entersekt

and you're in.

Fighting back against mobile banking and payments fraud in Europe

Consumers favor financial institutions that offer modern authentication methods to secure their data and transactions

An Entersekt consumer survey report

www.entersekt.com

Table of contents

Introduction

The new normal for European banking customers

The world of banking and commerce is rapidly evolving. Where brick-and-mortar banks and retail stores once stood tall, most of today's consumers have accepted mobile banking and payment methods, as well as online shopping, as the new normal.

And while consumers appear keen to embrace the latest technology for convenience's sake, it's clear that many still place a great deal of emphasis on the security of their transactions. In fact, as this report will reveal, security is such a high priority for some that even high levels of friction encountered during transactions are often overlooked in exchange. And their concerns are not without merit…

In the first half of 2022, in the UK alone, fraud cost financial institutions (FIs) an enormous £305.2 million — an increase of over 4% compared to the same period in **2021.**[1] Unfortunately, as mobile usage increases, so too do opportunities for criminal activity, bringing to the surface several **types of evolving attack vectors** that put consumers at risk. These include SIM-swap attacks, device cloning, man-in-the-middle attacks, and mobile banking malware, to name a few.

It's clear that FIs need to provide mobile banking and payment experiences that are both modern and secure if they want to meet the needs of today's customers – and drive loyalty.

Fighting back against mobile banking and payments fraud

In this report, we examine the results of a survey conducted on behalf of Entersekt on 5,000 banking customers across the UK, Norway, Hungary, and Germany. The aim of the survey was to gain a deeper understanding of end-customer sentiment, across regions, in three key areas:

1. How consumers use their bank's mobile banking apps,
2. Thinking around banking security and private data, and
3. Preferences pertaining to online payments.

The results provide valuable insight into the evolution of banking and banking security, as well as compelling reasons for banks to pay attention to the expectations of their customers if they're to conquer fraud.

Let's get started!

[1] Fraud Barometer: Half Year Highlights 2022, 2022, KPMG UK

Survey snapshot: Consumers appreciate convenience, but prioritize security

72% use their banking app several times a week

74% feel secure using their banking app for online banking

50% would switch banks if they felt their account was not secure

51% would hold their banks responsible for any fraud or cybercrime

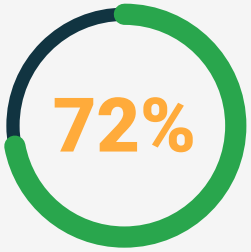
51% are worried about fraud when shopping online

71% said the security of a transaction is more important than a good experience

How consumers use their banks' mobile banking apps

Mobile banking becoming a creature comfort

The survey revealed that consumers, in general, are growing more comfortable with mobile banking. They're heavily reliant on banking apps that enable them to perform banking and related activities at their convenience. In just a few clicks, they enjoy being able to check their balance, pay a bill, or shop online. In this report, 72% of respondents indicated that they use their banking app several times a week.



72% of respondents indicated that they use their banking app several times a week

An increase in mobile banking activities

The report also indicates that customers use their mobile device for a variety of activities, with 74% saying they check their bank balance, followed by 69% using it for online shopping, and 65% of respondents saying they pay their bills on their mobile.

Mobile activities of consumers

74% check their bank balance.
69% shop online.
65% pay their bills.
56% send money to friends/family.
37% set up and manage automatic regular payments.

Perhaps not surprising is that users of different ages use their phones for different activities. For example, respondents aged 35-44 are more likely to use their mobile to check their balance (81%) and online shopping (77%), whereas those aged 16-24 are least likely to check their balance (62%), and those aged 55+ are least likely to shop online (60%).

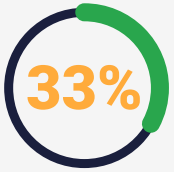
The data also suggests that if banking apps had more features and capabilities, that approximately half of customers between the ages of 16-24 and 25-34 would use them more often.

Essentially, consumers enjoy the modern conveniences of mobile banking, which is only possible if their financial service provider adopts modern banking and authentication technology.

High confidence in mobile banking security

Underlying the increase in mobile banking usage is a growing sense of trust in mobile banking security. The report indicates that that 38% of respondents are worried about fraud when using their bank's mobile app while a large proportion, 33%, do not harbor concerns about mobile banking fraud.

of respondents are concerned about mobile banking fraud



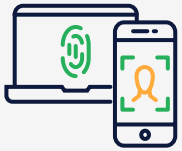
are not concerned about mobile banking fraud

Looking at the data in more detail — particularly, at what device is perceived as most secure for mobile banking — 74% of respondents indicated they felt most secure using their bank's app on their phone, followed by 95% on their tablet, laptop, or computer.

From these findings, it's evident that consumers are more concerned about the security of their data than the convenience and user experience.

C-suite checklist: Top 3 banking app usage takeaways

1. Consumers are growing more comfortable with the idea of mobile banking. Banks that don't prioritize their mobile offerings risk losing out to competitors.



2. Convenience is important. Banks that offer modern banking and authentication methods are more likely to attract new business and retain existing customers.

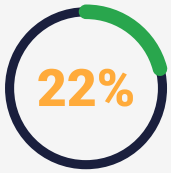
3. Security of data, however, is valued over convenience and user experience. Banks that emphasize security are more likely to be trusted.

Consumer thinking around banking security and their sensitive data

Account security

A significant finding that emerged was that 50% of respondents would switch to another bank based on how secure they think their accounts are. What's more, a further 22% strongly agree that they would switch to another bank if they felt the bank's security was compromised or weak.

would switch to another bank based on account security



strongly agree that they would switch to another bank if they felt the bank's security was compromised

The results also suggest that respondents are more likely to agree than disagree that they feel secure if their bank account is protected only by their password (40% vs 32%).

Along with the security of their overall account, respondents also expressed a range of reactions regarding the security of their personal data.

Sharing sensitive information

When it comes to sharing sensitive information, the data shows respondents feel more comfortable sharing certain details like their email address (55%) and date of birth (53%) with a representative of a bank's call center to attain a better user experience. They are less comfortable sharing info like their bank card PIN (26%) and their online account or profile password (28%).

How customers are most comfortable sharing information

- Email address (55%)
- Date of birth (53%)
- Street address (45%)
- One-time PIN sent via SMS (45%)
- Mother's maiden name (42%)

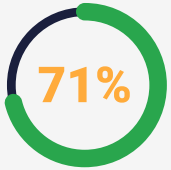
In the unfortunate situation of losing money due to fraud or cybercrime, 51% of respondents stated that they would most likely hold their bank responsible. This is closely followed by just under half of respondents saying the criminal would be responsible.

And, even though FIs partnering with world-class banking security innovators keep consumer data safe, some consumers revealed that they may perceive sharing sensitive information with their FIs as a risk.

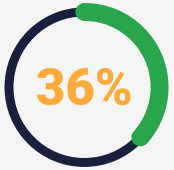
The security of online shopping

Although e-commerce is a common shopping method for many people, some consumers do still consider the activity to be risky. The report indicates that 52% of respondents are worried about fraud when shopping online and 19% say they strongly agree with this statement.

In fact, the security of shopping online can be more important than the actual shopping experience. For example, 71% of respondents said the security of a transaction is more important to them than a good experience, with 36% stating that they strongly agree. Interestingly, respondents aged 55+ are more likely to say security is more important than the experience (76%) compared to those aged 16-24 (64%).



prioritize security over experience



strongly agree

Ultimately, FIs should try to match these expectations with authentication solutions that don't interrupt their transactions or prevent them from going through. Rather, they should aim to introduce the right type of authentication, with the appropriate amount of friction, at the right time – using models such as Entersekt's Context Aware™ Authentication solution.

Maintaining secure transactions with appropriate authentication

The results show that a mix of methods are required when respondents authenticate their identity when logging in to their internet banking profiles. Though the most common method is a username and password combination (19%), this is followed by facial recognition (14%), fingerprint scans on their computer or laptop keyboard (14%), and SMS OTP (13%).

Respondents are least likely to be required to use their digital identity (10%), a notification or authentication request sent to their banking app (10%), OTP sent to their email (5%), or hardware token (5%).

Once logged in to their banking apps, and completing a transaction, 25% of respondents said they are required to scan their fingerprint to authenticate their transaction, whereas 21% said they are required to enter an SMS OTP. This is closely followed by 19% saying they scan their face and 12% sharing that they are required to respond to a message in their banking app.

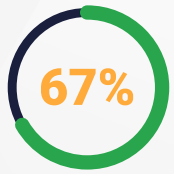
Only 7% of respondents are required to enter an OTP sent to their email, while just 3% are not required to authenticate transactions at all.

Most common transaction authentication methods

- 25% fingerprint scans
- 21% SMS OTP
- 19% facial recognition
- 12% message in banking app
- 7% email OTP

Interestingly, an additional opportunity to confirm a transaction made from their mobile device before it is carried out is clearly essential among respondents with a 90% score. In fact, 67% shared that they would like to confirm all their transactions beforehand.

of consumers want to confirm a transaction on their mobile before it's carried out



want to confirm all transactions beforehand

FIs that understand their customers' thinking around banking security, and how they prefer to make purchases online, have the tools to narrow the customer gap.

C-suite checklist: Top 3 reasons for FIs to prioritize security

1. Customers who think their accounts are at risk are likely to switch to another bank.

2. Over half of consumers would blame their bank should they fall victim to fraudulent activity.

3. e-Commerce transactions still carry a perceived risk. Consumers feel comforted by a degree of visible security.

Consumer preferences for online payments

Preferred payment methods

Customers each have their own preferences when it comes to online payment and authentication. And, as their expectations for modern, hassle-free experiences grow, FIs need to meet their needs with personalized, seamless customer journeys.

When shopping online, 29% of respondents are most likely to use PayPal to complete their purchases. Following this, 15% said they use a debit card and 13% use a credit card. The data shows that 64% of respondents typically feel secure when using their credit card or debit card for online shopping, with 20% stating they feel very secure doing this.

Preferred payment methods

- 29% PayPal
- 15% debit card
- 13% credit card
- 10% Klarna
- 7% cash on delivery

Although respondents of all ages appear to favor PayPal for online payments, it seems 25% of older respondents aged 55+ rely more on debit cards and credit cards (21%) for online purchases. Those aged 16-24 are more likely to use Apple Pay (11%), whereas only 2% of respondents aged 55+ said they use this method.

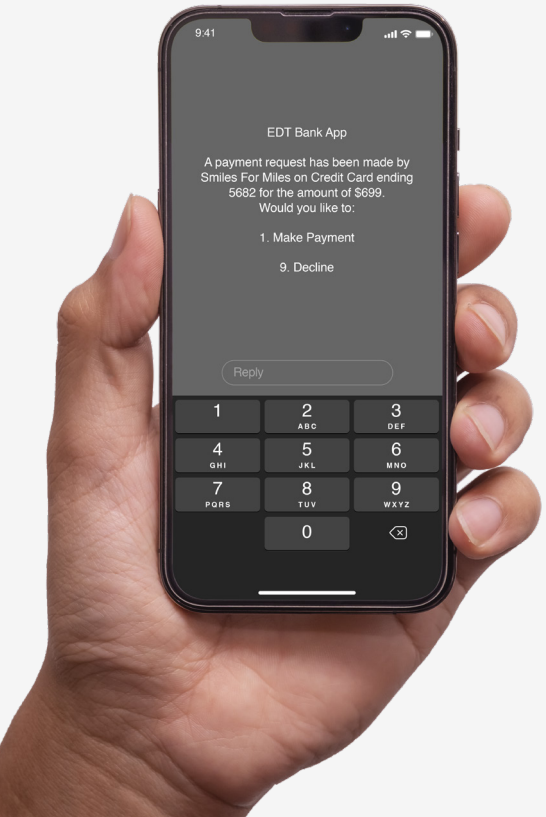
The data also shows differences in online shopping payment methods depending on the number of accounts respondents have. For example, those with 1 (30%), 2 (30%), or 3 (26%) accounts are most likely to use PayPal for online payments, whereas those with 4 or more accounts seem more likely to use their credit card (24%) over other methods.

> Considering the agility and personalization that fintech disruptors offer their customers, there's an even more pressing need for FIs to incorporate cutting-edge authentication that balances security and convenience.

Authorizing online payments

Almost a quarter of respondents said they authorize a payment by responding to an authentication request sent to their banking or authentication app.

Some 17% said they enter an SMS OTP and 14% said they enter a password or authorize it with their digital ID (14%). This is closely followed by 13% saying they enter a password and a one-time PIN sent to their mobile or email. Only 7% of respondents enter a one-time PIN sent to their email or answer a phone call to authorize the payment (3%).



How respondents authenticate payments

- 17% SMS OTP
- 14% password or digital ID
- 13% password and one-time PIN
- 7% one-time PIN
- 3% phone call authorization

C-suite checklist: What customer preferences mean for FIs

1. Depending on several factors, customers' preferences for online payment methods differ vastly.

2. The most popular method of authorizing payments is responding to an authentication request sent to a banking or authenticator app.

3. To stay ahead, FIs must incorporate cutting-edge authentication that balances security and convenience.

Conclusion: Security trumps convenience

The report findings indicate that banking and authentication technology is evolving and will continue to do so to meet the expectations of today's tech-savvy banking customers.

On the technology side, we see the preference for mobile banking is growing fast, along with a growing interest in open banking. Though the popularity of credit card payments across Europe varies by country, in general, consumers tend to favor less traditional payment solutions, such as Klarna and PayPal, and potentially Klarna Kosma (Klarna's new open banking solution).

Regarding perceptions around fraud prevention and security vs convenience, it's clear that security trumps convenience with the majority of respondents indicating they would switch to another bank if they felt their bank's security was inadequate.

The data also revealed interesting insights on the relationship between payment security and consumer choice. It has long been the assumption that banking customers would prefer frictionless transactions, however the research does not back this up. Given a choice, some customers would prefer to authenticate their transactions — with some kind of authentication trigger or action.

"It has long been the assumption that banking customers would prefer frictionless transactions, however the research does not back this up. Given a choice, some customers would prefer to authenticate their transactions."

In relation to authentication methods, the findings show a general shift towards more modern banking security tools. Yet, there is still a prevalence of outdated authentication practices in the industry, like SMS OTP. Unfortunately, SMS OTP is the least secure method of authentication when it's used as the sole factor to verify a customer's transaction.

Ultimately, the findings confirm that a one-size-fits-all approach to fraud prevention is not the answer. At Entersekt, we offer world-class customer authentication and payment authentication experiences that bring together convenience and security across all digital banking and payment channels, including open banking and Buy Now Pay Later platforms.

We know that listening to consumers fuels our innovation, and this translates to increased customer loyalty for banks, credit unions, issuers, and merchants.

Contact one of our experts to learn more.
Visit www.entersekt.com/contact-us.

Frans Labuschagne,
Entersekt VP Channel Partnerships

Methodology

This report was compiled using the results of an online survey conducted on behalf of Entersekt by global market research consultancy, Censuswide. The survey took place between the 21st and 27th of September 2022 and surveyed 5,000 respondents age 18+ with a bank account across the UK, Norway, Hungary, and Germany.

Censuswide is a member of the global association ESOMAR, the voice of the data, research, and insights community. It also complies with the Market Research Society (MRS) code of conduct based on the ESOMAR principles. Before fieldwork commenced, the questionnaire was compliance tested to ensure it was in line with MRS codes of conduct.

About **Entersekt.**

Entersekt provides transaction authentication to financial institutions that is both secure and free from unnecessary friction. Our single, cross-channel platform empowers these institutions to build great user experiences for their customers, helping to drive revenue growth without adding further costs and complexities to their ecosystems.

For over a decade, we have enabled some of the world's most prominent financial brands with the tools and confidence to conquer fraud, compliance, disparate customer journeys, and the related bottom-line impact of reputational damage and customer loss. Backed by companies like US-based Accel-KKR, one of the world's top private equity firms, Entersekt continues to innovate and expand its global footprint.

For more information about Entersekt, or to speak to an expert, please visit www.entersekt.com or email info@entersekt.com.

/Entersekt

@Entersekt

/Entersekt