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.

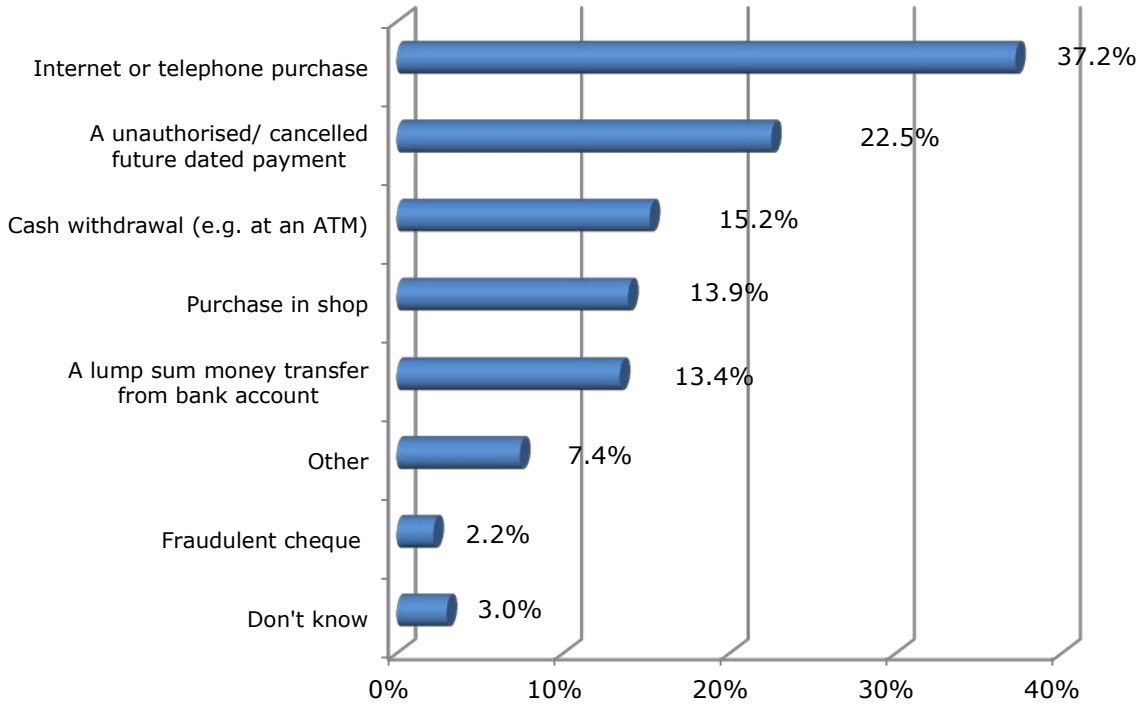
4.2.3 Type of account targeted and transaction value and type

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

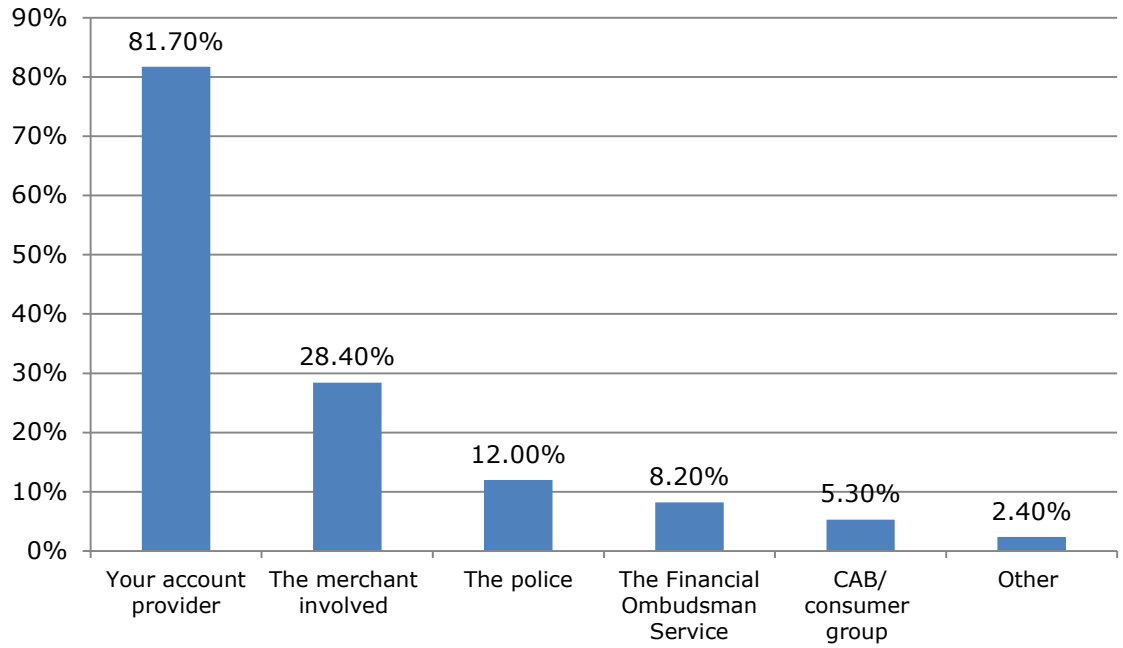
All the potential victims interviewed were upset by the unauthorised transaction, irrespective of how they came to find out about it and regardless of its value. They clearly recalled their feelings at the time in interviews, even though it was sometimes well over a year since the unauthorised transaction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

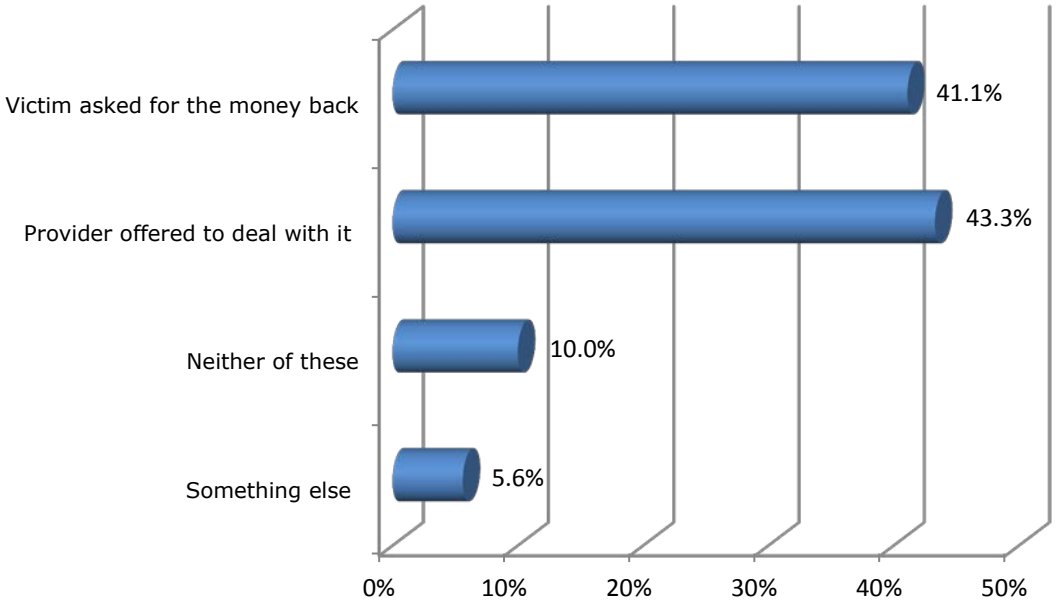
4.2.8 Emotional impact of the reporting and claims process

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

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?"