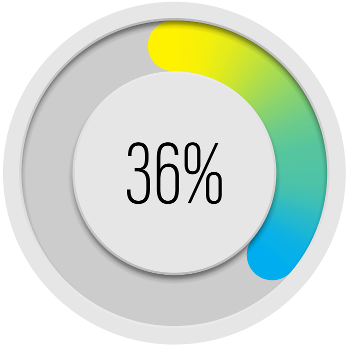
Payment security is critical for consumers

Consumers, rightfully, demand strong security from their payment methods. They want confidence that their transaction and payment credentials won't be compromised, putting them at risk of fraud or unauthorised transactions. For online payments, 58% of consumers list security as their biggest concern – ranking higher than any other factor – while for in-store payments, 38% of consumers still list security as their biggest concern.

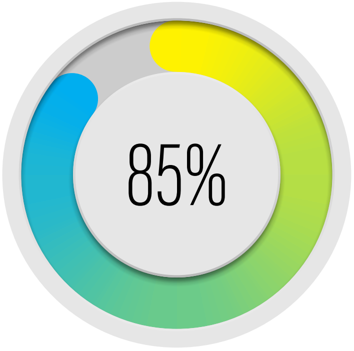
Concerns about the security of payments have implications for the way that consumers behave and pay.

Merchants will lose sales opportunities if they can't present secure payment options for customers. For example, 36% of consumers have refrained from buying goods or services from a particular online merchant because of concerns about payment security. Furthermore, only 15% of consumers will always store their payment card details with a merchant for easy checkout, while 23% of consumers claim they are never willing to store such details. This is due to concerns about the security of their payment credentials and personal information, as well as a lack of trust in the merchant to handle the stored card details appropriately. If merchants aren't missing out on sales opportunities because of this, at a minimum it means it is harder for customers to make repeat purchases, reducing a consumer's stickiness with a merchant.

Security concerns are not just an issue in the online payments world, but in the instore environment too. 52% of respondents have never used their phone to make a contactless payment, with the primary reason for not doing so being concerns about storing card data in the device. This stops consumers being able to leverage the benefits of biometric authentication on their device (and the security benefits that it delivers).

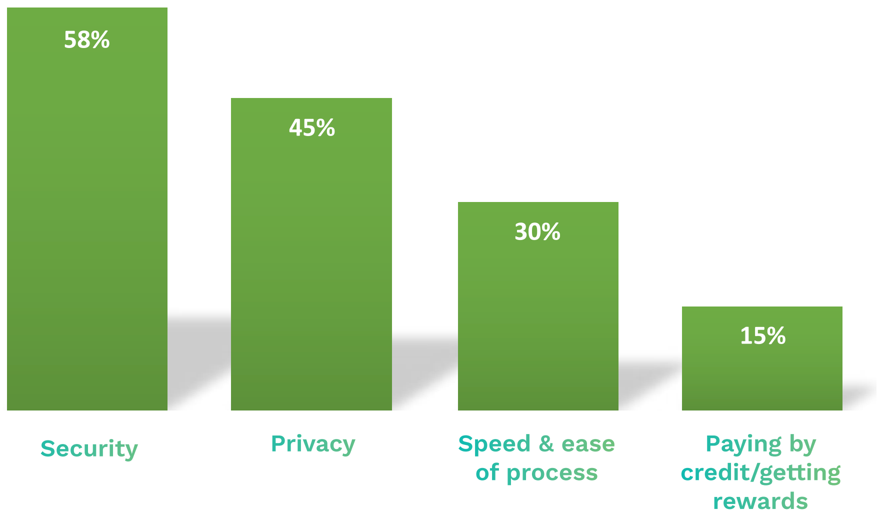


Consumers who have refrained from buying something online due to concerns about payment security.



Consumer who won't store their card details with all merchants

Concerns when paying online



[2] UK Finance Fraud – The Facts 2020, https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-11-June.pdf

Consumer concerns about security are not unfounded.

Payment methods present security risks

Payment fraud is high. The UK's most ubiquitous payment method, cards, suffers from ongoing challenges from fraudulent payments stemming from stolen card details and poor merchant processing practices. Our consumer research found that, in the last 6 months alone, 12% of cardholders claim to have had a fraudulent or unauthorised transaction on one of their payment cards.

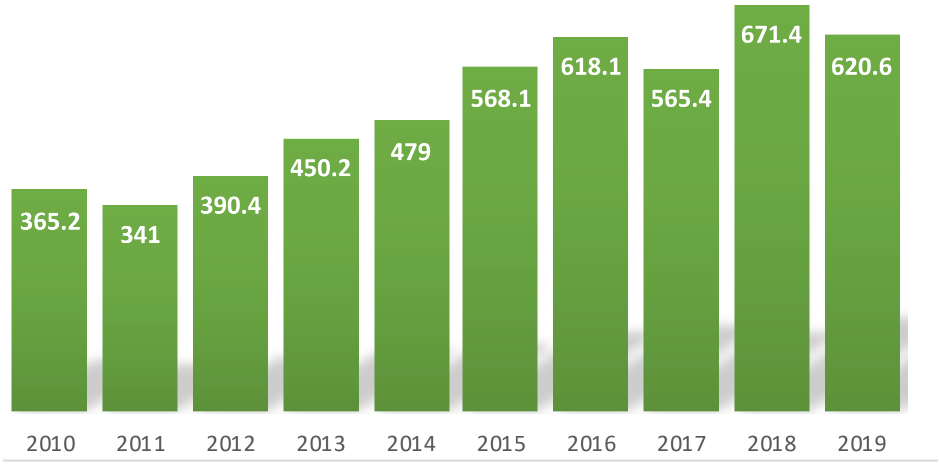
UK card fraud has been trending up over the last decade. Total losses from card fraud in the UK reached £620M in 2019 according to UK Finance([2]). This equates to 7.5p for every £100 spent in the UK.

> *Total losses from card fraud in the UK reached £620M in 2019."*

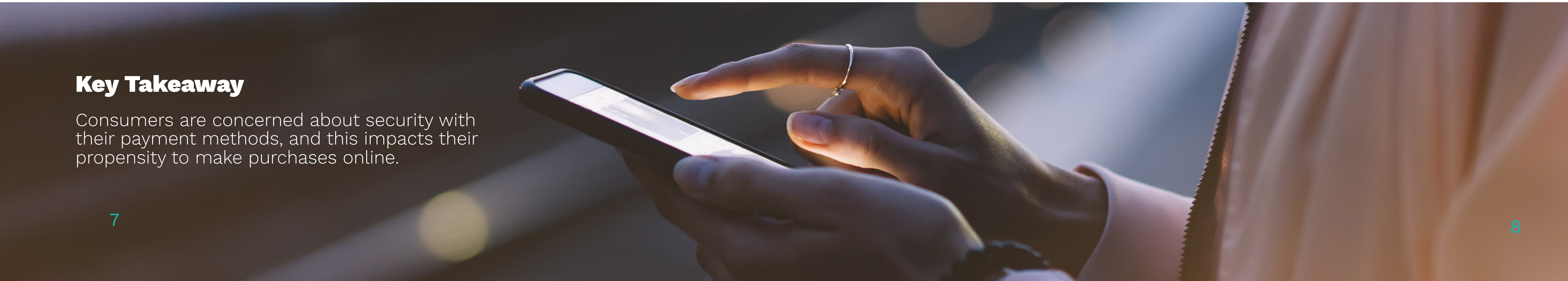
According to the study, the vast majority of the fraud in the UK – about 75% - comes from card not present fraud. This is where stolen card details are obtained, i.e. from a data breach on a merchant site, and used to purchase items online. This accounted for over £470M in fraud losses in the UK in 2019. Another recent report, Dark Market Report by Armor, highlights how inexpensive it is to buy cloned card details on the dark web to carry out this type of fraud ([3]). The research shows UK Visa and Mastercard details sell for between £11.50-15.00 online.

These fraud costs (losses) could be avoided if a consumer wasn't required to share their card details with a merchant just to make a payment.

Annual losses from payment card fraud in the UK (£M)

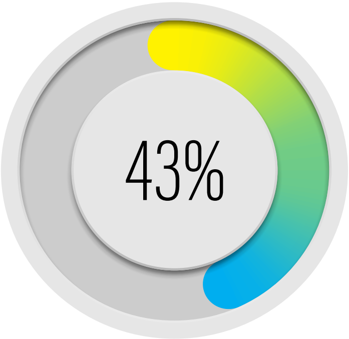


[3] Armor, Dark Market Report: The New Economy, https://www.armor.com/resources/the-dark-market-report/

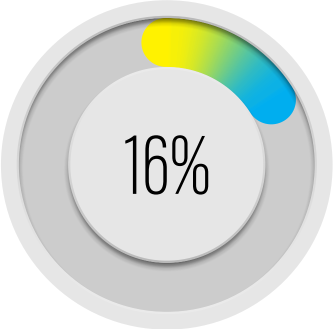


Key Takeaway

Consumers are concerned about security with their payment methods, and this impacts their propensity to make purchases online.



Consumers who say 3DS 'takes time and adds complexity'



Consumers who say 3DS puts them off paying by card

Are card schemes doing enough?

It seems payment cards have still not implemented additional payment security measures to address the risks with fraudulent transactions. This is despite the European Union introducing new rules for payment cards requiring Strong Customer Authentication (or SCA) to be used (initially to be implemented by September 2019, and now extended until as late as March 2021).

With the final implementation deadline looming many consumers are yet to see the use of SCA for their online card payments. According to the research, only 39% of consumers claimed to have needed to use SCA to make a payment via card online – a low number for late 2020.

The challenge for payment cards is the full introduction of SCA may only cause greater challenges. Only 40% of those who had used 3DS (the card schemes solution for SCA) described it as "seamless and easy". On the flip side, 43% said it "takes time and adds complexity", while a further 16% said that it is "painful and annoying" and "puts them off paying by card".

Furthermore, recent analysis by CMSPI ([4]) , a payment consultancy business, found 24% of online card transactions could fail if 3DS was introduced with a cliff edge. Failure rates that high would cause significant lost sales for merchants, not to mention causing mass consumer frustration.

[4] CMSPI, SCA Impact Assessment, September 2020

Plastic cards have biosecurity risks too

In a post Covid world, biosecurity is expected to become a more pertinent concern for consumers. Surprisingly plastic, payment cards don't stack up well here.

A research study by LendEDU ([5]) in May 2019 found that cards were in fact the dirtiest payment method of those studied, having an average germ score of 285. This compares to 160 for cash and 136 for coins. This is likely a result of their constant use, passing through multiple hands or being left on tables and bar counters. Equally, while the contactless limit has been increased in the UK, consumers still need to use PIN pads for a large number of transactions, a prime opportunity for the spreading of germs.

Consumers are now conscious of the risks of germs. The consumer research found that 42% of payers were concerned about the germs on payment cards. As payment methods and choices rapidly evolve, there may be a further evolution away from plastic cards, in favour of touchless payment solutions.

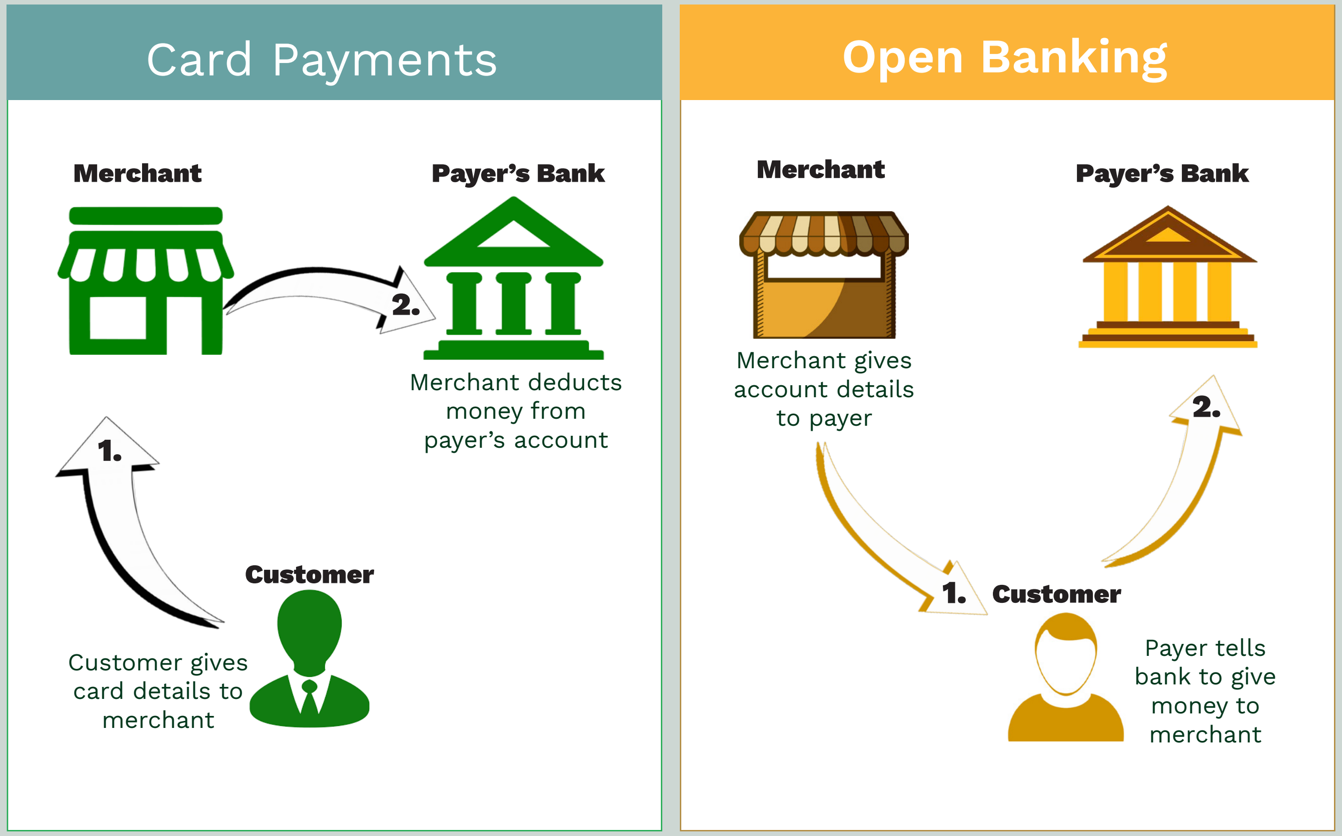
> *"42% of payers are concerned about the germs on payment cards."*

Consumers deserve a better option

Consumers and merchants both deserve better. They deserve a secure payment solution which doesn't require a payer to share their details, which enables a customer to complete SCA in a seamless way, and has low levels of fraud.

Open Banking payments have some fundamentally different security design features compared to payment cards.

Open Banking is designed as a push payment – that is, customers go to their bank and push a payment from their account to the merchant. This is the reverse of card payments. With card payments, a customer gives their card details to a merchant, who then goes to the payer's bank and pulls the money from the consumers account.


Card Payments
Merchant
Payer's Bank
2.
Merchant deducts money from payer's account
1.
Customer
Customer gives card details to merchant
Open Banking
Merchant
Payer's Bank
Merchant gives account details to payer
2.
1.
Customer
Payer tells bank to give money to merchant

***Push and pull illustration**, highlighting a card payment where the merchant pulls money from the customer's account vs an open banking payment where the customer pushes a payment from their bank account to the merchant.*

With Open Banking, consumers authorise the payment using their existing internet or mobile banking log-in credentials, directly into their normal mobile banking interface. In many cases, this authentication and authorisation of a payment is done using biometrics in their banking App, providing a seamless user experience. Importantly, no account credentials are ever shared with the merchant under this model, significantly reducing the risk for payer and merchant.

While these benefits are well understood by those in the Open Banking and increasingly the merchant community, these security benefits are not always understood by consumers. 32% of consumers that wouldn't be willing to pay via Open Banking said this was because they "don't want to share" their account credentials with the merchant – a complete misconception given the fact that Open Banking under PSD2 is inherently designed to avoid credential sharing.

This is the challenge of Open Banking providers to overcome.

Providers must communicate effectively with potential payers, explaining how the payments work and, most importantly, how they are authorised securely. If providers and merchants can overcome this challenge, then adoption will likely accelerate. Our research revealed an additional 28% of consumers would be willing to try making an Open Banking payment if they understood more about the security features of Open Banking.

> "An additional 28% of consumers would be willing to pay by Open Banking if they understood the security features."

[5] LendEDU, Dirty Money, https://lendedu.com/blog/dirty-money-credit-cards/

About Nuapay

Sentenial is a pioneer of Open Banking and is the industry's leading provider of Account-2-Account payment solutions. We securely process over €42bn every year delivering services directly to businesses of all sizes as well as being an outsourcing provider to many of the world's leading Banks.

Nuapay, a subsidiary company of Sentenial, is licenced by the FCA as a Payment Institution with the ability to provide accounts to businesses, process payments and deliver Open Banking functionality. Using the full scope of its licence, Nuapay has developed fully integrated products that extend the benefits offered by Open Banking and simplify the process of deployment.

Today, we offer partners a fully comprehensive, integrated payment solution that removes all traditional banking inefficiencies and unnecessary costs, saving you time, money and resources at every turn. This is banking as it should be.

www.nuapay.com

NUAPAY