Strictly Financial Limited a: 315 Highgate Studios, 53-79 Highgate Road, London NW5 1TL
t: +44 (0) 77100 43990 or +44 (0) 77923 62524 Company Registration No: 5942438 VAT Registration No: 862 742 019 www.strictlyfinancial.com

TEN-14-148
Research into experiences of customers who are victims of unauthorised transactions in pursuing their claims with payment providers

Research Report from Strictly Financial

Prepared for:	Financial Conduct Authority
Prepared by:	Claire Labrum/ Dave Skelsey
Job number:	14-0727
Date:	9th December 2014

Contents

Table of figures

1. GLOSSARY, ABBREVIATIONS AND DEFINITIONS

ATM: Automated Teller Machine

Chip and PIN: Card using an encrypted chip and user-changeable personal identification number for verification, rather than a user signature

Cloning: Making a counterfeit copy of a real card using stolen data (often stolen by skimming)

Continuous payment authority/ Future dated payment/ FDP: A type of regular automatic payment that is set up using a debit or credit card. Both the timing and the amount of the payment can be varied by the payee

ONS: Office for National Statistics

Phishing: Sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to trick the user into surrendering private information such as account security details, often through a bogus website set up for this purpose

PIN: Personal identification number

Potential victim of unauthorised transactions: someone whose account has had money taken from it without the account holder's knowledge or conscious authorisation

PSRs: Payment Service Regulations

Skimming: Using a counterfeit card reader to steal the security information on a credit or debit card

T&Cs: Terms & Conditions

Vishing: a scam that involves a fraudster using social engineering techniques over the telephone to fraudulently obtain personal and financial information. This information is then used to carry out unauthorised transactions, or to dupe customers into authorising transactions themselves, in which case the transaction may not technically be unauthorised.

Unauthorised transaction: a payment made from a customer's account without their consent. This can include:

- card transactions, including online and in retailers
- account transfers
- ATM cash withdrawals

- Continuous Payment Authorities (these are regular payments from a customer's account, which become unauthorised transactions if they continue to be taken after the point that the customer requests cancellation)

Unauthorised transactions can occur for numerous reasons. These include:

- fraud against customers
- duplicate payments (for example, a card payment that has been mistakenly debited from a customer's account twice)
- failure to act on customer's instructions
- theft of a debit or credit card

2. EXECUTIVE SUMMARY

Research approach

Qualitative research was carried out with consumers holding current, savings and credit card accounts, covering a range of locations, ages and providers. Separate group discussions were conducted with people who had and had not experienced an unauthorised transaction on their accounts. Telephone and personal depth interviews were conducted with consumers who had had an unauthorised transaction experience on one of their accounts.

In addition, as the by-product of a structured screening exercise designed to generate a sample for the qualitative depth interviews, a limited amount of quantitative data was also gathered. This quantitative data came from a nationally representative sample of 948 online interviews and a boosted (not nationally representative) sample of 231 people who were identified from their answers as potential victims of unauthorised transactions.

Summary of main findings

1. There was a tendency among consumers to make assumptions about what their basic rights are regarding their protection against unauthorised transactions on their account.
2. The common view was that they are entitled to their money back from their provider as long as the unauthorised transaction is not their fault.

3. The consumers researched had no real knowledge or understanding of the detail of their rights or obligations beyond the basic assumption that they would be given a refund for an unauthorised transaction, and that they for their part had a responsibility to keep their account details secure. It was widely admitted that they did not read the detailed terms and conditions of their accounts, which they thought might contain this information, although they also admitted that they knew they ought to.
4. A number of participants in the group discussion freely admitted that they did not keep their account security details as secure as they could in that they shared PINs and, to a lesser extent, passwords with family and sometimes with friends and colleagues. Passwords tended to be more closely guarded than PINs. There was a view that it is unreasonable to expect people not to share their account details with loved ones.
5. Some also wrote down PINs and passwords, often in their diaries/ notebooks or mobile phones in disguised form. They did this as a form of back-up, for fear of forgetting them, and this resulted from having too many to remember: most saw 3-4 PINs and passwords as the most they could remember, and if they had more than that they thought they would need to write them down in some form. For the same reason it was fairly common for participants to duplicate PINs and passwords (or variations of them) across both financial and non-financial accounts.
6. The consumer reaction to discovering an unauthorised transaction on their account was typically one of shock and a sense of invasion. It felt very personal, and they wanted this to be reflected in the way their provider treated them over their claim. In most cases the consumer relied heavily on the provider to provide instruction and information (including about whether to involve the police), or to take charge of the whole process.
7. In the event of a claim, the research participants expected to have to justify their claim to the provider, and saw this as reasonable for the protection of both the provider and its customers generally, so as to exclude bogus claims. It was also seen as both likely and desirable that the provider would take the customer's account history and previous behaviour into consideration when assessing the veracity of the claim.

8. The customer journeys of those making a claim for an unauthorised transaction varied from instant satisfaction to drawn out, frustrating experiences. Looking across the different customer journeys, a number of themes emerged. The perceived treatment at the hands of the provider played a greater part in the participants' consequent view of their provider than the outcome of the claim. Although not being given a refund in circumstances where participants felt they were entitled to one was clearly a source of both disappointment and frustration.
9. A good experience was characterised by the provider immediately adopting – and then maintaining – a supportive stance. This took various forms, but the key elements included expressing sympathy from the outset and providing immediate reassurance about the security of the account and/ or that the money would be refunded. Knowing the timescale for the refund emerged as less important than having the reassurance that it would happen.
10. The need for sympathy extended to how the provider asked the customer about the circumstances and details of the transaction(s) in question. A good experience included the provider's representatives asking questions in a gentle and sympathetic way and giving the impression that they could and would try to help. If, for whatever reason, they were unable to refund the money, expressing sympathy and solidarity (at least in principle) with the customer and their plight could go a considerable way towards helping them feel that they were being treated fairly by their provider. This included the way in which the reason for not giving a refund was communicated. In sum, throughout the claim process and whatever the outcome, customers wanted to feel that the providers were on their side.
11. In contrast a bad experience was often characterised by a perceived lack of sympathy from the provider. Customers were especially sensitive to this at the outset (reporting the transaction or discussing it with the provider for the first time), and this first contact experience tended to set the tone for the rest of the customer journey. If the claim experience started with a perceived lack of support, the customers tended to retain this view of the provider, even if they subsequently received a refund.

12. The customer's history with the provider and the account was an important element in forming expectations of a sympathetic response from the provider. Claimants were disappointed and sometimes indignant if their loyal and 'responsible' history with the provider did not seem to be taken into account in the provider's response to the claim.
13. Lack of communication from the provider during the course of a claim was a cause of frustration, even where the outcome was a refund. Claimants wanted to be kept up to date with the progress of the provider's investigation and were irritated if they felt they had to chase the provider for information and updates.
14. The longer the process took, the more sensitive customers were likely to become over this issue. This frustration could be exacerbated if claimants felt their claim was being passed around between different departments, as this was perceived as impersonal. However, being passed initially to a specialist (e.g. fraud) department, which then retained ownership of the process until the outcome, was seen as positive (subject to that department's behaviour).
15. Related to frustrations over what was felt to be insufficient communication were the frustrations associated with expectations being set by the provider, e.g. over how long the process would take or when the refund could be expected, and then not met. These were occasionally as a result of administrative errors by the provider, and such errors were frustrating in themselves, as well as for the delay they caused. The combination of unmet expectations and poor communication was seen as especially irritating.
16. Participants were frustrated by being left to deal with the recipient of the money directly themselves, rather than receiving the expected and desired support from their provider.
17. While most of the victims of unauthorised transactions interviewed were focused on preventing further loss and gaining a refund, a few were frustrated at not being told how the money was taken. This applied most to participants who saw themselves as careful with their account security, who were at a loss to understand how the money had been taken from their account. They were left feeling exposed and wondering if there was more they could do to protect themselves.

18. The unauthorised transaction victims interviewed typically modified their attitudes and behaviours as a result of the experience. In particular they became more careful about their use of ATMs or internet shopping, and more likely to pay close attention to their account balance and statements. However, their heightened concern with security tended to relate closely to how the money was taken, and was not always applied more widely to account security, so their increased caution would not necessarily protect them from a different form of attack on their account.

3. INTRODUCTION

The FCA has carried out work to discover whether consumers are being treated fairly in relation to unauthorised transactions.

94% of the adult population has a credit or debit card and, according to the Office for National Statistics (ONS)[1], over £2m people are victims of card fraud each year. Following the introduction of Chip and PIN card fraud incidence fell, but over recent years has begun to increase once more. Irrespective of the actual figures, it is clear that a large number of individuals are affected.

The FCA were specifically keen to understand the following:

- If customers are denied refunds solely on the basis that the card Chip and PIN were used in the transaction under dispute
- Whether customers face unfair burdens of proof when making a claim
- If customers face unfair burdens of responsibility in keeping their security details safe
- If claims are incorrectly categorised as merchant disputes, not unauthorised transactions

The FCA is reviewing this issue to determine whether the legal protections in place are working effectively and if necessary, minimise any detriment to consumers claiming for unauthorised transactions. It is also important to understand more about what journey consumers go through when making a claim in order to identify good and poor consumer experiences and firm practices.

It is challenging to measure the level of customer detriment accurately. Industry based figures suggest that the detriment is low, as the majority of claimants are given a full refund. However, figures derived from the Office for National Statistics (ONS) Crime Survey suggest the overall loss to consumers could be much higher than industry figures would indicate. This blurred picture of the true level of consumer detriment resulting from unauthorised transactions has led the FCA to seek a clearer perspective on the true scale of the problem.

[1] Office for National Statistics, Crime in England and Wales, Year Ending December 2014: http://www.ons.gov.uk/ons/dcp171778_401896.pdf

4. CONSUMER CONTEXT AND JOURNEY

4.1 Consumer context

This section covers how the participants perceived their rights in respect of unauthorised transactions on their account, and their obligations with regard to keeping account details secure. They were also asked about what would happen in the event of an unauthorised transaction on their account. Again the focus of discussion about what would happen was on assumed rights and obligations, but the discussion also covered what they would actually do and what they would expect providers to do.

Separate group discussions were convened with consumers who had never experienced an unauthorised transaction on their account, and with consumers who had had this experience in the last five years. The focus was on exploring their understanding of where they stood with regard to rights and obligations in the context of account security and unauthorised transactions on their accounts. This included what they thought they could expect from providers and what providers could expect from them. By running separate groups of those with and without experience of an unauthorised transaction on their account, we could explore how the experience changed people's understanding, perceptions and behaviours.

Consumers were asked in the groups about what they thought to be their rights in the event of an unauthorised transaction on their account. They were also asked what obligations they thought they were under with regard to managing the security of their accounts.

Most of the findings covering the consumer context are drawn from the group discussions. However, the depth interview participants (all of whom had experienced an unauthorised transaction) were also asked how their experience had compared with their assumptions and expectations and in some cases what they would have liked to see from their providers instead of what actually happened. Their responses are also reflected in the findings of this section.

4.1.1 Awareness and understanding of their own rights

The consumers in the groups thought that they had a degree of protection in the event of unauthorised transactions on their accounts, but they were vague as to how

much or what form it took. Most thought they were protected by law or through some aspect of banking regulation, but did not claim to know much more detail than that.

"It is my problem if money has been stolen from my account, but surely there is some kind of law that protects you" (London, younger, no experience of an unauthorised transaction)

The comment quoted above illustrates how their expectation of some form of protection also accorded with their sense of natural justice, in that they thought it would be unfair not to get their money back in the event of an unauthorised transaction for which they did not feel responsible.

The widespread view was that the provider *would* return the money to them if they could prove that they did not authorise the transaction. However, they were unsure as to how much, and what kind of, proof would be required. In this context several of the participants who had been victims of unauthorised transactions had been surprised at the response of their provider when they had contacted them. Some had not been required to provide proof, and had simply had their word accepted. Others had been dismayed that their version of events had not been taken at face value. Both types of provider response had been contrary to expectation.

There also seemed to be some confusion between the protection offered against unauthorised transactions and that offered against the non-delivery of products or services. Several participants suggested that they might have better protection on their credit cards than debit cards. This view seemed to stem from a sense that consumer protection is generally better on credit cards, and therefore by extension this might also apply to protection against unauthorised transactions. Card use itself was influenced by different forms of perceived protection: debit cards were used so that goods and services were fully paid for when purchased, and thus the consumer was protected from the credit trap; and credit cards were used because they were seen as offering stronger buyer protection.

Another reason given for thinking that credit cards offer better protection against unauthorised transactions than debit cards was that the money being taken is not coming directly out of the customer's account, rather it is the provider's money: from the perspective of participants taking this view, the money has not gone until it

is paid to the card provider and so is effectively 'their' rather than 'my' problem. In contrast money taken from your current account does not have this 'buffer'.

Some participants extrapolated this thinking into the likelihood that providers would have more efficient and advanced systems in place to protect their own money than that of customers, and for them this also made it likely that the protection afforded to credit card accounts was better than that of current accounts.

"As far as I know, if you can prove that it's not you, you get it back. I think credit cards carry more strength than debit cards, don't they? They do protect it more, whereas a debit card isn't as protected as a credit card payment, I think"
(Manchester, older, no experience of an unauthorised transaction)

Among those with no experience to draw on, mixed views emerged as to how providers might actually respond in the event of a customer suffering an unauthorised transaction on their account. At one end of the scale was the expectation that the provider would reassure the customer and try to help them, and this was the majority view. The opposite view was held by the minority: that the provider would try to find a way not to repay the money, and might do so by attempting to blame the customer for what had happened.

There was also a fairly widespread view that the degree of sympathy, reassurance and help that would be offered to the customer would probably depend on the circumstances of the authorised transaction. For example, most expected less sympathy and help if they were known to have given away their security details. On the other hand, some thought that more support would be offered if the loss involved larger sums of money or a greater proportion of the customer's total wealth.

It was thought that the customer relationship itself could also be an influence on how the provider might respond. A long-standing and loyal customer might receive better treatment, especially if their past customer behaviour had been beyond reproach.

"I think they will be more sympathetic to someone they'd perhaps value as a more important customer, so I think they might be more sympathetic to a gold card holder than to someone with less money. But I think they would also be more sympathetic to someone to whom the loss is a large amount of their money, regardless of how much money that was" (London, younger, no experience of an unauthorised transaction)

In expressing these views, the participants seemed to be drawing on a combination of direct and second-hand experience (e.g. of a friend), and what were perceived as relevant parallels from other financial services, notably general insurance. The specific parallel given with general insurance related to claims, e.g. for theft, where it was felt that insurers would sometimes try to sidestep their obligation to pay the claim by suggesting the fault lay with the claimant (e.g. for some security lapse). These negative expectations of provider behaviour were also influenced by generally low opinions of the financial services industry as a whole.

Most participants assumed that the provider would want to investigate the claim before refunding money, and this again may have been a view influenced by knowledge and perceptions of general insurance claims. This was seen as perfectly reasonable – providers have a duty to ensure any claims are genuine, and protect other customers from the minority that might make spurious claims.

"I think they'd give you a timescale and say that it's a matter of how many days and we'll look into it and we'll keep in touch" (Manchester, older, no experience of an unauthorised transaction)

Those with experience of an unauthorised transaction drew on this in describing their expectations and assumptions about what would happen following such an event. As a result, some expected that their provider would be supportive and refund the money (and do so quickly), while others thought they might have to justify their claim. There was a tendency to assume that their own experience was in some way typical of how providers respond, unless they had other experience (e.g. that of

friends) to the contrary. These assumptions included how long it would take for the money to be refunded.

It is worth noting that those who had had an experience did not display any greater real knowledge of their rights or obligations regarding unauthorised transactions than those without, and this was especially notable in the context of timing of the refund. Their experience had influenced their expectations, but not necessarily made them better informed in an absolute sense.

4.1.2 Consumer perceptions of their own obligations and responsibilities: Keeping details secure

There was universal awareness in the groups that you are not supposed to share your PIN or password with anyone. However, in practice there seemed to be some distinctions drawn between PINs and passwords in terms of how careful people were about not sharing them.

Many of the group participants openly admitted to sharing their PINs, especially with close family (most commonly husband, wife or partner, but also parents, children and sometimes siblings). This applied to both those who had, and those who had not, had experience of an unauthorised transaction on their account. Among the younger participants it also seemed fairly common to share PINs with friends or even work colleagues. The most common examples of this were giving someone both the card and the PIN to buy a round in the pub or to withdraw cash from an ATM. Though this practice was less common among older respondents, it was not without exception:

"I know I shouldn't have done it ethically, but because he's your best friend. It's like we all know we shouldn't share it with family and friends, ethically you shouldn't, but you do it because you trust them" (Manchester, older, no experience of an unauthorised transaction)

This finding was substantiated in the structured screening exercise undertaken. Here a substantial minority of potential victims admitted to sharing secure banking details, mainly with a family member or close friend.

Passwords were shared less widely than PINs, and among the younger participants less casually. They were less likely to be shared at all, and if they were it was usually limited to the person's husband, wife or partner. However, passwords were often shared between accounts, so that a number of different accounts held with different providers might all have the same password. This was especially common among non-financial accounts. For some, passwords were shared across financial accounts, and sometimes across both non-financial and financial accounts.

However, if any accounts had unique passwords that were not shared with other accounts, these were likely to be financial accounts. Sometimes the passwords used were similar but not identical, e.g. variations on the same word or on the use of capitalisation in the word, or use of the same letters with different numbers.

PINs were also often shared across different cards. In these instances the PIN itself was seen as secure (e.g. changed from the one issued, memorised and not written down), and using the same one across different cards was easier to remember than which PIN applied to which card.

When challenged on sharing security details with close family or even friends, the participants defended this behaviour. They tended to see trusting these people with personal information as a matter of personal responsibility and judgement. This outweighed the 'duty' to the provider not to do so, and there was an element of indignation in some of their responses to the idea that the provider might seek to prevent them from sharing their security details with loved ones. This was particularly true among older respondents in long marriages: as one put it:

"If you can't trust your wife, who can you trust?" (Manchester, older, no experience of an unauthorised transaction)

More broadly they generally took the view that it should be the customer's decision whom to trust, not the provider's, and many saw nothing wrong in sharing their details with people they trusted.

Although they knew they were not supposed to do so, it was also common for participants to keep security details written down. There was a widespread view that

it is not possible to remember more than a few (most group participants said 3-4) sets of security details, so writing them down constituted a form of back-up.

These written details were often disguised, typically as somebody's contact details or as a key prompt phrase. This information was kept in diaries, notebooks and on mobile phones. Again this was not seen as doing anything wrong, and the justification given for this view was that the information was sufficiently well disguised or encoded that no one would be able to identify it for what it was.

"I find I've got to write it down, because I have a husband and son who are useless, and they rely on me to remember theirs. I've got three people's codes, and there's no way I can remember them all" (London, older, experience of an unauthorised transaction)

It is worth noting that among the very small number of people researched who both admitted to the provider that they had shared their details and were refused a full refund following an unauthorised transaction, only one was given sharing their details as a reason for the refusal.

Most group participants claimed to be responsible with their cards in banks, shops and online. Apart from the examples given above, mainly among younger respondents, most did not let anyone other than their spouse or partner use their card. Equally, most claimed to shield their PIN when entering it and to be aware of the environment in which they were doing so. In this regard they also respected the privacy of other people, e.g. by not standing too close to other shoppers paying by card, or to people using an ATM. Some claimed only to use their cards in shops or inside bank branches, rather than using external ATMs, where they felt more exposed.

Most claimed to be wary about giving out financial details online, and were careful about which sites they put their card details into. When shopping online they tended to use mainly retailers they saw as reputable, such as eBay, Amazon and the online stores of high-street retailers. Several also claimed to look for the security lock symbol on the web page where they were asked to enter their details.

However, the view also emerged that scam websites could be hard to distinguish from the real thing, and here there seemed to be some difference between generations. A couple of the older group participants said they had seen fake websites which had looked very convincing. In contrast the younger participants were more inclined to feel confident about which sites were safe and which were not. Some of them attributed this to their generation being more 'internet-savvy'. As a result they also tended to be more blasé about online shopping.

It should also be noted that several people thought they had had money taken by sites they had visited, where they were sure they had not input any of their card details. They were at a loss to understand exactly how or when these sites had obtained their details – the best explanation was that some form of Cookie had automatically captured their details.

4.1.3 Consumer perceptions of their own obligations and responsibilities: informing the provider in the event of an unauthorised transaction

In the event of discovering an unauthorised transaction on their account, participants thought they were under an obligation to report it to the provider as soon as possible. They saw this obligation as moral as much as contractual: it was about responsible and sensible behaviour. The primary concern was to prevent further transactions occurring, and so the best way of achieving this was by contacting the provider to put a 'stop' on the card/ account. Several assumed that a mechanism to reclaim money would be in place, and the more quickly they reported the transaction the more likely this was to be effective. There was also a sense that, if they delayed, the provider may be less helpful and supportive (although in many cases this was based on assumption rather than experience).

"I think you've *got to keep the timescale, haven't you? If you delay sending it back two weeks, then what they're saying they can do, they can't do, so it's got to be like that" (Manchester, older, no experience of an unauthorised transaction)*

They were less sure about whether or not they ought to call the police. Some thought they would need a crime number, and this could only be issued by the

police. Others thought the police could not possibly cope with being contacted by every victim of an unauthorised transaction, and therefore they did not need to be involved by the victim.

"It's a theft. Somebody's stolen something out of your bank account, so it's a crime, so I would presume that that would have to be reported to the police" (Manchester, older, no experience of an unauthorised transaction)

"Can you imagine if everybody who was having a problem with their credit card contacted the police?" (Manchester, older, no experience of an unauthorised transaction)

There was a suggestion that the need to involve the police might depend on the type of crime. For example, theft of money from an account might not require involving the police, whereas physical theft (e.g. of a card) might.

As the tenor of the comments quoted above suggests, beyond a clearly understood requirement to contact the provider and let them know about the unauthorised transaction, discussion about exactly what to do involved a fair amount of speculation. Many felt there was not much they could do beyond informing the provider. It was expected that the provider would then tell the customer what they needed to do, what the provider would do, and possibly what sort of timescales to expect.

The participants also thought that if they left it 'too long' before reporting an unauthorised transaction, it might count against them in obtaining a refund. However, they were unsure what delay might constitute 'too long'. Estimates and guesses ranged up to a year after the event had occurred, but the participants thought the period after noticing it was more important than the period after the event itself had occurred. For example, someone who looks at their account every day or every week online would have a greater responsibility to report the matter quickly than someone who receives account statements every three months.

"I think from the bank's point of view, they've got to have a timescale, because they've got to have some kind of leeway to try and chase that account up. If you came back after about six months, there's just no trace then really, is there?" (Manchester, older, no experience of an unauthorised transaction)

"I get a text from my bank every day, so I think my duty of care would be to get in touch with them as soon as I found out. If you get monthly statements I think it must be different" (London, older, experience of an unauthorised transaction)

In reporting the unauthorised transaction to a provider, there was an expectation that the customer would be required to identify which transactions were theirs, and which were not. It was also thought likely that some evidence might need to be provided to support the claim.

4.1.4 Consumer perceptions of providers' obligations and responsibilities

As mentioned above, it was widely assumed that providers are obliged to pay back money taken from customers' accounts without their authorisation. It was also thought that there was a chance that providers might try to find a way not to do so, e.g. by suggesting the fault lay with the customer.

In making this assertion, the participants were not taking into account the possibility of having given authorisation for the withdrawal without being aware of it. For them the concept of authorisation carried the sense of a conscious act: it was 'knowing authorisation', and this was how they would expect providers to interpret it as well.

This suspicion that providers might try and find a way not to refund the money applied particularly where password or PIN details had been shared. It was also seen as possible in cases where these details had been written down and kept, rather than destroyed. The provider might take the view that any sharing of details or keeping them written down was irresponsible behaviour, and might therefore not be obliged to refund the money. For this reason most participants said they would probably not admit to having done so in the event of an unauthorised transaction on their account, and the point was made that an unauthorised transaction could well be unrelated to the sharing of security details with family or friends.

For some, who did not share their details, such a position on the part of the provider was not seen as completely unreasonable.

"It's certainly foolish to do that, and if you owned up to the bank that you have done that I think at the very least they would tell you off, and I think they would have a case for saying you were liable" (London, older, experience of an unauthorised transaction)

However, others could see circumstances in which it would be necessary to share security details with other people, and this generated discussion about how financial security obligations should apply to the more vulnerable, especially the elderly and disabled, who might need to share their security details.

"I work as a support worker with people who have disabilities, sometimes severe disabilities. They have to write certain things down. Why should they be penalised for that?" (London, younger, no experience of an unauthorised transaction)

A consensus emerged across the groups that disabled and elderly people should be treated with leniency by providers in the event that their money was taken as a result of sharing their details. There was also the view that some people are more open to being conned than others, and this again included (but was not restricted to) the elderly. It was felt that these people should also be more protected from the strict interpretation of the 'rules' of security than the participants themselves (who did not see themselves as falling into this category).

With regard to providers' obligations in the event of an unauthorised transaction online, the general assumption was that most online fraud was the result of hacking rather than customers being careless with their security. Again the question of unwitting authorisation was not spontaneously considered. There were fewer perceived grey areas where customers might be at fault than in cases related

specifically to cards, and therefore participants thought the provider would simply be required to reimburse the customer for the money taken.

Participants were also unclear how long a refund should take: some thought it should be full and immediate, others that it might need to wait for the provider to make an investigation, or that it might vary depending on whether the money taken could be tracked or had disappeared. Equally there was speculation as to whether the norms (or even the rules) of procedure would vary depending on the amount of money involved.

"I think there's a duty of care for them to refund it, but they're going to have to look into it first" (Manchester, older, no experience of unauthorised transaction)

"I can't see it being one rule for £10 and one rule for £10,000. I can't see it, because it would become very complicated" (Manchester, older, no experience of unauthorised transaction)

The clear and widespread expectation was that it was the provider's role to tell the customer what would happen next when the customer reported the unauthorised transaction. For many this simply meant that they wanted to be reassured that the money would be refunded, and some were less concerned with knowing how long this would take than that it would happen.

The other widespread expectation was that the card in question would be cancelled and the account possibly frozen for a while, to prevent further withdrawals. The latter was seen as a temporary measure, but no real definition of its duration was forthcoming.

How long the provider would or 'should' take to refund the money was also open to question, and varied in people's estimation from 24 hours to several weeks. The delay was thought likely to vary depending on the circumstances of the unauthorised transaction, and possibly the amounts involved. Such variation was seen as reasonable – the provider is obligated to investigate any claim thoroughly to ensure it is bona fide and this will take time.

In discussion about what, if anything, providers should do beyond refunding the money taken, a few participants thought the customer should be compensated by the provider as well, for having failed in their 'duty of care' by allowing the money to be taken when they should have been looking after it. They should compensate the customer for not having had sufficiently robust protection in place. However, this was very much a minority view.

Other follow-through behaviours from the providers which participants wanted to see included written confirmation that the money had been returned and that the matter was now closed.

"They sent me out a new debit card straight away, but it took some time for the money to be credited to my account, and I felt that I had to do all the asking. And when the money came back into the account, they didn't tell me that either" (London, older, experience of an unauthorised transaction)

Some also wanted to be told what had happened and whether the criminals had been brought to justice. Those wanting to know what had happened were a minority, generally of people who had experienced an unauthorised transaction and had no idea of how it had been carried out. Part of their interest was curiosity, but there was also concern that there were (further) precautions they could take if they knew, to prevent it happening again.

"I thought that I would find out more about what had happened, because I just wanted to know. It was bugging me how they'd got my details" (London, older, experience of an unauthorised transaction)

Advice on precautions and general security tips were welcomed by most as useful reminders or new measures that they could take, though a few with experience said they had only been told to do things which they already did.

There was speculation as to how visible the money trail would be to the provider: would the banking 'system' enable them to see what had happened and where the money had gone? And if so, did that mean that they would be able to 'claw back' the money that had been taken? Several participants thought so.

4.1.5 Behavioural biases that may be affecting consumer behaviour

During the research we identified a number of behavioural biases that are potentially affecting consumer expectations and behaviour. This section is not meant to be an exhaustive discussion of behavioural economics theory[2], or indeed a complete list of all biases and heuristics operating in this market, but it simply makes some observations about which biases were most obvious during the course of the research.

We saw these biases amongst consumers with no experience of unauthorised transactions on their accounts (and how they talked about account security and, hypothetically, about unauthorised transactions), and also how potential victims recounted their experiences and the effect they had had.

Among people with no experience of unauthorised transactions, there was evidence in account security management of people defaulting to the path of least resistance: for example, using the same (or simple variations on the same) password across accounts, or using the same PIN across accounts. In doing so, consumers were trying to balance the practical need to remember security details for a number of different accounts with the cognitive challenge of doing so, and so finding a solution that seemed to offer both security and ease of management. This suggests that there is both a practical and emotional 'cognitive limit' – people can/ are only prepared to 'learn' a certain number and complexity of PINs. Once this limit (which may be different for different individuals) is reached, then 'short cuts' are used to help minimise the additional effort required. This effect is perhaps even more pronounced for passwords, which tend to be longer and inherently more complex.

Similarly, the assertion by several participants that the 'code' they had used to disguise their security details when they wrote them down (for fear of forgetting

[2] For a full discussion please refer to the FCA's Occasional Paper No 1, 'Applying behavioural economics at the Financial Conduct Authority', published in April 2013 - http://www.fca.org.uk/your-fca/documents/occasional-papers/occasional-paper-1

them) could not be broken by anyone else, was based on their own skills and limitations rather than a wider knowledge of how secure their efforts really were.

It was notable that some participants talked openly about their willingness to lie to a provider (e.g. about having shared account details with someone else), if they thought the truth would weaken their position when reporting/ claiming for an unauthorised transaction on their account. Their justification for this was that if sharing their account details had not been the cause of the unauthorised transaction, then it was irrelevant, and they were therefore morally justified in discounting (and hiding) it. This selective approach to disclosure did not have a negative impact on self-perceptions of honesty and morality.

The impact of hindsight bias was apparent through the way participants described selectively modifying their behaviours following an unauthorised transaction on their account. For example, they might take more care at an ATM (shielding a PIN or avoiding ATM machines located in less salubrious locations), because their PIN had been skimmed, but this might not prevent them from continuing to keep a written record of their PIN, because this had not been the way that their account security had been breached. This was a sign that the specifics of their experience had heightened the importance of certain behaviours or actions, possibly at the cost of other, wider, security considerations.

Hindsight also inclined people who had suffered an internet-based unauthorised transaction to be wary of internet shopping generally, but they were nonetheless prepared to make exceptions for well known, 'respectable' sites like Amazon, eBay or the online shops of leading high street retailers. This is because these retailers are seen as trusted, even on the internet, and even where the internet is seen as potentially unsafe. The brand reputation is overcoming any security reservations in these cases.

The effect of telescoping bias on people's recollections of unauthorised transactions is that the impact of the experience heightens the memory of what happened and makes it seem more recent than it actually was. Similarly, recency bias has increased their concerns about something similar happening again (compared to their original concerns about an unauthorised transaction happening in the first place), and also driven the behaviour changes which the victims described following

their experiences, in an effort to prevent a recurrence. This suggests an increased need for post event reassurance from providers to help individuals overcome the emotional impact of these events.

4.2 Consumer experience of unauthorised transactions

This section covers people's experiences when there was what they or their provider saw as an unauthorised transaction on their account. It includes output from the data generated as a by-product of the structured screening, as well as feedback from consumers as to how the discovery of the unauthorised transaction made them feel.

This section also goes into detail about the potential victims' experiences in dealing with their providers, highlighting both the positive and negative aspects of what happened, as well as how long it took. In some cases and, as appropriate, contrasts between expectations and the reality of people's experiences are drawn out.

One specific area covered in this section is that of communication and here again comparisons are drawn between expectations and what actually happened.

Finally, this section covers an outline framework of what consumers would (and in some cases already do) see as good practice on the part of the providers, as well as what kind of behaviours the providers should try to avoid.

This section draws closely on the output from the individual depth interviews, and also from the group discussions among people who had experienced an unauthorised transaction on their account, and from the data generated by the structured screening.

4.2.1 Areas the FCA were keen to understand in more detail

The FCA set out a number of areas it felt needed to be understood in more detail, in order to establish the extent of any consumer detriment in relation to unauthorised transaction claims. These were:

- Customers might be being denied refunds on the sole basis that Chip and PIN were used in the unauthorised transaction
- Customers may face unfair burdens of proof when making a claim
- Customers may face unfair burdens of responsibility in keeping security details safe

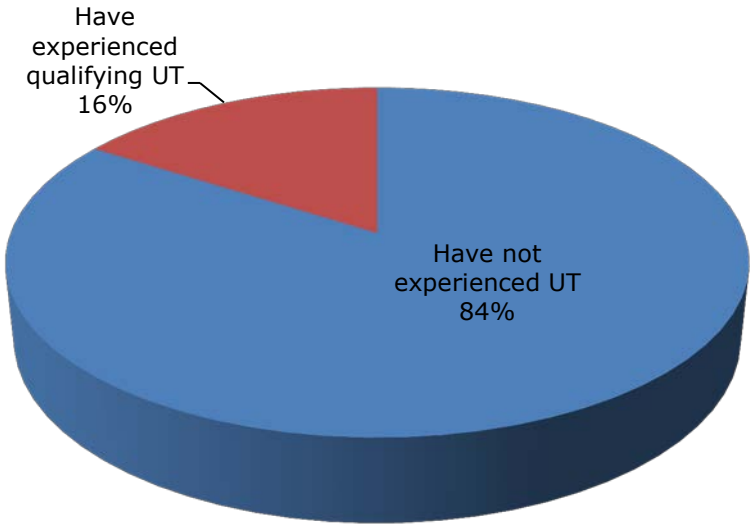
Some disputes might be being incorrectly categorised by providers as merchant disputes rather than unauthorised transactions. These areas are addressed individually in Section 4.2.16.

4.2.2 Incidence of unauthorised transactions

As part of the structured screening exercise to identify victims of unauthorised transactions to interview, we needed to set our own benchmark of incidence which the remainder of this research could tie into directly, rather than rely on existing third party findings and try to 'graft' this research onto pre-existing figures. Therefore a nationally representative sample of 948 consumers was asked if money had been taken from their account without their permission in the last 12 months.

The structured screening generated a sample of people who had recently been victims of unauthorised transactions (according to their answers to the screening questionnaire, all had had this experience within the last year). These people were followed up with 30-50 minute qualitative telephone interviews, to add further detail and specifics of individual customer journeys to the broad outline gleaned from the group discussions.

As Figure 3 below shows, 16% claimed to have had this experience, and relatively speaking younger people and those in higher social grades/ wealthier were more likely to have experienced an unauthorised transaction.



Q8 Have you had any money taken without your prior permission or knowledge from a bank, building society or credit card account in the last 12 months? Base 948: Claimed incidence amongst a nationally representative sample

Figure 3: Incidence of claimed unauthorised transactions in the last year

Among those research participants who said they had had an unauthorised transaction on their account in the last 12 months, closer examination of the circumstances revealed that a small group (34 individuals) did not appear to have had an experience where money had been taken without their authorisation. This assessment was based on their own description of the events that had taken place: some of them resulted from merchant errors (e.g. reading the wrong meter, inputting account details incorrectly or over-charging by mistake), or bank charges triggered by Direct Debits taking the account into overdraft. Others were simply too ambiguous to classify. For the purposes of this research, given that the objective of the structured screening was to identify case studies for the qualitative phase, these respondents were excluded from further analysis. However, it does imply that any figures are likely to be affected by a relatively small degree of 'consumer error' when claiming to have experienced an unauthorised transaction.

Where closer examination showed the potential for an unauthorised transaction claim, further analysis was conducted, and these participants were labelled as 'potential victims', and this is how they are referred to in this report.

For the vast majority of those experiencing an unauthorised transaction, this was their first such experience. However, a minority (around a fifth) seemed to be serial victims of unauthorised transactions.

One point of interest which emerged when these potential victims were followed up for individual interview was that, although all of them had stated in a questionnaire that the incident had occurred within the past 12 months, when we talked to them in depth it became clear that for some it had actually been longer ago: up to two years. It would seem that the emotional impact was such that it made the event loom large in people's memories and feel more recent than it really was. This is a well-documented phenomenon known as Telescoping Bias, or the Telescoping Effect, and in this context it seems to have resulted in a degree of over-claiming.

Another point which emerged regarding incidence was that we encountered people who had signed up for what they thought was a free product trial (often of health or beauty products), but in fact the small print authorised the vendor to take future payments. Equally, people who had used online brokers to find payday loans had sometimes found themselves being charged substantial amounts, even where they had not taken a payday loan. Again, the small print had authorised the broker to take these payments. In the view of the consumers we spoke to, these payments were unauthorised because they had not signed up to them willingly, or even knowingly.

It also became apparent that some fraudulent transactions were blocked by providers. It may be that consumers sometimes regard this unauthorised activity as an unauthorised transaction, even though no money has been taken (this happened in some of the interviews). Similarly, they may not always report what they see as an unauthorised transaction if they find their own solution to it. For example sorting out a merchant error by dealing directly with the merchant, finding that friends or family have withdrawn money from their account, or realising later that they themselves have made a mistake. Asked about unauthorised transactions in

research, consumers might include this sort of example, even where they have not had any interaction with their financial provider about it.

All of these points could be contributing factors to some of the apparent anomalies between different sources of information as to the incidence of unauthorised transactions.

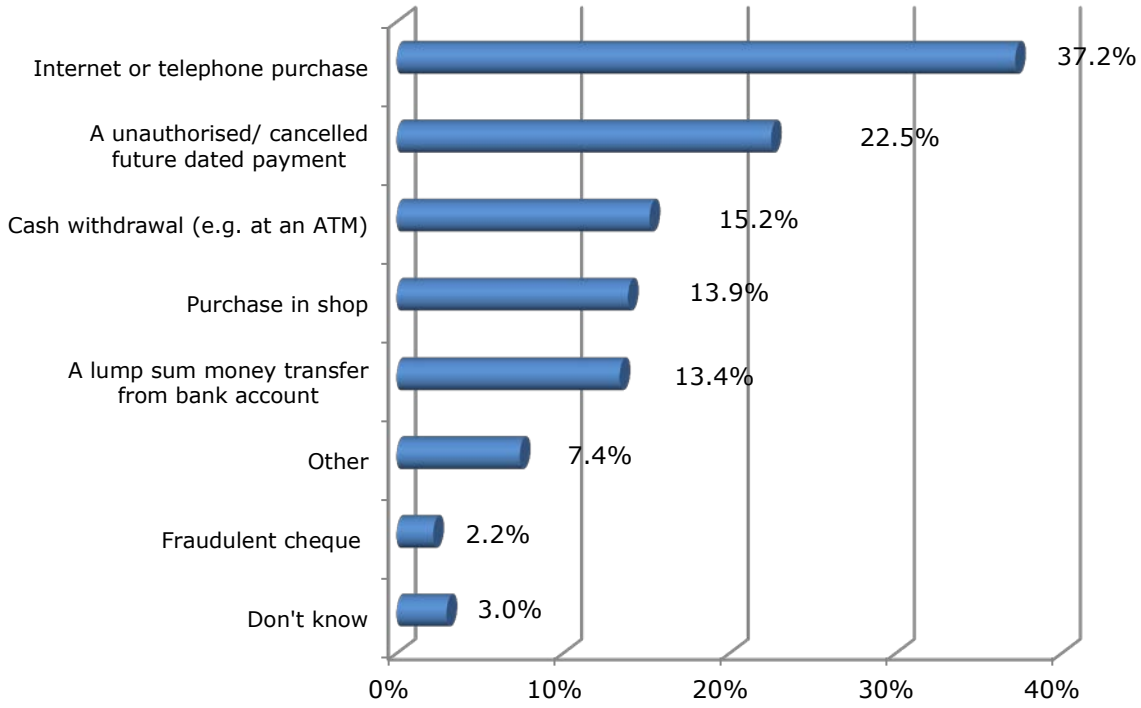
4.2.3 Type of account targeted and transaction value and type

Among the potential victims (i.e. those who had reported an unauthorised transaction), the most common type of account targeted for unauthorised transactions was their current account: 73% of those to whom an unauthorised transaction had happened said it had been on their current account. In comparison, credit card accounts made up 21% and savings accounts 4%. Prepaid cards and other accounts (mainly Paypal) made up 2%.

The unauthorised transactions on credit cards tended to be of higher value than those on current accounts, and the potential victims were more likely to be older. Current accounts tended to involve smaller amounts and were more likely to involve issues around future dated payments.

Just under a third of unauthorised transactions (31%) were for £50 or less, 32% were for £51-250, and the remainder (39%) were for over £250.

Figure 4 below shows the type of unauthorised transaction reported by consumers in this research.



Q16: What was the nature of the transaction? Base 231: all UTs

Figure 4: Nature of the unauthorised transaction (defined by the consumer)

Over 37% of the unauthorised transactions as defined by the potential victims were internet or telephone purchases, and another 28% were split between cash withdrawals and lump sum transfers from the consumer's bank account. Over a fifth were related to future dated payments, while nearly 14% involved purchases in shops.

Among those experiencing a cash withdrawal, shop, internet or telephone purchase, the great majority (85%) still had their card in their possession. Where the unauthorised transaction involved remote activity such as internet or telephone purchase or some sort of money transfer to another account, over half (55%) had had no previous relationship with the company or individual concerned. A third of those who had experienced a single or regular lump sum withdrawal from their account saw themselves as victims of a phishing or vishing scam.

4.2.4 Identifying the unauthorised transaction

Overall the vast majority (78%) of unauthorised transactions were noticed first by the account holder. Among these, it was typically within a day (69% of them) or within a month (27%) of the transaction.

Account holders were more likely to spot the transaction first with current accounts (82%) than credit cards (72%). Larger amounts (£250 or more) were more likely to be noticed by the provider, and the greater incidence of providers noticing unauthorised transactions on credit cards fits with the finding that such transactions on credit cards tended to be larger.

As well as being more effective in spotting larger unauthorised transactions, providers were more likely to detect them among the over-35s. This could be due to the difference in how older customers operate their accounts when compared with younger customers. In contrast, providers were least likely to notice unauthorised transactions among C2DEs, possibly because the transactions tended to be smaller and less easy to identify as an unauthorised transaction. Future dated payments were also difficult for providers to identify as unauthorised transactions, and only 10% were identified as such by the provider.

Looking more closely at provider-identified unauthorised transactions, providers noticed card present fraud in 28% of unauthorised transaction cases where the card was present, and in 22% where the card was not present.

4.2.5 Discovery of the unauthorised transaction

The unauthorised transaction came to the attention of the potential victims in a number of different ways. These included:

- They spotted it online during a routine check of their account
- A couple spotted it using a smartphone app for their current account
- They received a call from the provider (in a few cases this took the form of a synthesised outgoing message)
- They received a text from the provider
- They received a letter telling them they were overdrawn
- They saw a mini-statement from an ATM
- The ATM receipt did not match the amount of cash they had taken out

In some instances this coincided with another event, such as the loss of a card.

The first two examples above illustrate that the increased use of online banking by some consumers makes it possible for them quickly to spot unauthorised activity on their account. With regard to providers noticing unauthorised activity, consumer views as to the efficacy of the providers' systems were mixed. Several of the participants in the qualitative research expressed surprise (and in some cases admiration) that automated systems were able to detect a specific transaction as unauthorised. Others thought the systems should have been more effective than they were, detecting an unusual transaction and either blocking it automatically or sending an alert to the customer to inform them of the activity on their account.

4.2.6 Emotional response to the unauthorised transaction

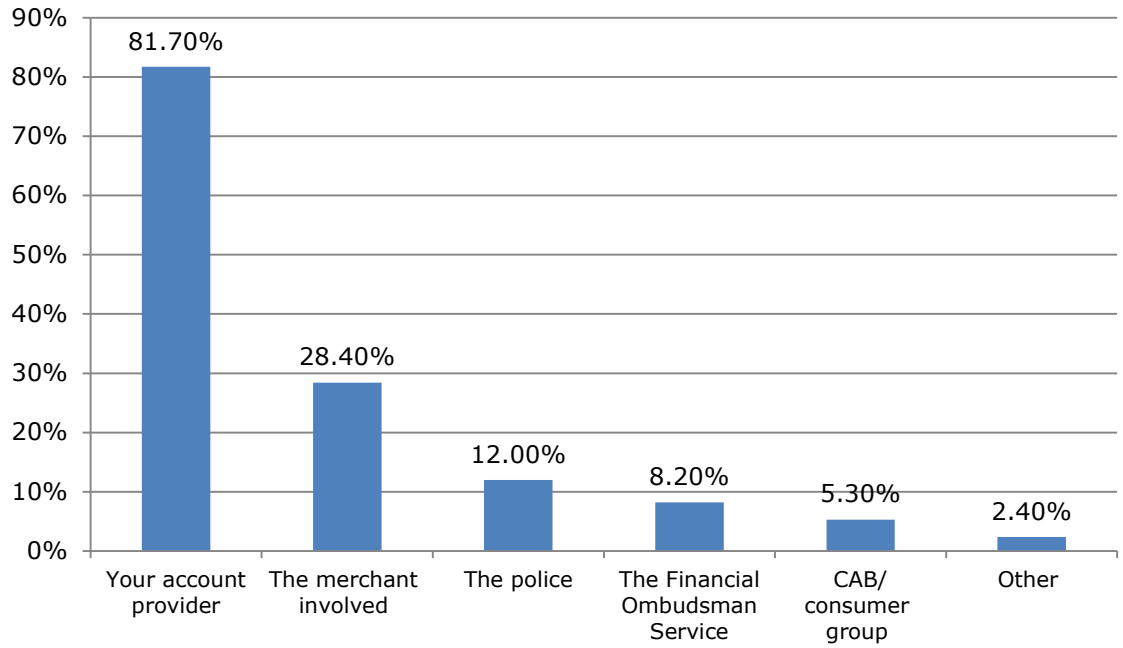
All the potential victims interviewed were upset by the unauthorised transaction, irrespective of how they came to find out about it and regardless of its value. They clearly recalled their feelings at the time in interviews, even though it was sometimes well over a year since the unauthorised transaction had happened.

The prevailing emotion described was a feeling of invasion or violation, akin to being burgled. This was coupled with concerns about getting the money back and basic questions related to this. Chief among these were: how much help and support would they receive from the provider? And would their version of events be believed? For some there was also the question about how they would cope financially in the short term, and this was a particular concern for those whose finances were tight.

For those who did not know how the money had been taken from their account, there was often an added unease: not knowing how it had been done left them feeling exposed and unprotected. This seemed to apply particularly to those who saw themselves as security conscious and careful about their security details, behaviour at ATMs and payment points, and who limited their online shopping activity to what they saw as respectable outlets and websites.

4.2.7 Interactions during the claim process

The provider was the main point of contact for the potential victims of an unauthorised transaction, with over 80% of those researched having been in touch with their account provider.



Q24: During the process, which of the following organisations did you have contact with? Base 208: All who either asked or were offered their money back

Figure 5: Interactions during the claims process

The next most popular point of contact was the merchant, followed by the police (12%), the Financial Ombudsman Service (8%) and Citizens' Advice or other consumer groups (5%).

It was clear from the interviews that potential victims' success in dealing directly with the merchant was mixed. In some cases they had been encouraged by their provider to talk to the merchant, but there were reports of frustration with this, leading to the provider being required to intervene with the merchant on their customer's behalf. Typical frustrations included the merchant being unobtainable, or being inflexible, unhelpful or dismissive of the customer's complaint, or otherwise generally unresponsive to the customer. This attitude seemed to change when the

provider took a hand, and potential victims reported more success on the part of their provider, which they attributed to the provider having more power and influence to bring to bear on the merchant than the individual customer can.

Reporting the unauthorised transaction to the provider was driven by the desire to prevent any further unauthorised activity on the account, and so this action was usually taken as quickly as possible. Other reasons given for contacting the provider included identifying the merchant involved (and thus double-checking if it was in fact an authorised payment), and trying to reclaim the money.

The most common form of contact with the provider among potential victims was by phone, as this was seen as the quickest and most practical way to get in contact. There may also have been a desire to speak to somebody at the provider, rather than simply log the event onto an automated system, and telephone contact offers that possibility. Some had also thought that a specialist department might need to be involved, and that it would be easy to be put through to them on a telephone call. However, some had gone into a bank branch to report the unauthorised transaction, and some had received a call from their provider alerting them to the unauthorised transaction (rather than making a call to the provider to tell them).

All the potential victims had been required to go through some security questions, as they had expected, and then they had dealt with customer services (or branch staff for those who had gone into a branch). At this point some were transferred to the provider's fraud department, while others continued to deal with customer services. Their experience in dealing with the fraud department was that the personnel were generally knowledgeable, clear and concise in what they had to say, while the experience with customer services staff was more variable.

In a couple of instances the potential victims were asked to wait until the money had left their account before reporting the transaction as unauthorised, and told that the bank could not take any action until the money had left the account. A few others were asked to approach the merchant directly, and were left feeling that the provider was being unsupportive and appeared uninterested in helping.

For the majority of potential victims the reporting process was a positive and reassuring one, and for some this was more the case than they had anticipated. This was especially true for the people who were given an immediate assurance that

they need not worry and that the money would be returned. In some cases they were also told when this would happen.

A few potential victims also reported that the person they were talking to had proactively searched the account history for other similar or related transactions, or had mentioned that the provider was aware of this particular merchant and associated problems. This contributed to the potential victims' sense of being supported by their provider, with the latter appearing to be actively working in the interests of the customer and trying to identify the scope (scale, time and value) of any wider unauthorised activity.

However, a minority of participants found the reporting process to be frustrating, or even disconcerting. There were a number of (sometimes inter-related) reasons for this:

- They felt they were not believed
- They felt that years of being a loyal and 'good' customer suddenly counted for nothing
- They felt that blame was being placed on them by the provider

"I still had my debit card, so it turned out it was cloned. It was online transactions. But I felt I was no longer the victim, it was almost as if I was the culprit. The sort of questions they were asking, could anyone else in my household have done it… I know they have to check, but I was quite upset, and it was almost like they were blaming me" (London, older, experience of an unauthorised transaction)

These feelings were notable with, and expressed quite strongly by, a number of participants who had had money taken by a loan company: they felt their provider had no sympathy with their plight, and one participant described it as being as if his provider thought he deserved what had happened to him for going to a loan company in the first place. However, there were other instances of the perceived treatment described above which were unrelated to loan companies.

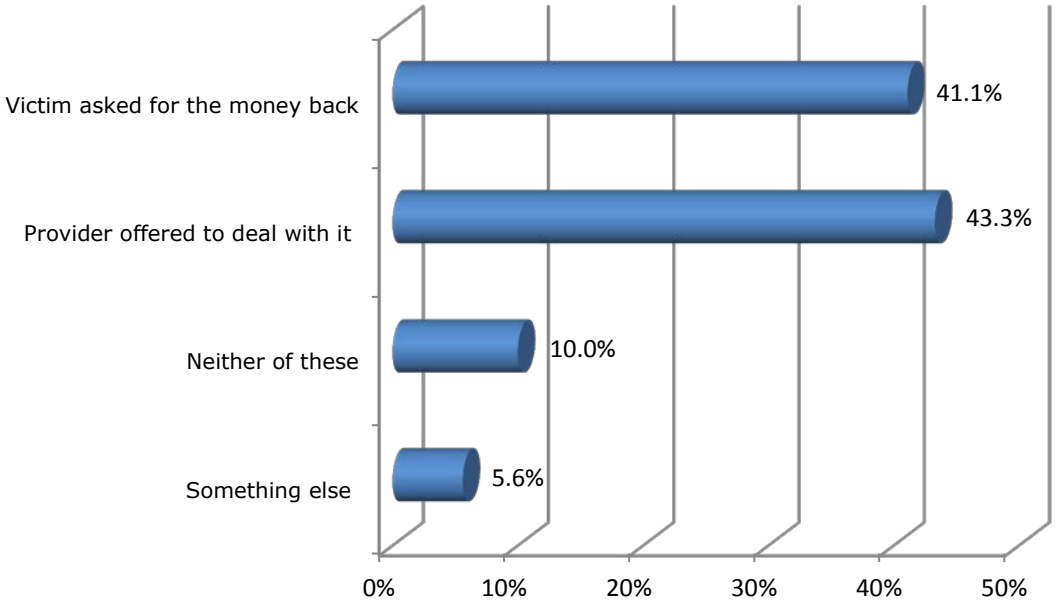
4.2.8 Emotional impact of the reporting and claims process

There were two broad reactions on the part of potential victims to the reporting process: relief that 'everything is going to be okay' following immediate reassurance and support from the provider; and frustration and even anger that they were not being listened to or believed. As mentioned above, this latter response was a minority reaction, but it did lead a number of potential victims to consider changing their bank, and a small number had actually done so in the period following the unauthorised transaction experience.

It is notable that the potential victims' eventual feelings about their provider depended more on their perception of how they were treated during the claim (and particularly reporting) process than on the eventual outcome: we spoke to people who had had their money returned but were left with a much lower opinion of their provider than before, and to people who had lost their money but still retained a high opinion of their provider. When pressed on this, both types of participant explained their feelings based on the way they felt they had been treated by the provider during the process. If they were treated with sympathy and respect, they gained or retained a high opinion of the provider. If they felt they were disbelieved or treated with what they saw as antipathy or a lack of respect, the provider-customer relationship seemed to be badly (sometimes irreparably) damaged as a result.

4.2.9 Asking for or being offered the money back

84% of participants who had suffered an unauthorised transaction asked for (41%) or were offered (43%) their money back from/ by their provider. Among the sample, 23 people (10%) who were potential victims did not pursue a claim. The main reasons given were that the amount involved was small, that the money had been taken by a family member or friend and that they had dealt with this themselves, or that they had come to the view that they themselves were to blame through carelessness or had made an error. Two thirds of these people (14) dropped out of the process after they had started it, while the remainder (9) had decided at the outset not to pursue a claim.



Q21: Once it became clear that money had been taken without your authorisation, did you request the money back or did the provider say they would give you the money back? Base 231: all UTs

Figure 6: Making a claim – most customers were being offered, or requesting, the money back from their provider

Note: for those that said 'something else', in most cases the provider dealt with the issue and/ or refunded the money.

4.2.10 Supporting documentation or paperwork required as part of the claim process

Just under half (49%) of the potential victims who took part in the online structured screening process were asked to provide documentation, or were sent paperwork by the provider to complete and return. Most of these (77%) found it 'easy' or 'very easy' to complete this paperwork.

The majority (67%) said they were given up to two weeks to complete and return the paperwork, and several said that they dealt with it and returned it as soon as they received it. Most said they were aware that a refund they had already been given might be reclaimed if they took longer than the allotted time to return the

paperwork, or that their claim would not be processed. Only a few said they were unclear on this point.

A similar picture emerged from the qualitative interviews. Many had had contact only on the phone, and in some cases the matter had been dealt with in a single call with no further contact being required. Some were asked to return paperwork they were sent, others were not sent anything. Those who were asked to complete and return paperwork did not see this as unreasonable, as they assumed it was part of the provider's investigation process and thought it demonstrated a degree of rigour. They found it easy to complete, and the requirement for their signature also made sense to them. The paperwork was often completed and returned immediately, as the participants thought it was important to do so.

Why the providers adopted different approaches to the process, and specifically to the need for paperwork to be completed and returned, is unclear, but it may have depended on the differing circumstances of both the customers and the unauthorised transactions, as well as the differing requirements of the different card schemes.

4.2.11 Outcome of the claim

Over two thirds (68%) of those taking part in the structured screening questionnaire said they had received their money back from the provider with no problem. Of these 81% received it either immediately (41% said the same or next day), or within about one week (40%). A further 19% of participants who received a full refund did so after further contact with the provider, and this took between two weeks and three months for 17%, and over three months for 2%. Most of the refunds (77%) were from the provider, while 14% were from the merchant.

A minority of 7% (15 people) had their claim declined by the provider. The main reason given was that they had entered into a contract with the merchant which authorised the transaction (e.g. a continuous payment authority, often related to a product trial). In only two cases was the reason for declining given as use of Chip and PIN. In one case, the PIN had been used at the ATM where the transaction occurred, and in the other the claimant had shared their PIN with a friend who had subsequently used the card. Two participants said they had not been given a reason for their claim being declined.

Most of these people (12 out of the 15) did not think the reasons given by the provider for declining their claim were fair, and half said they did not understand them, but eight of the participants did not challenge the provider's decision. Five remembered being given information about the appeal/ complaint process, and three made a formal complaint about the provider's decision.

In the qualitative interviewing, the details of the outcome and how it was arrived at were explored in more depth. A number of different positive and negative outcome scenarios emerged.

Among the positive outcomes the money was refunded by the next day, after a few days or after a few weeks. Where it was refunded by the next day, no further telephone contact was required after the first call. Some, but not all, had been sent paperwork to complete and return, and the money was credited back to their account beforehand. Where the money was refunded after a few days, this was often after the claimant had been sent paperwork which they had completed and returned, and the money had been credited shortly afterwards. Where the process had taken several weeks, the participants expressed some frustration in the interviews. Several felt unsupported, or even that some blame was being placed on them by the provider. Reference was also made to having to take the lead and chase the provider for progress updates, because there was little sign of proactivity from the provider. For most of these people the refund simply appeared in their account, with no other notification of the refund being provided.

Expectations among the potential victims in the qualitative interviews of how long the process ought to take varied, and in many instances were quite vague. More consistent was the expectation that the provider needs to conduct a thorough investigation. This was thought likely to include checking on what had actually happened, ensuring that the customer was not making a false claim, and identifying who had received the money. This assumption (or sometimes speculation) itself provided a degree of reassurance, as it suggested there was protection in place for the customer, and that unauthorised transactions of any value were taken seriously by providers. It was as a result of the view that the provider needed to conduct an investigation that expectations of timescales were vague: it was assumed that different circumstances might take more or less time to investigate, and so

timescales were likely to be variable according to the specific details of the unauthorised transaction. In principle this was generally not thought to be unreasonable.

Among the negative outcomes (i.e. where the money was not refunded), the main reason given was that the customer had authorised the transaction. This authorisation was in the small print of the terms and conditions, which the consumer had not read (and a few suggested that this print was so small as to make reading it literally quite difficult). In one case the money was refunded initially and then withdrawn after the investigation.

As mentioned earlier, the customer response to these negative outcomes depended on how they were put across and how the customers felt they were treated by the provider during the process. Those who felt they were being blamed by the provider had a similar (critical and negative) response to those who had been refunded, but who had felt they were being treated unsympathetically or blamed during the process.

Several of the potential victims had challenged the provider's decision and referred the matter to the Financial Ombudsman Service. In some cases they claimed to have chanced upon the option to involve the Financial Ombudsman Service, e.g. through talking with friends or browsing on the internet (and specifically through visiting the Martin Lewis website), rather than recalling this information being offered by the provider. Where they had involved the Financial Ombudsman Service their experience had been consistent: the Financial Ombudsman Service was extremely professional and helpful, had requested documentary evidence from the claimant, considered the case and then delivered a verdict. All of these potential victims who had involved the Financial Ombudsman Service had gained a verdict in their favour, and while the process had not been particularly quick, the complainants appreciated that the Financial Ombudsman Service needed to make a thorough investigation of the circumstances of the consumer complaint.

Asked about where the refund came from, the unauthorised transaction victims often stated that they were mainly focused on obtaining a refund, rather than who was providing it. Where they had received the refund from their provider, several mentioned that they assumed that the provider had reclaimed the money from the

receiving account (merchant or individual), while others assumed that the providers had themselves claimed on some sort of insurance or contingency fund set up to deal with unauthorised transactions.

4.2.12 Effect of the event on victims

There were two broad strands to the effect of the unauthorised transaction experience on the research participants interviewed qualitatively: how it affected their perception of the provider, and how it affected them more personally.

As mentioned earlier, the effect on their perception of the provider was driven more by how they felt they had been treated (and specifically how sympathetically and helpfully), than it was by whether or not they received a refund. If they felt treated 'well', they were well disposed towards the provider as a result. If they felt treated 'badly' they were not, and some had subsequently changed provider. This seems to have been at least in part as a result of their unauthorised transaction experience, though there were also sometimes other contributing circumstances such as prior dissatisfaction with the provider. Even here, their treatment by the provider over this experience seems to have acted as a spur to moving their account.

Where participants had felt treated well but had not received a refund, the provider's perceived attitude was a key factor: sympathetic to the customer's plight, not suggesting the customer has been at fault in any way, and where possible being proactively helpful, e.g. by looking for other similar transactions, or providing the customer with information about the merchant or what had happened (such as how or why the money had been taken).

To illustrate this point, one participant had had money taken because she had signed up to a 'free' trial which contained a continuous payment authority agreement in the terms and conditions she had accepted. The provider explained that this was what had happened, but did so in a way that placed the blame on the merchant for being deliberately deceptive rather than on the customer for not being more aware of what she had agreed to. The provider further explained that they were aware of this merchant and were strongly opposed to its business practices, but that in their view they were powerless to act and could not give her a refund. Despite not receiving

her money back, the customer was full of praise for the provider when interviewed, because she had felt that they were genuinely on her side.

With regard to the more personal effects of the unauthorised transaction, the potential victims were generally more affected by the fact of it happening than by whether or not they received their money back. They were shaken by money having been taken from their account, and often claimed to have modified their behaviours, and sometimes their attitudes, as a result. Typical changes in behaviour included taking more care over security at ATMs or when inputting their PIN in a shop, only using ATMs inside a branch, paying more attention to exactly where their cards are at all times (or at least more of the time), monitoring their account balance and transactions more closely and more often, and shopping at different (typically bigger and more well known) stores, both physically and especially online. Other changed activities include not giving bank details to new websites visited, not visiting bank sites in internet cafés, and reading statements more often and more closely.

For some there had been a wider impact: being more distrustful of websites generally, no longer buying goods on the internet (though Amazon and eBay were cited as exceptions to this), being more distrustful of financial services providers (e.g. where they had been seen as insufficiently supportive over a disputed transaction), and keeping account balances low while using cash more.

Most participants who had experienced an unauthorised transaction had become generally warier about security as a result, and specifically less relaxed about ATM use and remote shopping. Those who already saw themselves as security conscious and careful wondered what more they could do, but nonetheless felt less 'safe' than before. For a few, this was combined with an almost blasé attitude about what would happen if money were taken from them in this way again: their provider would simply refund them.

4.2.13 Communication during the claim process

Communication during the claim process varied in frequency and degree of proactivity from the provider, but some broad patterns emerged.

The process usually started with a phone call, either to or from the provider. Where it was to the provider, the response in terms of communication was usually good. If

the customer was not transferred to the fraud department immediately, he or she was usually promised a call back within a specific period. This call was then usually received within the stated period. The fraud department personnel usually took the information efficiently over the phone, though were at times cold and matter-of-fact to the point of seeming unsympathetic, and some potential victims had found this experience disagreeable.

Where the initial call was from the provider, communication sometimes broke down at the outset. Some people had been left a message by a synthesised voice, and they were inclined to treat these messages with distrust. A message left by a real person was much more convincing. A couple of potential victims suggested they should have been sent a text, while others said they had received one. This approach seems to have been quite effective.

When documentation was sent to complete and return, this was generally described as easy to follow and to complete (though one potential victim said he was not really able to 'fit' his description of the event into the options provided on the form). It usually arrived quite promptly: within a couple of days of the initial phone contact.

After this, communication tended to tail off. Updates or progress reports were not generally forthcoming from the provider as their investigation progressed, and a few potential victims felt they had had to chase their provider to find out what was happening. Some were told, either when they chased for progress or in the initial call, when they could expect a refund, but there seemed to be little written confirmation provided. Refunds typically appeared without further communication saying either when it would happen or that it had: victims simply saw the money reappear in their accounts.

In the few instances where potential victims had reported the unauthorised transaction in a branch, their recollections were again driven by how sympathetic a reception they had received from the provider, and this had varied considerably. Again there seems to have been little outbound communication while the matter was being investigated. In a couple of instances there seemed to be poor communication internally at the provider, as what participants were told on the phone and in branch did not always match.

The main gaps in the pattern described above between what potential victims would like and what actually happens are in the period when the unauthorised transaction is being investigated and when the investigation is over. Potential victims would like to be updated with progress and told when the case is closed, and this seemed to apply particularly when the case was drawn out over more than a few days. Progress updates would provide reassurance that something is being done, not just to return the money but to find out what happened and prevent the perpetrators from 'getting away with it'. Confirmation that the investigation is over would help victims draw a line under what has happened to them. It would also give the provider an opportunity to offer or restate advice on consumer security, although some of the potential victims interviewed said they had been given this advice over the phone.

4.2.14 Conclusions

The main conclusions based on this research are set out below.

It would seem that the great majority of victims of unauthorised transactions receive a refund from their provider. However, the timescale of this refund seems to vary considerably: from immediately (the same day as reporting or confirming that the transaction was unauthorised) to several weeks later. Victims are often not told when the money has been refunded, rather it simply reappears in their account.

Consumers are largely unaware of how long a refund should take, and their expectations of what is a reasonable time are less demanding than the stipulations laid down to the providers. The greater concern to consumers is that they will get their money back in the event of an unauthorised transaction, not that they will do so immediately.

In terms of the victim/ provider relationship, the way the victim feels treated by the provider is more important to the continued health of the relationship than whether or not the money is returned: the key for victims of unauthorised transactions is to feel supported by the provider, and this is more about the provider's perceived attitude and the details of their behaviour than it is about the final outcome.

Expanding this latter point, it is possible to draw up some basic precepts of good practice for providers to consider adopting, and of poor practice to try and avoid, in

dealing with customers who think they have been the victim of an unauthorised transaction. These are set out in the next section.

4.2.15 Identifying elements of good and bad practice

The consumer view of what constitutes good practice on the part of providers was largely built on reassurance, sympathy and supportiveness.

The participants acknowledged that certain questions need to be asked by the provider, specifically identification questions and establishing whether or not security details have been shared. It was felt that these questions (especially the latter) can and should be asked sympathetically.

Beyond that there was the view that the default stance adopted by the provider should be that the customer is in the right and has not behaved irresponsibly. Acknowledging and taking into account the customer's account history and prior account behaviour would make them feel supported (and not doing so proved to be one of the more emotive and damaging aspects of provider behaviour).

Potential victims wanted to be told what would happen and when, at least with regard to the immediate next steps, and needed to be reassured as early as possible about the return of their money, again with timescales wherever possible.

If there is no immediate resolution, consumers wanted to be given updates on progress, preferably by phone. When the process is complete, formal (written) confirmation of this, and that the money has been returned, would be welcome. If the money cannot be returned, a sympathetic explanation of why not would also help the consumer.

Further reassurance could be provided by telling the customer that their account will continue to be monitored for a further period, or where relevant that the merchant will be monitored. Reassurance could also be provided by providing follow-up advice and security tips for avoiding fraud in future. This would give consumers some action they can take in a situation where they are largely reduced to a passive role.

Based on the findings of this research, much (but not all) of the above is already being done, albeit inconsistently.

Much of what the potential victims saw as poor practice was simply the inverse of the above, but some specific examples of behaviours to avoid also emerged.

Phone messages left for customers should use a real (not synthesised voice), and should include a name, department, phone no. and hours when the caller can be contacted. Failure to provide this information can inhibit a quick consumer response, and at worst can raise consumers' suspicions as to the legitimacy of the call.

Asking apparently hostile questions or lacking sympathy for the customer can alienate them from the outset, and the research findings suggest that damage done to the provider-customer relationship at this point is hard to repair. Providers need to keep in mind that potential victims are likely to be shocked when they find out about the unauthorised transaction, possibly upset, and probably worried both about getting the money back and about the possibility of further withdrawals and other consequences (bank charges, missed payments, etc.). They need to be treated with sensitivity and sympathy.

As mentioned above, not taking prior customer loyalty and account behaviour into consideration can provoke a strongly negative reaction: customers can feel defensive, and if they think they are not being believed can feel insulted, all at a time when they need sympathy and support. Equally they can be alienated if they feel they are being treated in an impersonal way just when they need a personal touch from their provider.

Not telling the customer what will happen next and when, and what they need to do, can leave them uncertain when what they are looking for is reassurance that a process which will help them is now in train. By the same token taking too long to send out paperwork or a replacement card can extend their anxiety. In this context 'too long' probably equates to more than three days. If this is not practical, an explanation and alternative timescale would help, but the timescale would need to be adhered to once the expectation has been set, or the reassurance risks being lost.

Not informing customers of when funds have been or will be returned places the onus on them to check their account in order to find out. Although they are likely to do this anyway, they would prefer to be told by the provider as well.

4.2.16 Addressing the areas the FCA were keen to understand in more detail

In this section and the next, we revisit the areas the FCA felt needed to be understood in more detail in view of the research findings, and add our own hypotheses.

Customers might be being denied refunds on the sole basis that Chip and PIN were used in the unauthorised transaction: We found little evidence of this in either the qualitative research or the structured screening exercise, although we also encountered examples of people sharing PINs (and on a more limited basis passwords) with others. Where this was done casually, there was some willingness to lie about this to providers in the event of an unauthorised transaction.

Customers may face unfair burdens of proof when making a claim: We found that consumers expected providers to take a rigorous approach, and were indeed in some cases having to justify their claim. However, we did not see evidence of people being unable to prove what had happened or that the burden of proof was too onerous. In some of the cases we examined, no evidence was required at all (and not all the victims had been required to sign any paperwork).

Customers may face unfair burdens of responsibility in keeping security details safe: We certainly did find that some of the consumers we spoke to found it unreasonable to be expected to remember so many different passwords and PINs. Their solution was to use the same ones (or variations of them) across different accounts, or to write them down (often in a disguised form) on paper or in their phone. However, we saw no evidence that keeping a record of security details had impacted against potential victims receiving a refund after an unauthorised transaction, and some evidence that it had not.

Some disputes might be being incorrectly categorised by providers as merchant disputes rather than unauthorised transactions: We saw no evidence of providers miscategorising disputes, but customers are not always reading merchant T&C's, and therefore disputing transactions they have 'technically' authorised. We did pick up (sometimes strong) feelings that some merchants put future dated payment authorisation into the detail of T&Cs deliberately as a form of scam, and that this practice should be outlawed.

4.2.17 Strictly Financial's hypotheses

We did find that victims of some types of unauthorised transaction have less protection than others, e.g. where the victim had in fact authorised the transaction, such as with a future dated payment. In the research we found a number of victims of transactions which they had unknowingly authorised. Typically they had been offered a free trial of (usually health or beauty) goods, or they were using a payday loan broker to find the best short term loan deal.

In both types of case, the victim had relied on the headline marketing offer, and not read the fine detail of the T&Cs. As a result, they had authorised future payments without being aware they had done so. In the view of the consumers we researched who had had this experience, these transactions were unauthorised because they had not been made aware of the longer term commitment contained in the terms and conditions. Deeming it to be a 'marketing ploy', they saw this as a deliberate deception on the part of the merchants in order to take their money, often using quite emotive language to describe this (scam, con etc). This was often not helped by the merchants themselves adopting a hard line attitude when disputes arise – in many cases, they were both elusive and unhelpful.

The telescoping effect referred to elsewhere in this report could itself be having an effect on the figures being measured with regard to incidence of unauthorised transactions: with people remembering these events as having taken place more recently than they actually did, there is a risk that incidence could be recorded at an exaggerated level, e.g. if people are asked about experiencing an unauthorised transaction in the past 12 months. This possibility was illustrated in the research by the fact that all the people interviewed individually had answered a question to the effect that they had suffered an unauthorised transaction experience within the last 12 months, but when it came to describing it in depth it became apparent that some people's experiences had been 18-24 months ago: they seemed more recent because they had made a substantial impact on the victims.

The brief referred to the possibility of mistakes being made in the reporting of transactions (i.e. a transaction not being reported as unauthorised when in fact it was). We saw some evidence of the opposite of this, with transactions being reported as unauthorised when they were in fact errors by the merchant where the

transaction was authorised by the customer. We saw occurrences such as accidental over-charging by the merchant, with the consumer failing to recognise the name of the merchant (possibly because the name on the statement was different from the name of the merchant where they had made the purchase), or charging the wrong consumer (e.g. through reading the wrong gas or electricity meter). We also saw instances of bank charges having been incurred unexpectedly, for example as result of a Direct Debit going through earlier than expected and before sufficient funds were in the account to meet it, and so triggering the bank charges. In these instances, the individual elements were authorised, but the circumstances created a situation in which the consumer was faced with charges they saw as unauthorised or unjustifiable.

We also saw examples of what some consumers described as unauthorised transactions which had been attempted, but blocked by the provider. Nevertheless in interviews some of our participants referred to these in the same way as transactions which had gone through. In their minds the difference seemed to be more about whether or not they had authorised it than whether or not the money had been taken. In some ways this echoes the finding that the event itself had a greater impact on people than whether or not they received their money back: the issue is the activity rather than the money.

Another hypothesis considered was the possibility that there are unauthorised transactions for which no claim is made to the provider, but which are nonetheless reported as such, e.g. in market research. Examples of this we encountered in this research included instances where money was taken by a relative using a card and PIN and where small amounts were taken by a merchant (on the internet). In the latter cases the merchants were dealt with directly, but the unifying factor in these instances is that the consumers had an unauthorised transaction which they reported in the research, though not to their providers.

5. THE CUSTOMER JOURNEY: CASE STUDIES

The main aim of the research was to understand the different experiences of customers when making a claim. Below we have summarised the journeys of a number of individuals which are representative of a variety of circumstances and provider reactions to an unauthorised transaction.

5.1 Case Study 1: FDP trial

Bernard is a retired financial adviser. He is very knowledgeable and organised with his finances.

What happened?

He saw an advert for a miracle slimming pill which offered a free trial for only the cost of P&P. The company, based in California, then took £89 from his account immediately and a further £79 a fortnight later.

"The thing that you do wrong is that you don't read it all because it's a great big long blog that goes on and on. What they do is, as soon as you send to take £89 out of your bank and then, a fortnight later, take another £79"

Bernard called the company who claimed that, in signing up for the offer, he had committed to purchasing an initial month's supply (charged immediately) and a further month (charged two weeks in advance). The merchant was unhelpful, and blamed Bernard for not reading the term and conditions of the offer closely. The company refused to enter into any discussion or refund the money – despite Bernard not receiving any of the promised goods (other than the initial free sample which he subsequently returned).

The claim

Bernard noticed the transaction on a mini statement produced at an ATM and immediately went into the branch to investigate. The branch cancelled the card straight away, and said that they would investigate the transactions.

"The first thing the customer service bod did was say, 'right, we will cancel the card and we'll investigate and in the meantime.' They refunded me £79, that was the start of it, and then they have to investigate which would take them three weeks to do so"

Bernard was panicking because £160 had been taken from his account in the space of two weeks without his knowledge, and he was worried about further withdrawals being made. He did not necessarily expect to get the money back – he was focused on preventing more money disappearing.

"I was feeling very upset because £160 had gone out of my bank without my authorisation. He was very helpful in the bank … I didn't expect to get my money back to tell you the truth, particularly as they are in America"

Whilst in the branch he signed an authority for the bank to act on his behalf, and subsequently received a letter confirming this and letting him know what action they would take. They contacted him three weeks later with the news that they had retrieved the money from the Californian company and returned it to his bank account.

Bernard is very grateful to the bank for preventing further withdrawals so speedily, for acting on his behalf with the merchant and getting his money back (he assumes that the bank would have more clout than any individual). The bank exceeded his expectations, kept all their promises and appeared to be working on his behalf.

"He said what would happen before I left the bank and the letter that followed, reiterated what they were going to do … they did work within the timeframe they said. They were more than satisfactory, if I'd done it on my own wouldn't have got anywhere"

Bernard felt that he was scammed, and is now more careful about giving out his details and in reading to the bottom of any 'contract' he is entering into.

5.2 Case Study 2: Cloned card

Sandy is a retired civil servant. She is fairly organised with her finances, shopping around for the best deals and checking her balances on line every morning.

What happened?

Sandy and her husband returned from a holiday abroad and, the next day, received a phone call from her bank saying that they had noticed some irregularities on her account. There were three transactions totalling around £500 – a payment to a company in Singapore, one to a company in America and a payment to O2.

Sandy was extremely shocked and worried that this could happen, particularly as she had no idea how someone had obtained her details. The bank appeared to think that her card had been cloned, and that this could have happened at any time in the previous six months.

"It was a shock of never had anything like that happen before … I was quite worried and upset, it was the thought that somebody had done that and not knowing how it happened, was quite worrying. It's the thought that if it happened once, it could happen again"

The claim

The bank immediately reassured Sandy that she would receive her money back – it noticed a pattern of similar transactions on around 10 other accounts over the previous couple of days and so were closely monitoring these companies. As a result

the transactions were picked up almost immediately and 'cancelled' – Sandy clearly had the impression that the bank had 'caught' the payments before they left the account.

"They said, you don't need to worry we will immediately cancel those payments and you don't need to worry about it at all, but we will send you a form that you need to fill out to confirm that you knew nothing about them … It was excellent. Really, and more than I would have expected in a bank"

The bank did ask some questions about her usage of the card, but this was done in an enquiring way to see whether they could spot any similarities between Sandy and the other customers who were affected. Sandy received the form from the bank and completed and sent it back that same day – she felt some urgency to deal with it immediately and not delay. She was aware that if she did not complete it then the bank may take further action.

"They were really efficient, I was very impressed with the way they behaved all the way through … I couldn't fault them"

5.3 Case study 3: Stolen card

Kulvir is 34 and lives with her parents. She works in the National Health Service and is very organised with her finances – she knows to the last penny exactly what is in her account.

What happened?

Kulvir was in a night club with her friends when she left her bag unattended and it was stolen. She, her friend and the security staff searched

the club but were unable to find her bag. By her own admission, she was quite drunk and it was in the early hours of the morning – so she decided to go home and report the theft the next day. She admits that she probably was not thinking straight, and was in no condition to have a coherent conversation with her provider.

"I'd been drinking and I was a bit drunk and my mobile phone was gone and I didn't think they would go spending it so late at night, so I thought I would do it in the morning. Stupidly thinking back now, I should have just reported it"

The claim

The next day she called the bank and explained the situation – only to find that £200 had been withdrawn from her account. The bank stopped her card, noted down the story and referred the case to the fraud department. She was contacted two days later and the bank said that they were refusing to refund the money. The reasons given were that she had left her bag unattended, and had not reported the theft immediately it had been noticed (thereby allowing the withdrawal to be made later that evening).

Kulvir reiterated her position and reasons for not reporting the bag theft straight away but did not feel that she was being listened to.

"The person who phoned me was quite harsh, and they weren't really sympathetic to me. That could happen to anyone … They weren't listening. They weren't empathetic"

She received a letter from the bank confirming the decision to refuse the claim, and enclosing information about the Financial Ombudsman Service. Kulvir then contacted the Financial Ombudsman Service to take the matter further. After some investigation the Financial Ombudsman Service found in her favour and the bank refunded the money.

"They said the bank was quite unfair because what I did is what a lot of other people would have done. Because it was quite late at night and I've been drinking it was sensible that I called the next day"

Kulvir feels that the bank was unsympathetic and unwilling to listen to her side of the story.

"I've had that account with them since I was 13 years old, so you've been a loyal customer. Nothing like this has ever happened to me before, and the one time you need help, and it's not your fault. They come up and say this to you. I still got my account with them, but I'm not happy with them"

5.4 Case study 4: Remote purchase

Mandi is married with two young children, and works as a legal secretary. When she divorced from her first husband, her finances became messy. She and her second husband then took out a large loan for home renovations which they struggled to repay – as a result, the household finances have been 'hit and miss' for a while. Her father, an accountant, has taken charge and developed a spreadsheet on which they put all incomings and outgoings – and as a result, they appear to have regained control.

What happened?

Mandi spotted that several payments had been made to iTunes and on further investigation realised that these withdrawals had been going on for around 8 months. Whilst each withdrawal was for a small amount (£1-2), they added up to £54 in total. No one in the house has an iTunes account, so she knew that these were incorrect.

The claim

Mani rang the bank the next working day and reported the transactions as being incorrect. The bank immediately referred her to Apple, asking her to deal direct with the merchant.

"I think it was the fact that somebody else had used my card on my details. You just feel a bit violated. I know it's a small amount, but you just think how the hell has someone got my information and what else do they know"

However, Apple were less than helpful, continually asking her for her iTunes account number (which she does not have) and saying that they were unable to help without it (despite money clearly coming out of her account).

Finding herself in a Catch 22 situation, Mandi called the bank back and was referred to the fraud team. She was not expecting a refund, but wanted to prevent further transactions as well as let someone know that iTunes was fraudulently taking money from her account.

"I didn't think the bank would give me my money back. I rang them to tell me that iTunes wouldn't help me and ask what could I do now and it's then they said they would put me through to the fraud department and they put my mind at rest"

The fraud team sent a form for her to complete which was relatively easy to do, and the money was recredited to her account once the form was returned. Mandi was very pleased with the bank's response and the fact that they were prepared to refund her money.

"It's only 50 quid, but it's my 50 quid … They took my word for it and made it really easy. The bank was great. They were really quick and it was no questions"

5.5 Case study 5: ATM cloned card

Elizabeth is retired, with three children and one grandchild who she helps look after. She in financially organised and checks her balance twice a day – at midday and just before she goes to bed.

What happened?

Elizabeth has been a lifetime customer of her bank and is cautious spender, withdrawing regular and small amounts from her account for her daily needs. She was unaware of any problems until she received a phone call from the bank saying that £500 had been withdrawn.

The claim

The phone rang and, when Elizabeth answered, an automated voice announced that it was the fraud squad from the bank. Elizabeth was very shocked and simply slammed the phone down in panic and turned to her husband who said that she should have listened. The phone immediately rang again and this time she took the call.

"I thought, why would the fraud squad want to ring me up? It was a shock … it said this is the fraud squad [from the provider], please hold the line. My heart was going on. I was thinking, oh my God, what's happened. Then this person came on the line and said Mrs X your card has been cloned"

The bank explained that a withdrawal had been made in America for £500 which was extremely unusual behaviour for Elizabeth. On further investigation, it appeared that an ATM machine that she had used the day before had been doctored, and that the fraudsters had 'tested' her account by withdrawing 1p before attempting the larger amount.

"I said, oh my God, what I do what I do? She said, don't panic will send you a new card and will give you the money back but it won't be back instantly"

The bank did not ask any questions or request any proof – the withdrawal was so clearly outside of her normal behaviour that this was unnecessary. Equally they were reassuring and calmed her down. She was told that they money would be refunded within 10-14 days and that a new card and PIN would be issued.

"I panicked at first I thought I'd worked all that month and I've been robbed and I was frightened that they wouldn't get the money back but they were quite reassuring from the beginning that that wouldn't happen. They were fantastic"

5.6 Case study 6: Unauthorised Transaction - PayDay Loan

Tom works in administration, and is engaged with two young children. He is disorganised when it comes to finances, and clearly they are struggling to make ends meet. In the past Tom has got into debt with credit cards and so now avoids using them. However, Tom does like using a mobile banking app, and checks his available balance every day – this is more to see what cash is available than looking at specific transactions.

What happened?

Tom fell into arrears with his PayDay loan company. He negotiated with them, and agreed a repayment plan of £10 a month over 10 months – everything was confirmed by email. However, the company took the full £100 in a single lump sum.

The claim

Tom noticed the same day and was extremely upset and annoyed. He emailed the company and did not get a response that day, at which point he called his bank, who

were extremely helpful. The bank explained that because this was a direct debit payment, they were unable to take any action until the funds had cleared from his account which would be in two or three days. The explanation felt reasonable, honest and fair and so Tom monitored his account over the next couple of days to check when it had cleared.

At this point, he called the bank back and was thanked by the bank for being patient and waiting to make the claim. They raised a dispute and completed the form whilst he was on the phone, and recredited the amount (which appeared in his account the next day).

"Everything was done over the phone, very simple and very well explained"

He was told that if evidence came to light that called his version of events into question they would claw the money back – he was unconcerned, as he had paperwork from the PayDay loan company proving his point.

"They did explain that this was pending investigation and if they had evidence from the company that proves that they had authority to take the amount then the account may be debited for that amount"

Tom was extremely pleased with their response and helpfulness – the loss of the £90 (i.e. the difference between the agreed repayment amount and the total debt) would have caused significant financial pressure for him and his family, so to get the money back quickly was greatly appreciated.

"All in all it's a very straightforward process and the bank listened to me well"

6. APPENDIX

6.1 Research objectives

The overarching objectives fell into three broad areas of exploration:

- The consumer context and perception of their own and provider responsibilities
- The customer experience and claims journey, in order to identify good and poor practices
- Understanding and identifying why discrepancies may exist in the statistics available from different sources as to the value of unauthorised transactions occurring on people's accounts and the scale of consumer detriment associated with this

To meet this wide range of objectives we adopted a mixed methodological approach, with each stage designed to inform specific areas of the project requirements. Each exploratory area was broken down into a number of more specific research objectives – a full list of these objectives is included in the technical report, but we have provided a broad overview of the areas of investigation below:

6.1.1 Consumer context and perception of their own and provider responsibilities

We needed to explore the extent to which consumers knew their rights with regard to unauthorised transactions on their account, and specifically what they thought they were and were not entitled to expect from their financial provider. Equally we needed to understand what they thought would be expected of them by the provider in the event of an unauthorised transaction, and what they thought the provider was entitled to expect.

Particular areas of interest included what people perceived to be enshrined in law or regulation, and which elements of the providers' terms and conditions they thought might be relevant when making a claim for an unauthorised transaction.

In order to be able to place this in context, we also needed to understand what consumers thought their obligations were in respect of looking after the security details of their accounts, how reasonable they thought these obligations were, and to what extent they met them. Against this background we needed to understand what consumers' expectations were of the process of making a claim for an unauthorised transaction: how to go about it, how long the process should take, what the various

steps were, and what both they and the providers needed to do as part of this process.

6.1.2 The customer experience and claims journey

We needed to gain an understanding of the consumer journey when making a claim: how the unauthorised transaction was discovered and by whom, and how the process unfolded from there. As well as exploring the process the consumers went through in making a claim, it was important to understand how they felt, and this applied equally to the impact of the unauthorised transaction on them and how they felt treated by the provider during the claim process.

As part of this exploration we also needed to understand if and why people had either decided not to make a claim in the first place, or had abandoned the claim during the process.

Part of the examination of the claim process involved looking at how well consumers understood their options if their claim was refused by the provider, as well as what they did in these circumstances (and why), and how they felt about it. This included their knowledge and use of any outside sources of information or help, including the Financial Ombudsman Service.

From this close examination of peoples' real experiences we could identify examples and details of what could be defined as good, and conversely, poor practice.

6.1.3 Understanding and identifying why discrepancies may exist in the statistics

Here the key objective was to gain an insight into why different sources of data suggested different volumes of unauthorised transactions on people's accounts, as well as to understand what factors might be contributing to these discrepancies.

In parallel with this, we wanted to help the FCA to understand the extent of any consumer detriment resulting from unauthorised transactions on their accounts, and whether this varied by type of consumer.

6.2 Research methodology

In order to meet the requirements of the project, we adopted a mixed methodological approach, each aspect of which was designed to meet a particular need or objective. The research involved four stages, of which the first two ran concurrently.

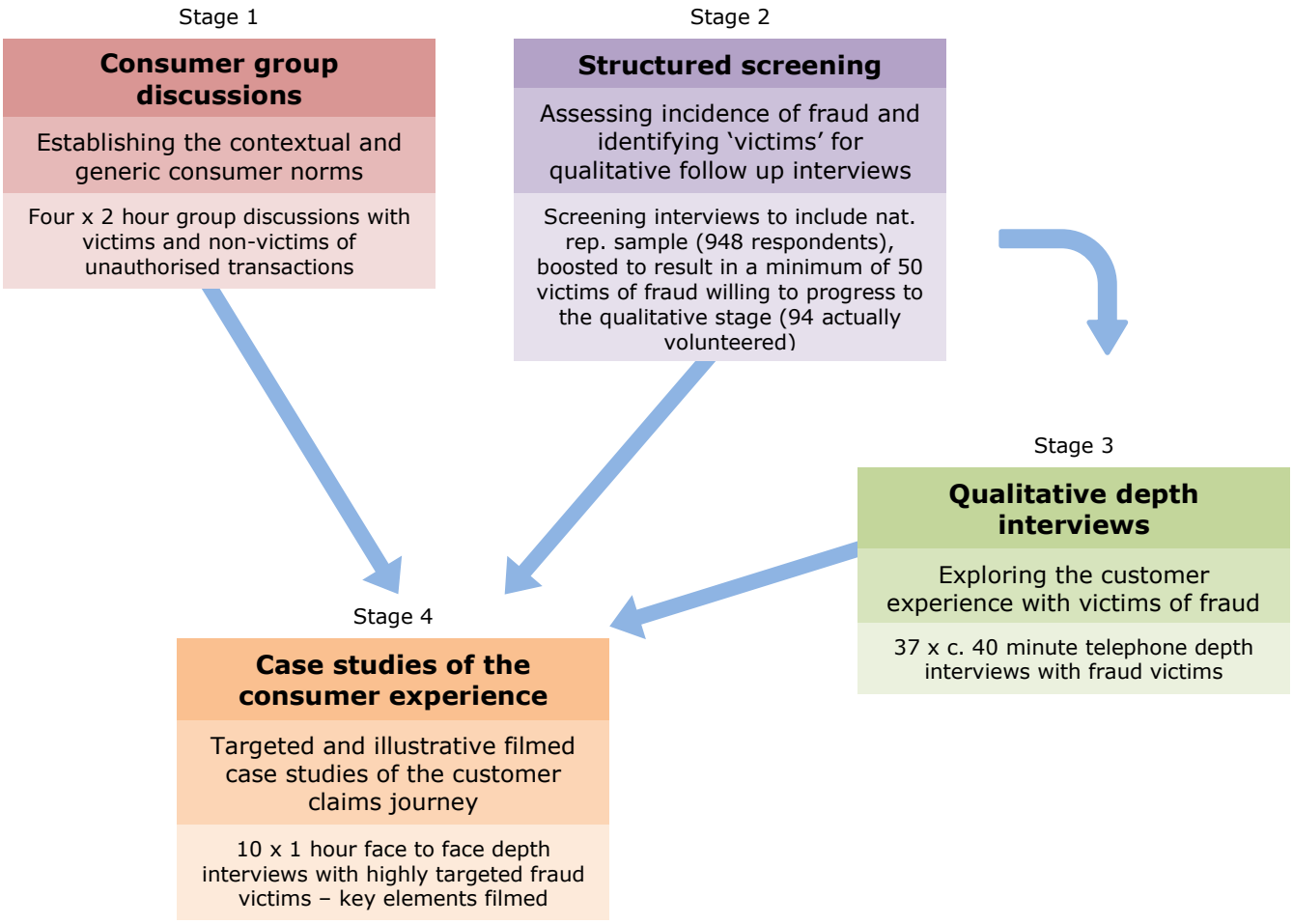


Figure 1: Overview of methodology

We have provided a more thorough description of each stage in the sections below.

6.2.1 Stage 1: Consumer group discussions

The main purpose of the group discussions was to understand the underlying attitudes, perceptions and expectations among consumers regarding their own and the providers' obligations and behaviours in the context of unauthorised transactions. This included attitudes and behaviours around account security, and the expected and actual experience of dealing with providers after an unauthorised transaction had occurred.

We conducted a total of four group discussions lasting two hours each, with victims and non-victims of unauthorised transactions. Two of these were groups with people who had not experienced an unauthorised transaction, one younger (up to 45) and one older (over 45). The other two were with people who had experienced an unauthorised transaction in the last 5 years, again one younger group (up to 45) and one older (over 45).

The groups were conducted in Manchester and London.

6.2.2 Stage 2: Structured screening exercise

The primary purpose of this stage was to identify recent victims of unauthorised transactions (within the last year), so they could be followed up with a qualitative telephone interview focused on their experience, both of the unauthorised transaction and dealing with the provider in the aftermath. The secondary purpose was to provide quantitative indicators of the scale of different types of unauthorised transaction and of refunds being given or not by providers.

The challenge posed was that of identifying and recruiting individuals to tell us their 'story' – we needed people who had been victims of fraud in the last year and who were broadly representative in terms of the different types of unauthorised transaction and varying claim value.

However, it was clear that such statistics as are already available do not specifically identify the audience required for this research, and so it was unclear exactly how many people would qualify and what the nature and split of experiences would be.

It was therefore decided to use a panel approach as a solution to this problem - primarily as a recruitment tool in order to identify a selection of 'unauthorised

transaction victims' who we could then interview on an individual basis. An online structured screening exercise was designed to identify people who had experienced different types of unauthorised transactions and target them for follow up interviewing. The design of this structured screening also generated quantitative data about the scale and type of unauthorised transactions.

The panel was initially used to generate a nationally representative sample of people to see what the incidence rate of claimed unauthorised transactions was amongst the general population. The initial question used replicated that used by the ONS[3], but we then went on to ask more detail around this response, including one totally open ended question asking respondents to describe the experience they had in their own words.

This was a crucial question in the subsequent review of the data – using this response (together with other data points), the research team and FCA project team reviewed each case individually and 'categorised' it accordingly. During this process, we identified 34 people whose experience did not appear to be one where money had been taken illegally, or where it was unclear exactly what had happened. This included merchant mistakes and errors, cases where a different merchant dispute appeared to be taking place or simply cases that were too vague to define. As a result of this process, 231 individuals appeared, on close inspection, to look as though they had the potential to make an unauthorised transaction claim (referred to as 'potential victims' throughout this report).

[3] The ONS question was "Have you had any money taken without your prior permission or knowledge from a bank, building society or credit card account in the last 12 months?"

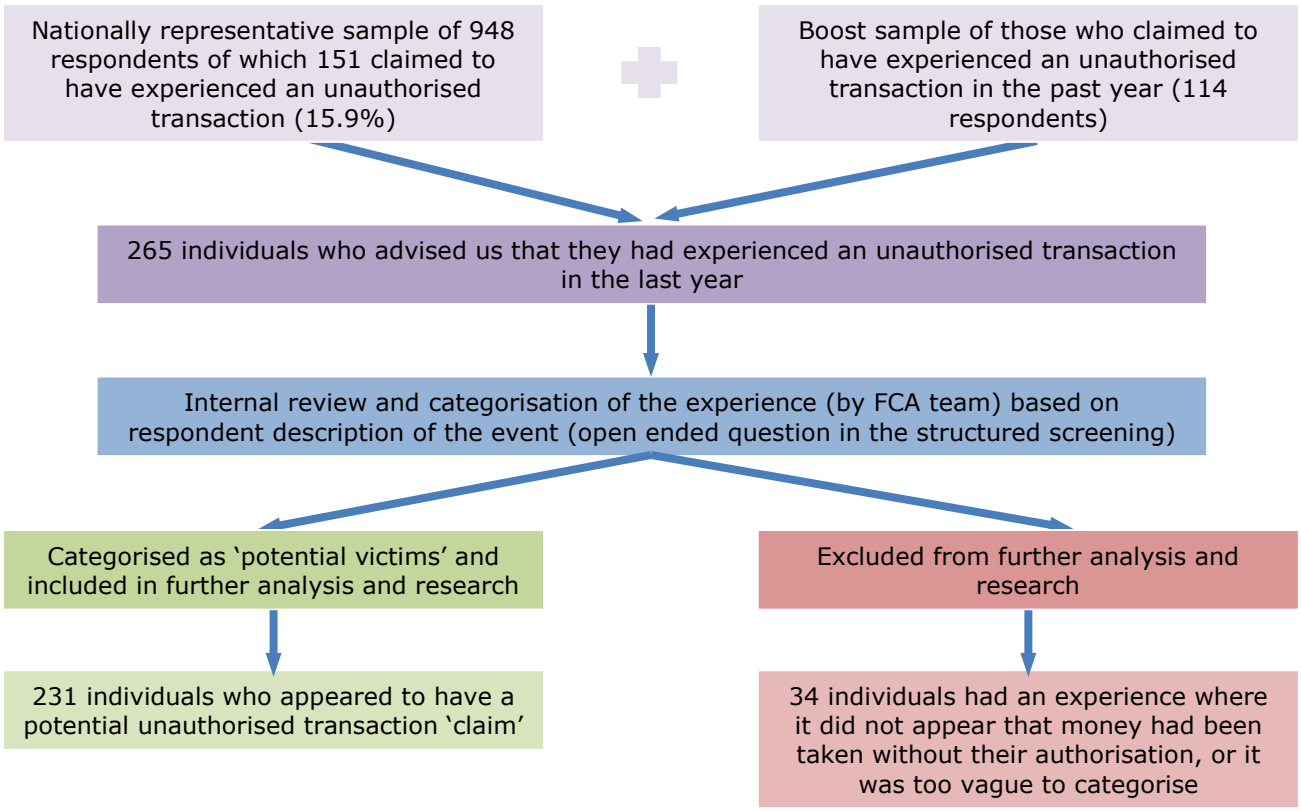


Figure 2: Overview of structured screening exercise and outcomes

Note, whilst we applied as much rigour as possible, we do not claim that this process was 'scientific' in the sense that we were relying on sometimes difficult, confused and complex descriptions by our respondents. We were surprised at the amount of detail provided in many of these descriptions, but inevitably there were some which were less detailed and more ambiguous.

Examples of responses describing what happened:

"The purchase was in a British Airways travel shop. I have no idea how my bank details were obtained or how the payment was made"

"Used on the internet to buy early morning £20 phone credit, then an hour later to buy a phone. My account must have been hacked online"

"Card stolen by someone I know and used three times at same bank by ATM - was a so called friend who stole card and PIN from my room"

"Phone call promising me to win big money sounded really real, asked for my details, and I stupidly gave it"

"After shopping at the supermarket I mislaid my debit card. Looked at my bank account online 2 days later and found the money had gone from my account"

As the purpose of the exercise was to identify a range of experiences and consumer profiles, the decision was taken to concentrate on those which were clearer, so that we could direct our focus for the qualitative phase of research.

Each of the descriptions provided was then categorised – we had no initial assumptions about the range/ nature of experiences, but simply created the categories to reflect the information being given. The categories fell into two main areas – unauthorised transactions related to continuous payment authorities, and unauthorised transactions related to fraud. Within unauthorised transactions related to continuous payment authorities, we saw three main types: cancelled permissions, loan related transactions and withdrawals relating to trials/ deals (i.e. consumer unaware that they were committing to a longer term contract). Under unauthorised transactions relating to fraud we saw a range of different experiences, including ATM withdrawals, PayPal withdrawals, shared and stolen cards, remote and point of sale transactions and phishing/ vishing fraud.

While this was not the primary purpose of the structured screening exercise, it did generate some data which provided useful insights into how customers view unauthorised transactions and the decisions they take during the journey. We have incorporated this data, where relevant, into this report, but with the caveat that it should be seen as indicative only.

6.2.3 Stage 3: Telephone depth interviews to ascertain the customer journey

The third stage comprised 37 telephone depth interviews of 30-50 minutes with consumers identified in the structured screening, covering a range of experiences. These included:

- 12 with those whose claim was rejected by the bank and/ or who took the case to the Financial Ombudsman Service. Three of these were related to loans, two to merchant disputes, and the remainder to a range of remote purchase, ATM use, and other fraudulent purchase
- 25 with those whose claim was accepted by the provider. Three of these related to remote purchase, three to fraudulent purchase, and two to each of loan and ATM related transactions. The remainder related to a range of other transaction types
- 6 with those whose unauthorised transaction was as a result of a continuous payment authority (in effect authorised, though perhaps unwittingly).

The purpose of this stage was to gain a detailed insight into the customer journey of those who are the victims of an unauthorised transaction: how people found out about it, what they and the provider did, how they felt about the unauthorised transaction itself and the provider's response, and how the experience affected them both emotionally and in terms of their subsequent behaviour.

The telephone depth interviews were conducted with consumers across the country. All depth interview participants were the sole or equal joint account holder on the account affected by the unauthorised transaction and all stated in an online questionnaire that the transaction in question had been within the last year. The focus of the research was on debit and credit cards, and these included a range of the major brands including the main high street providers, smaller brand names and online based credit and debit card providers.

6.2.4 Stage 4: Customer filmed case studies

The final stage involved 11 face to face interviews with unauthorised transaction victims, selected to cover a range of experience and outcome. Six of these had been interviewed in the previous stage, and five were new participants in the research. Parts of these interviews were video-recorded in order to provide material for the FCA to use internally.

The purpose of this stage of the research was to capture consumers describing in their own words how it felt to be the victim of an unauthorised transaction and to deal with the provider as a consequence. These 'vox pop' interviews were intended to bring the consumer experience to life in a more immediate way than the findings alone could do.

Types of unauthorised transaction covered included withdrawal of cash at ATMs, transfer of monies to merchants' and individuals' accounts, and use of cards for in-store and online purchases.