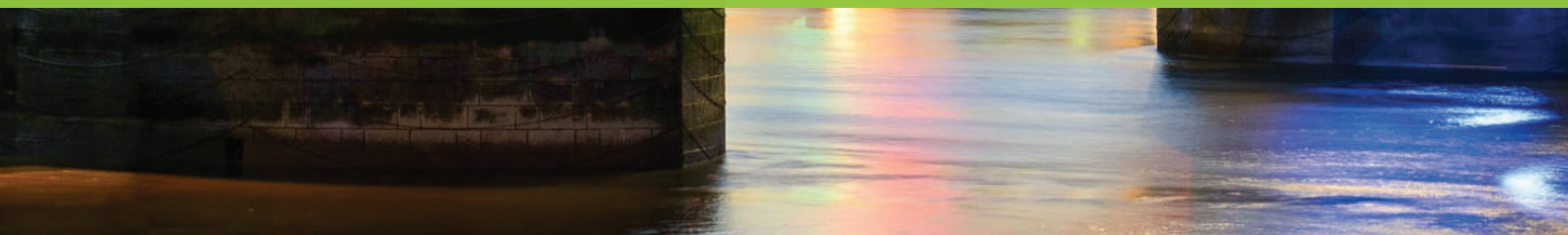
THE BANKS' BALANCING ACT: FRAUD RISK VS THE CUSTOMER EXPERIENCE

CONSUMER REPORT 2017



Introduction

It's no secret that all banks and payment services providers are universally challenged with protecting customers from increasingly sophisticated fraudulent techniques to separate them from their money. This challenge is exacerbated as the UK's adoption of banking technology reaches new maturity with the advent of mobile banking, which some reports have found has taken over "internet" (desktop or browser-based) banking. According to the most recent statistics from the British Banking Association (BBA) in July 2016, desktop-based online banking had fallen for the first time, while mobile banking had risen. On average, customers logged onto banking websites 4.3m times a day in 2015, down from 4.4m in 2014, while apps went up from 7m logins a day in 2014 to 11m in 2015.

As consumers of all ages switch in droves from the browser to the smartphone to manage their personal finances – from current and savings accounts to credit cards – the world of banking is opening up many more doors for criminals to take advantage of. The numbers speak for themselves: according to the Crime Survey bulletin from the Office of National Statistics released in December 2016, 'cyber-related' fraud made up over half (51%) of all 3.8 million fraudulent incidents during the preceding 12 months to March 2016. Of this number, two-thirds (66%) were categorised as 'bank and credit account' fraud. Which? also reported that in 2014-2015, losses soared by 64% to £133.5 million for online banking (including mobile).

As a result, fraud follows the channels of adoption. Consumers adopt mobile banking because it is convenient; it is easy to use and fits in with today's increasingly digital lifestyles – according to Ofcom, smartphone penetration among UK adults is at 93%. Although we are far from being a cashless society (Payments UK predicts that by 2020, cash will drop to being used for just over a quarter of payments), UK consumers, more than many others worldwide, are used to tapping, waving, touching and even using their own biometrics to make both simple and complex transactions.

With rapid developments in technology also come changes in regulation, guidance and legislation. For instance, the European Parliament formally adopted the revised Payment Services Directive (PSD2) for online transactions at the end of 2015. The following regulations seek to boost the protection of payments by requiring that providers use more sophisticated identity authentication techniques, to defend against the increasing fraud landscape.

The ruling means that payment services providers (PSPs) are now required to use multiple methods of authenticating someone's identity before payments can be completed. The rules state the two or more methods of authentication must be independent so they cannot be compromised by one another. For instance, a bank could require a card reader to accompany an account password, to make sure that two separate verification processes protect customer data. Some devices also offer biometric options such as voice verification (via a quick call to the contact centre) and fingerprint recognition. But these verification methods bring about a whole set of challenges of their own – especially with the popular use of SMS to send one time passcodes. As a result, a very sophisticated type of fraud, known as SIM Swap, where criminals can essentially "switch" your digital identity to their own device, is now common place. This fraud relies upon the inherent vulnerability of SMS communication, and occurs when someone unlawfully obtains an identical SIM card, which re-directs communications away from the intended recipient and towards the fraudster.

Consumer expectations, however, are a huge roadblock when it comes to adopting more advanced security tools, potentially laden with friction along the customer journey. If a company we buy from or deal with does not match up to the customer experience we are used to today, we'll simply walk away. For banking customers, ease of change has been facilitated by the seven-day switching rule, introduced in 2013. There is also the consideration of the big, traditional banks, which have established technology frameworks (often legacy) that must integrate with modern tools to provide exceptional customer experiences. The challenger banks and building societies have no such agility issues and, while they do not have hundreds of years of experience in the market, they do have extreme flexibility and resources normally the reserve of larger organisations thanks to advances in cloud computing and the cost effectiveness of access.

With all this under consideration, there is one end goal for any bank today. There is a distinct balance that needs striking. Ultimately, the new banking experience must be as frictionless as possible, yet also ensure adequate protection from criminal activity.

Do banks invest in the best possible levels of security, but at the cost of irritating the customer and making transactions longer? Or do they play the convenience card, and increase the risk of fraud, potentially upsetting the customer even more in the long term?

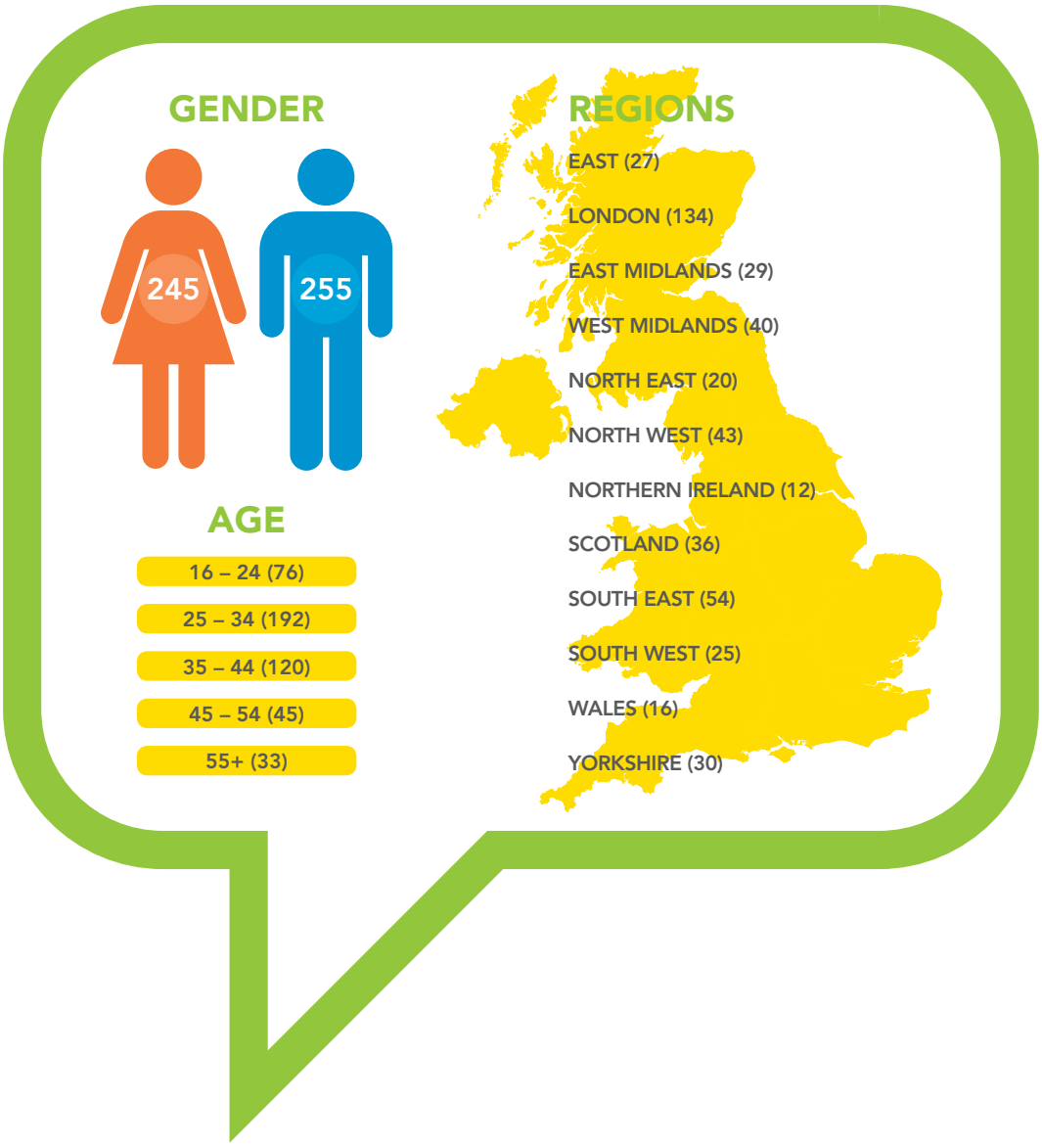
This research set out to find out just how far banks, building societies and credit card providers have come in the eyes of the UK consumer when it comes to delivering on their expectations, while keeping us safe.

Methodology and sampling

Aspect Software set out to discover the experiences of UK consumers who had suffered at least one incidence of banking fraud in the 12 months to April 2017. 500 consumers over the age of 16 years old were asked 13 questions about the occurrences, with a specific focus on how the bank, building society or credit card provider dealt with them – from being aware of the fraud to resolution and next steps.

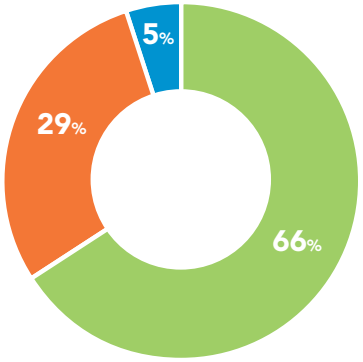
A total of 255 male respondents and 245 female respondents from England, Wales, Scotland and Northern Ireland took part in the study. Respondents were customers of a broad range of financial organisations, with more than 700 individual reports of fraudulent activity in the past year, with 34 individual financial services brands.

The study was conducted through a secure online portal by Censuswide, and commissioned by Aspect Software.



Findings Overview

In the past 12 months, how many incidences of fraudulent activity have you experienced on your bank or credit card account?



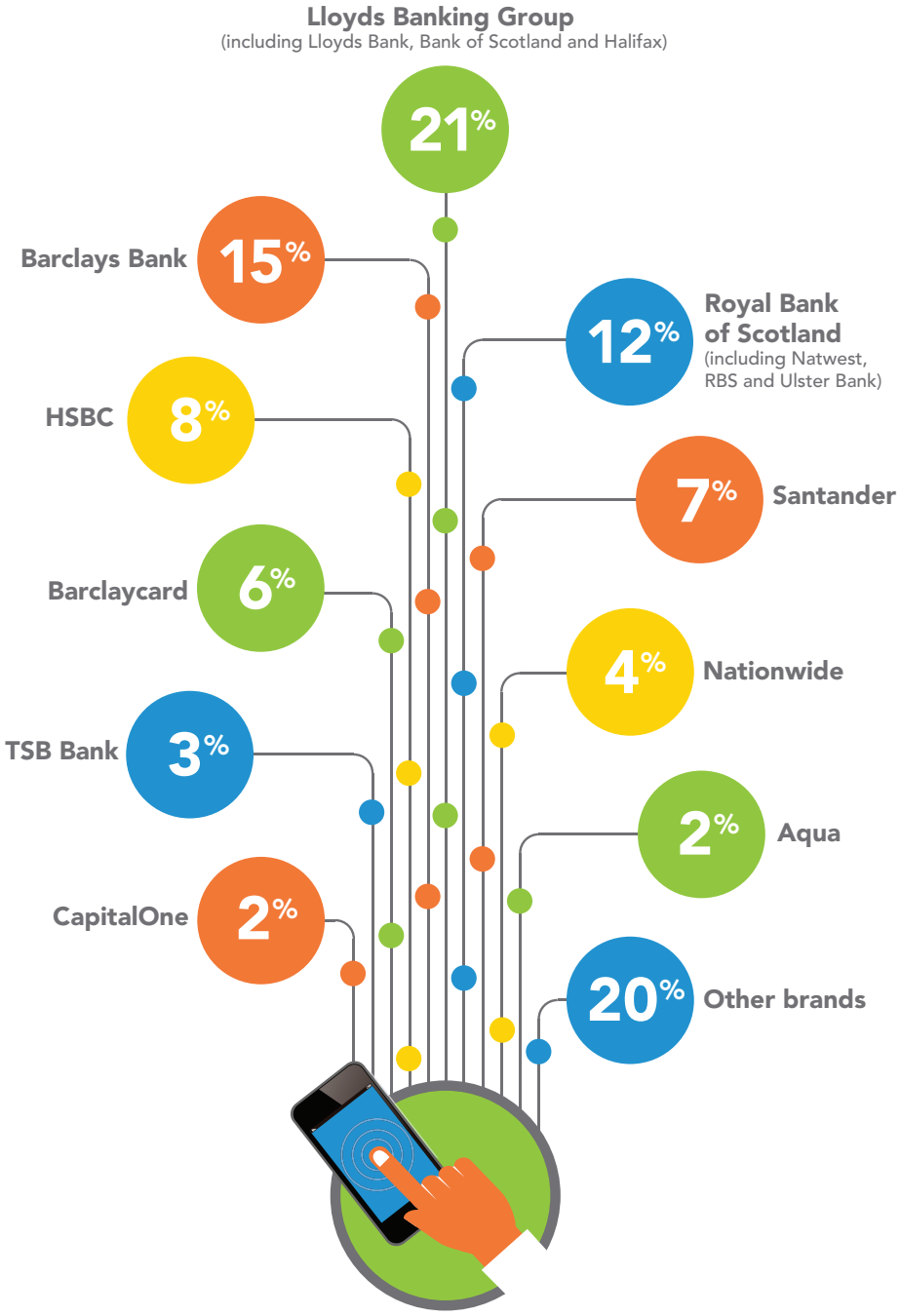
ONE INCIDENT
TWO INCIDENTS
THREE INCIDENTS

MEAN INCIDENCES: 1.42

When asked about the number of fraudulent incidents (any activity deemed fraudulent by the customer, such as a transaction not made by them) respondents had experienced in the 12 months prior to April 2017, two thirds of people (66%) reported just one incident. A further 29% reported two, with 5% reporting 3. Less than one% (0.4%) reported more than one incident, with the most claiming they were defrauded financially ten times in the given period. The mean number of fraudulent incidences was 1.42.

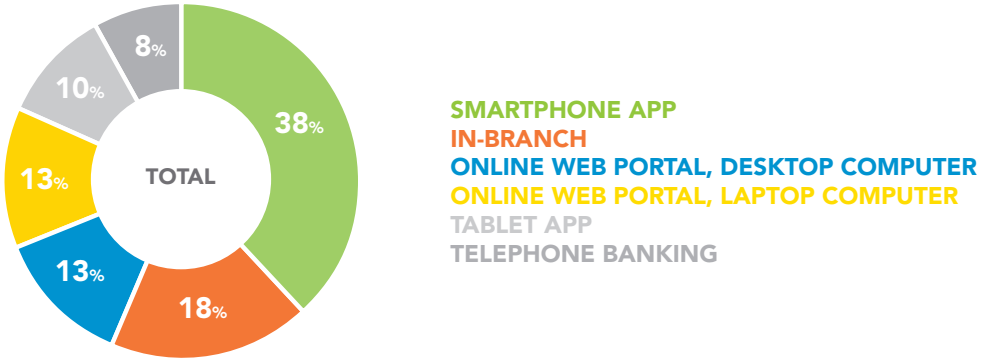
66% reported one fraudulent incident, 29% reported two and 5% reported three

Which banking or credit card provider was this with?



The banking groups and providers identified for all of the fraudulent incidences were proportional to the size of the organisations. Perhaps unsurprisingly, with a number of key brands under its umbrella, Lloyds Banking Group were targeted 21% of the time according to the sample, followed by Barclays Bank with 15% and RBS with 12%. The biggest standalone credit card provider was Barclaycard (not included under the Barclays brand for this report) with 6% of incidences.

What method do you use the most for accessing the account on which you experienced the latest incident of fraud?



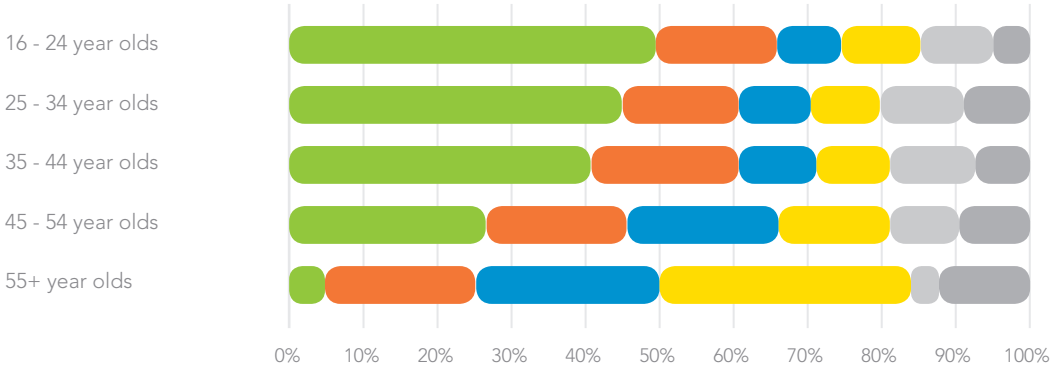
Smartphones were the top device, with 38% across all ages, genders and regions

Respondents were asked via what channel do they mostly access the defrauded account – not necessarily how they think the fraud occurred, but their preferred method of managing their money on that account.

Smartphones were fingered as the top device, with 38% across all ages, genders and regions, with a browser-based option or online portal coming in second with 26% (both desktop and laptop) – this was followed by branch with 18%.

Looking across the age ranges, it is perhaps pertinent to note device usage trends.

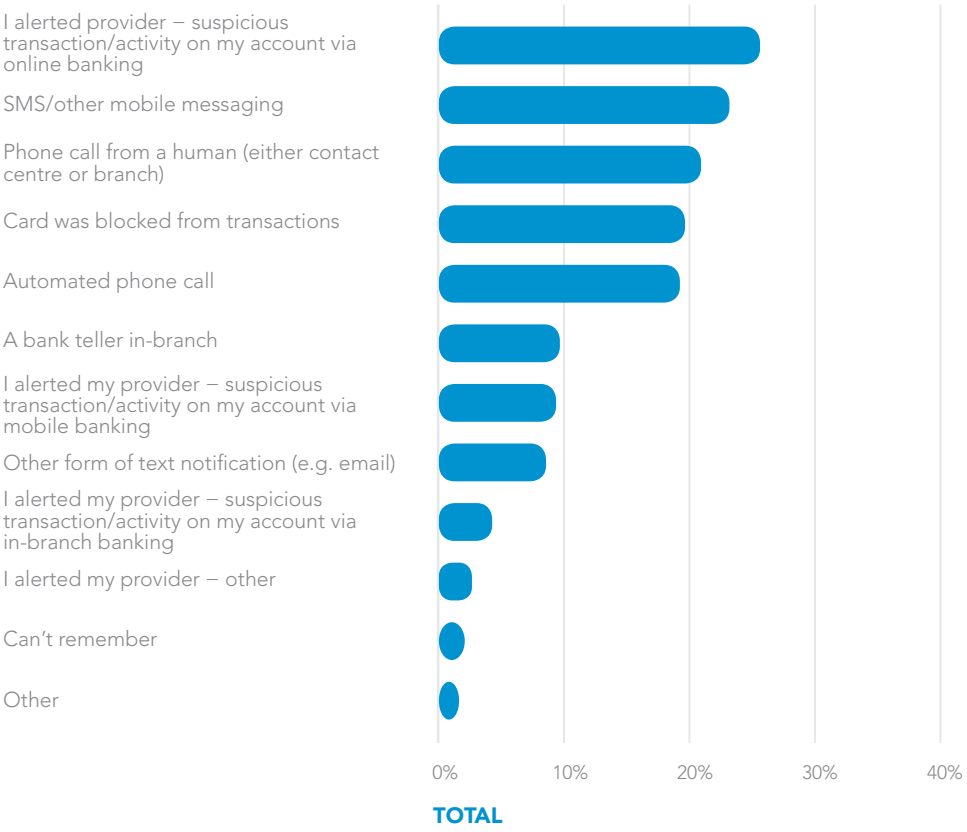
What method do you use the most for accessing the account on which you experienced the latest incident of fraud?



Those aged between 16 and 44 were the biggest users of smartphones to access their money, with 44% of the age range sample preferring mobile apps. Those aged between 45 and 54 years old identified the computer as their most used channel, with a combined percentage of 35% (28% for mobile apps). Only 4% of those aged over 55 years old prefer a mobile app, with 58% choosing a desktop or laptop computer. This age range was also the biggest user of the branch, with 21% selecting it as their most used method for accessing the account in question.

Detection, prevention and management of fraud

How were you first alerted that there had been fraudulent activity on your bank or credit card account?



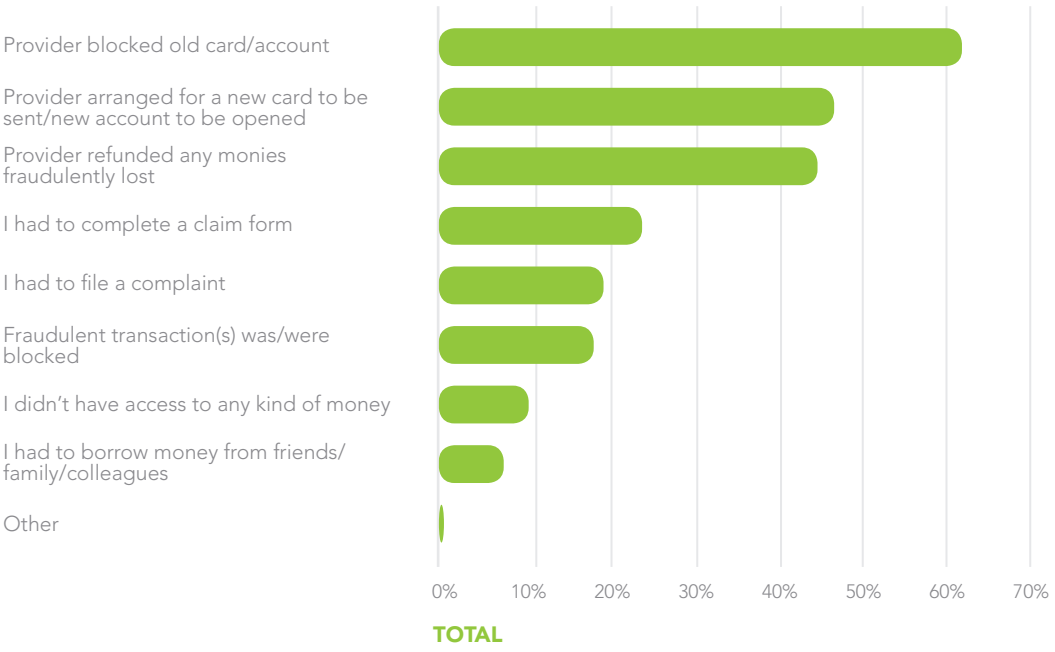
Mostly banks alert customers to a suspected fraud via an automated SMS or other mobile messaging

The most common way that customers were first alerted to any fraud on their bank, building society or credit card account(s) was that they personally saw a suspicious transaction/activity via online banking. Furthermore, in over a quarter of the instances (28%) the responses admitted to having to alerting their provider to the fraud first in some way, rather than any other form of notification from the provider to the customer. Disregarding whether they subsequently received any notification from the bank, arguably this number either shows that people are more likely to be keeping an eye on their finances and transactions, thanks to mobile banking, or that a quarter of providers are not being proactive or quick enough to keep customers notified of issues.

The most popular method for banks to use to alert a customer to a suspected fraud was via an automated SMS or other mobile messaging (such as iMessage), as shown by 24% of the response. This was followed by an automated phone call in 19% of instances, a physical conversation with a bank teller in-branch (10%), and email or other form of text notification (8%).

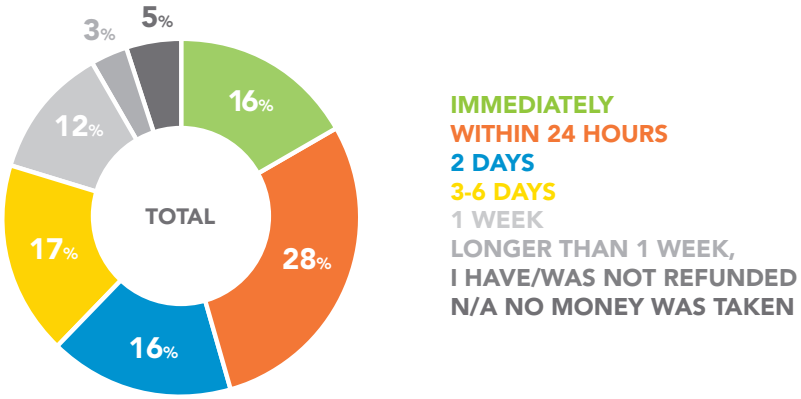
In one in five instances, the customer claims they were first aware there was an issue when their card was blocked from making transactions. Depending on the provider, cards may be blocked and re-issued on immediate detection of suspected fraud, or only blocked once the customer confirms that suspicious activity was not of their own doing – we see this again when asked in general, what happened after being alerted to the fraudulent activity, when 63% of people say their card was eventually blocked altogether. Almost half of the time (47%) the provider immediately arranged for a new card to be sent to the victim, reducing unavoidable frustration where possible, but relying on the slow postal system. Is there perhaps a better way of giving people access to their money in this digital age?

What happened once you were alerted to the fraudulent activity?



In 9% of instances, customers claimed that they had no access to any money until their replacement card arrived. This may lead to borrowing from friends and family (8% of times).

How long did it take to get refunded by your provider for the fraudulent transaction(s)?



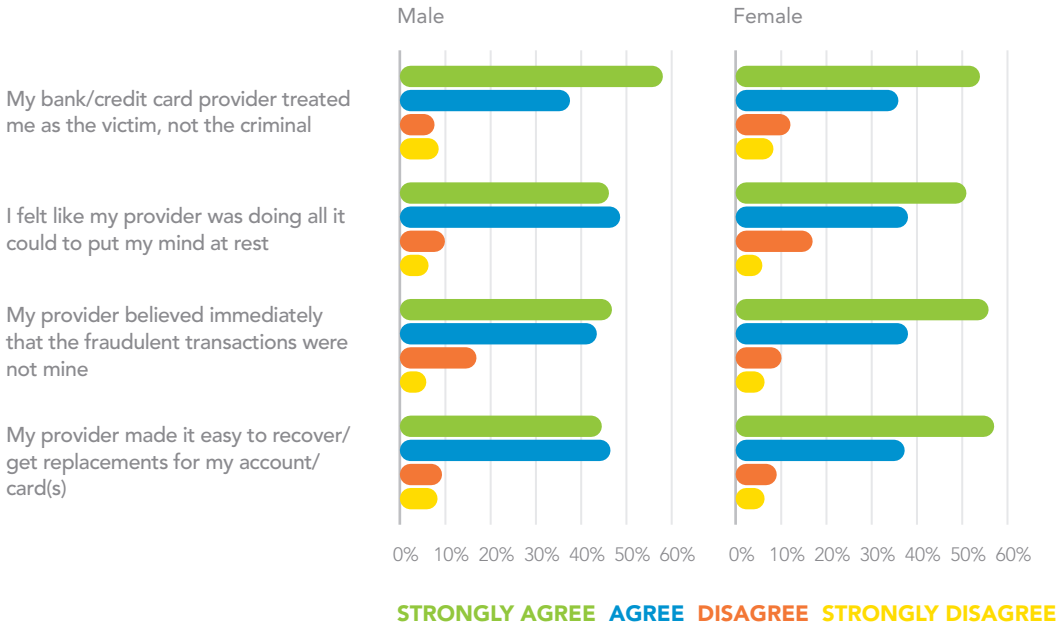
While in the previous question we discovered that in 44% of cases, monies lost to fraud was refunded, in this question we find out that on average banks took over 3.7 days to return funds to accounts. The mode result was closer to 24 hours, in 29% of instances. Alarmingly, 3% of people claim that it took longer than a week to get their money back, with a further 2% saying that they never received their money.

Interestingly, in 5% of occurrences, no money was actually taken.

In 44% of cases, monies lost to fraud was refunded, taking 3.7 days on average

The customer experience of fraud

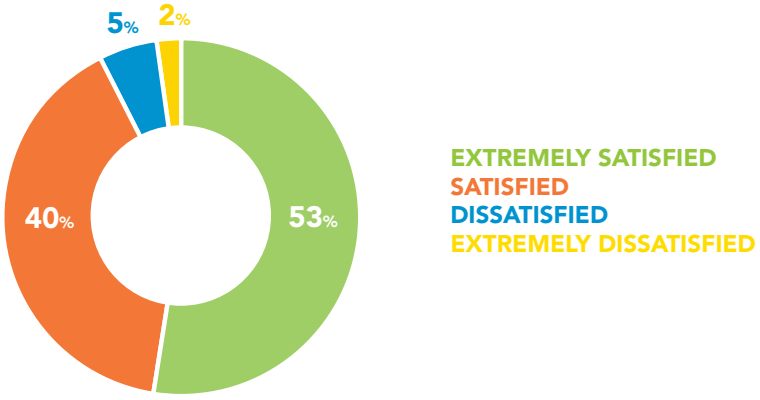
How strongly do you agree/disagree with the following statements, upon dealing with the fraudulent activity with your provider?



Encouragingly for the financial services industry, most people overwhelmingly felt that they were treated as a victim and not a criminal during the period of dealing with the last fraudulent event. Almost 9 in 10 people (89%) agree or strongly agree that this is the case. In the remaining instances (11%), people admitted to feeling like the criminal, despite any other measure the bank may have taken.

A similar proportion agreed that the provider was doing all it could to put the customer's mind at rest (88%), and the same for feeling like the bank did believe that the fraudulent transactions were not the customer's (88%). 89% of respondents agreed that the provider made it as easy as possible for the customer to recover/get replacements for their cards/accounts.

How satisfied were you with how your provider dealt with the fraudulent incident?



Encouragingly, most people overwhelmingly felt that they were treated as a victim and not a criminal by their provider

Considering the general population, the vast majority were either "satisfied" or "extremely satisfied" with how their provider dealt with the fraudulent incident in question, with 93%. Deviating from the norm is the older demographic; not one respondent over the age of 55 was dissatisfied with the service they received. The most 'disgruntled' age group was 25 to 34 years old, with 10% claiming dissatisfaction of some level.

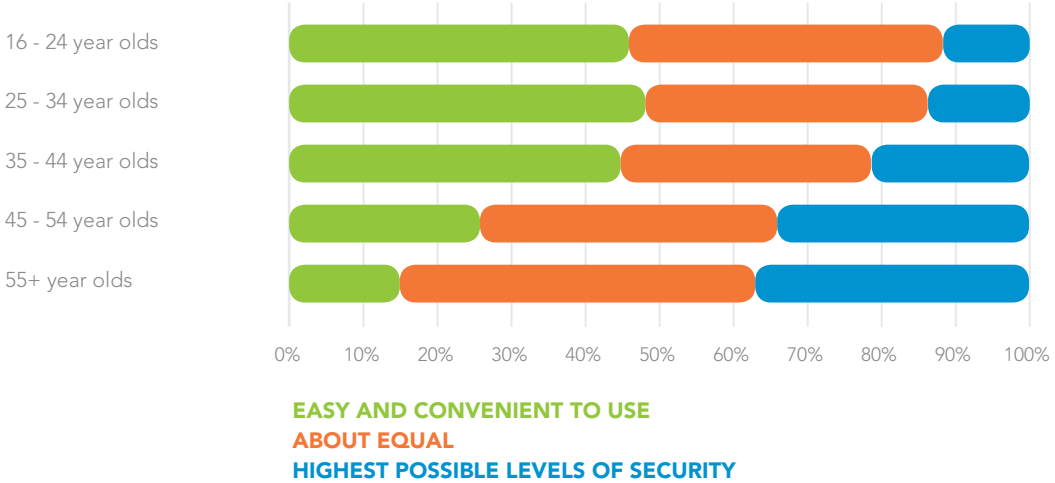
The most 'disgruntled' age group was 25 to 34 years old, with 10% claiming dissatisfaction of some level

How confident are you that your provider is implementing the necessary levels of security on your online/mobile banking account?

When asked about their levels of confidence around the security applied to their bank, building society or credit card accounts, the answers were split into general online banking (e.g. via a browser on a computer) and mobile banking.

The results show that consumers have a lower trust in mobile banking when compared to internet banking. 9 in 10 people in the total sample agreed that they were either confident or very confident that their provider was adequately protecting their online banking account (91%). When asked the same about mobile, just over 8 in 10 (84%) claimed confidence of any level.

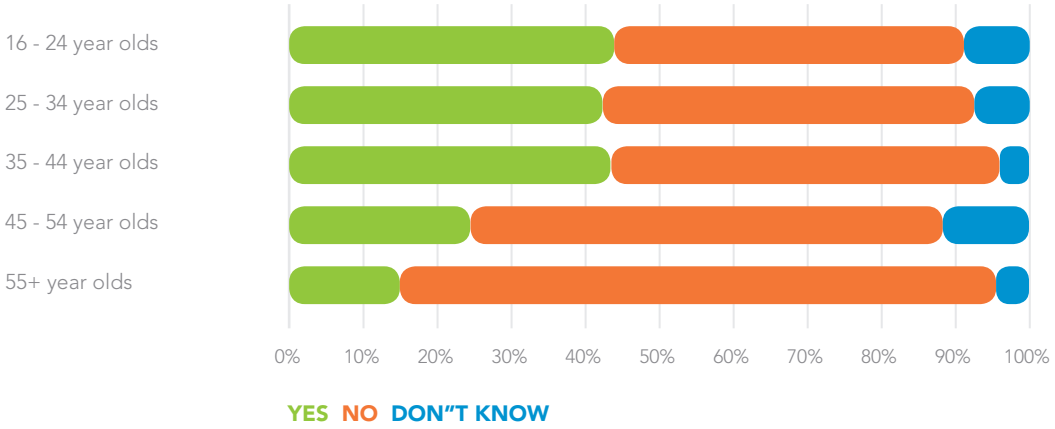
Would you rather mobile banking was easy and convenient to use, or had the highest possible levels of security?



On first glance, it is easy to analyse that the general sample errs on the side of convenience and ease of use when asked about how they'd prefer mobile banking, rather than favouring security measures. Most people only marginally want convenience over a balance (41% versus 39%), with only 20% choosing the highest possible levels of security.

However, the deviation around age groups becomes clear quickly. The younger demographic favour ease of use more than security, whereas the older demographic would prefer more focus on security by their providers. Just 11% of those aged 16 to 24 said they'd want the highest possible levels of security, compared with 38% of those over 55 years of age. Conversely, 48% of those aged 25 to 34 want an easy mobile banking experience, compared with only 15% of those aged 55 or over, who instead favour a balance (48%).

Do you feel restricted by your bank or credit card provider by procedures that are in place to protect you from being exposed to fraud?



The message becomes even clearer that the younger demographic prefer a friction free customer experience when managing their money, as 43% of those aged between 16 and 24, as well as those aged between 25 and 34 (42%) and 35 to 44 (43%), say they feel restricted by their provider, compared with 24% of 45 to 55 year olds and 15% of those aged over 55. This could be explained with the higher proportion of mobile banking app usage among the younger age groups, as well as the experiences of banking growing up. Those over 55 are more likely to have started their banking experience in branches, where historically the main method of authentication was personal familiarity of the tellers with customers. Since the number of channels were low compared to today, fraud was also restricted by how it could occur.

16 and 24, 25 and 34 and 35 to 44 year olds, say they feel restricted by their provider and prefer a friction free customer experience

Logging on and paying out – a frictionless experience?

When the sample was asked about the actual process of authenticating their identity for online and mobile banking, the overwhelmingly the most commonly used method was username and password – no matter the channel nor the level of complexity of transaction.

Digging deeper: the sample was split between two types of banking – online (via a browser or computer) and mobile (via an app). This was split further into three by type of transaction – logging in, a simple transaction (like paying an existing payee) and a complex transaction (like paying someone new).

What different types of authentication do you recall needing to do to perform transactions via your ONLINE banking?

ONLINE AUTHENTICATION	Online banking Logging in	Online banking Simple transaction	Online banking Complex transaction
Password	57%	47%	41%
Username	60%	37%	36%
Email address	35%	21%	21%
Partial password	19%	15%	10%
Unique/account number from bank upon registering for online/mobile banking	25%	15%	15%
Your card PIN	13%	10%	9%
Postal address (or partial)	15%	9%	10%
A different PIN	13%	8%	11%
I don't recall needing authentication to perform this transaction	—	7%	7%
A card linked to the account	7%	6%	6%
Partial unique/account number	10%	6%	7%
A one-off (timed) SMS code	5%	6%	9%
A hard token	5%	5%	7%
A voice call to a human	3%	4%	3%
Fingerprint recognition (e.g. Apple iPhone Touch ID)	4%	4%	3%
A voice call to an automated line	5%	3%	6%
Other	3%	2%	4%
Facial recognition	1%	1%	2%
Iris scan	1%	1%	2%

The most popular method for authentication is username and password

What different types of authentication do you recall needing to do to perform transactions via your MOBILE banking?

MOBILE AUTHENTICATION	Mobile banking Logging in	Mobile banking Simple transaction	Mobile banking Complex transaction
Password	47%	36%	38%
Username	45%	32%	33%
Email address	22%	17%	17%
Partial password	18%	10%	13%
Unique/account number from bank upon registering for online/mobile banking	17%	12%	14%
Your card PIN	10%	8%	9%
Postal address (or partial)	10%	10%	7%
A different PIN	12%	8%	10%
I don't recall needing authentication to perform this transaction	—	10%	9%
A card linked to the account	4%	4%	5%
Partial unique/account number	6%	7%	7%
A one-off (timed) SMS code	3%	4%	9%
A hard token	4%	5%	7%
A voice call to a human	4%	4%	3%
Fingerprint recognition (e.g. Apple iPhone Touch ID)	6%	6%	4%
A voice call to an automated line	4%	4%	6%
Other	2%	2%	3%
Facial recognition	1%	1%	2%
Iris scan	2%	3%	2%

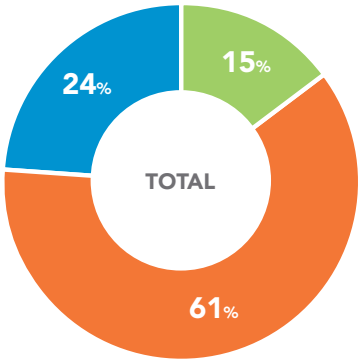
There is still a long way to go in provider adoption of methods such as voice biometrics or iris scans

The table here tells us that despite the likelihood that a number of different types of authentication are used in these transactions, the majority still rely on a username and password or a combination of password characters, PINs and numbers. For logging into online banking, 88% of customers identified some form of code that needed to be memorised (including username and password). Even down to performing a complex transaction via a browser, 75% say they require a character combination to authenticate alongside any other method.

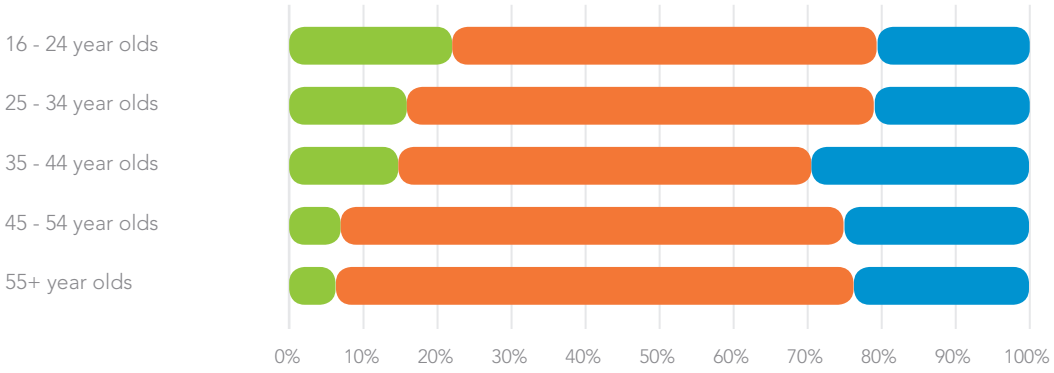
For mobile banking, the story is similar, as are the figures. Logging in requires a character combination 85% of the time. A complex transaction needs letters and numbers to be memorised 75% of the time.

Thinking of more advanced technologies, there is still a long way to go in provider adoption of methods such as voice biometrics or iris scans. For example, focusing on mobile banking as the newer channel, 6% of people claim to need to use fingerprint recognition to log in, or perform a simple transaction. 4% need it for a complex transaction, which is more likely to request the use of an SMS code (9%) instead of more letters and numbers-based verification.

In order to maintain higher levels of security against fraudulent activity and protect customers, some companies are able to use publically available data to protect individuals against fraud, without passing sensitive data on. How much do you approve of such developments?



DON'T APPROVE AT ALL
SOMEWHAT APPROVE
DEFINITELY APPROVE



Given the emerging trends from the research, the responses to leveraging publically available data to perform newer, easier to use authentication with less friction, were largely positive.

84% of respondents in the survey said that they approve or somewhat approve of the use of data.

Leveraging publically available data to perform newer, easier to use authentication, were largely positive

Conclusions

1. Fraud follows channels of adoption

While this report is not able to prove where the fraud occurred, and part of this reason is because so much fraud goes unreported (by the banks and the individual, as well as from businesses), what it can do is reinforce the message that fraud follows the channels of adoption. The advent of mobile banking has given way to grow the risk of fraud as well as other new types such as SIM Swap and mobile takeover.

2. Banks should be more proactive and leverage automation

Disregarding whether they subsequently received any notification from the bank, 28% of respondents had to notify their provider which either shows that people are more likely to be keeping an eye on their finances and transactions (thanks to mobile banking) or that a quarter of providers are not being proactive or quick enough to keep customers notified of issues. Ideally, customers should be told that a company is dealing with an issue, even before they were aware of it. This general rule applies also to customer engagement as a whole across many industries – banks, building societies and credit card providers must work towards reducing the effort on the customer's part. Whether this is through proactive notifications or effective self-service tools (such as chatbots that use natural language understanding), the customer must feel it is effortless to do business with an organisation, even if there are many background checks and automated processes going on behind the scenes.

People are more likely to be keeping an eye on their finances as providers are not proactive enough

However, it is important to note that perception is everything – the customer must also feel protected, so a certain level of 'showing the customer' what processes are for their security could also remain important.

3. Customers need to feel less restricted by their financial provider – especially younger generations

At the first sight of fraudulent activity, the card is largely blocked (63%). This has a high nuisance value and shows a lack of flexibility – even if this is only performed once the customer has, for example, confirmed that suspicious transactions are not theirs. With 9% saying that they had no access to money whatsoever, and some banks taking up to a week to refund any fraudulently obtained monies (with over half not refunding for two days), where does this leave the customer? If they have low income, are a student or particularly vulnerable, they could be placed at risk in other ways.

The younger age brackets overwhelmingly favour ease of use over security, and also, feel more restricted by their banks. Two in five of those aged 16 to 24 years old say they feel restricted. Those under 44 in the sample are also the biggest users of mobile banking with 44% preferring to use mobile banking apps over any other method of managing their money, including browser-based/internet banking.

The study also highlighted that the younger you are, the less likely you are to be satisfied with the way the provider handed the fraud case. 50% of 16-24 year olds claimed to be "extremely satisfied" compared to 75% of over 55s. It's no myth that Millennials have increasingly higher expectations from the organisations they buy from and engage with – they want it personalised, mobile and they want it quick.

Ultimately, proactivity rears its head again here, as well as a need for flexibility and alignment with our digital lives. Reduce friction, reduce effort and reduce lag to boost loyalty and satisfaction.

4. Banks will be challenged with finding a balance between easy use and increased security

The age-old reliance on passwords, usernames or a combination of characters from partial codes that need to be memorised by the user are not reliable, not frictionless, and heavily vulnerable unless backed up with a number of other methods (multi-factor authentication). That 88% of the sample claimed they needed characters to log into internet banking and 85% for mobile banking is not a bad thing, but it is crucial that banks look at more advanced methods of verification to secure the customers further and reduce the risk of financial crime.

Banks need a long-term solution to increasing security without adding more friction. When a bank discovers a mobile fraud attempt it may prevent a repeat attack, and repair the damage, but would not always share information about the incident with the wider financial community so that it, too, can prepare for and deal with similar incidents. They must also work harder to ensure they are certain of the transacting party's identity. With mobile banking, this is easily achieved by the use of mobile data, behavioural data and so on. The natural course of progression is for the industry to become more collaborative and harvest the information available to them in order to build a strong defence against the fraudsters.

On the consumer side, they expect an adequate level of security and identity authentication that doesn't disrupt their fast-paced, mobile lifestyles. Too much security causes friction and affects the customer experience; too little opens the door to fraudsters.

The natural course of progression is for the industry to come together and harvest information in order to build a battlefront

SIM Swap detection, for example, can be run imperceptibly to the customer, and offers an extra layer of identity authentication for complex transactions. Divert and location detection tools are also useful for better protecting customers against fraud, by recognising when SMS messages are being diverted from the intended SIM card and alerting customers through alternate channels. Layering verification in this way offers the best protection to date against fraud. However, no method is future proof and foolproof; hackers are getting more and more aware of how to bypass outdated security measures. The willingness of financial services providers to work closely with their security and authentication partners can help to keep them and their customers safe as new threats emerge.

5. The disparity between "online" and "mobile" will decrease, and confidence in financial providers will grow

The research raises an interesting point around the confidence and trust that consumers have in their financial providers. It shows that consumers are less confident in their banks, building societies and credit card providers' ability to protect them when it comes to mobile banking across all age groups, but yet the adoption levels are soaring. The convergence of mobile, desktop and cloud – digital transformation – will be key in levelling out the consistency of service and facilitating effective and new ways of authentication.

About Aspect

Aspect Software helps to deliver remarkable customer experiences across every conversation and every channel in the financial services industry. Aspect's technology portfolio features a host of products designed to support all types of customer engagement processes in financial services – from omni-channel self-service to identity verification. Aspect's wealth of financial services expertise means it provides customer engagement solutions to many of the leading financial organisations, globally.

Aspect's products, Aspect Via for complete customer engagement in the cloud, Aspect CXP Pro for multi-channel self-service deployment, and Aspect Workforce and Back Office Optimisation suites, seamlessly orchestrate people, processes and touch points for today's financial services organisations. Aspect Verify provides frictionless digital identity verification for seamless online and mobile banking experiences.

www.aspect.com/uk/verify

aspect™

Corporate Headquarters East

300 Apollo Drive
Chelmsford, MA 01824
+(1) 978 250 7900 office
+(1) 978 244 7410 fax

Corporate Headquarters West

2325 E. Camelback Road,
Suite 700
Phoenix, AZ 85016
+(1) 602 282 1500 office
+(1) 602 956 2294 fax

Europe & Africa Headquarters

2 The Square, Stockley Park
Uxbridge, Middlesex UB11 1AD
+(44) 20 8018 8000 office
+(44) 20 8561 4476 fax

Asia Pacific & Middle East Headquarters

8 Cross Street
#25-01/02 PwC Building,
Singapore 048424
+(65) 6590 0388 office
+(65) 6324 1003 fax