Financial Conduct Authority

Fair treatment for consumers who suffer unauthorised transactions

July 2015

Thematic Review

TR15/10

Contents

1. Overview

What does this report cover?

1.1 We have carried out work to discover whether consumers are being treated fairly in relation to unauthorised transactions. This involved assessing ten regulated firms providing current accounts and/or credit cards to understand if the consumer protections[1] in place are effective and whether firms are delivering fair outcomes for their customers. This report includes some examples of good practice and some areas that firms should consider further, as well as the results of independent consumer research, which helped us to understand more about unauthorised transactions from the perspective of consumers.

What we found

1.2 We focused on how firms ensure that customers receive refunds for unauthorised transactions and how these decisions are reached. We found that firms are generally meeting their legal requirements and are making a good effort to deliver fair outcomes for their customers. Firms tend to err on the side of the customer when reviewing claims and we did not find evidence of firms declining claims on the basis of customer 'non-compliance' with prescriptive security requirements in the terms and conditions.

1.3 This is a complex area, particularly for unauthorised transactions made using overdrawn current accounts where there are different legal requirements. We also identified issues with some of the content of account terms and conditions and found some fairly minor problems around how some firms organise their decision making, for example a lack of clear policies for complex cases and a heavy reliance in a small number of firms on experienced staff. Overall, however, firms seem to be trying to balance the need to consider claims on a case-by-case basis with consistent decision making.

1.4 Beyond the core question of decision making we looked at a range of areas including:

- customer communications and awareness, including how firms educate their customers on fraud risk
- prevention and detection of unauthorised transactions
- customer experience, including whether the processes in place are likely to act as a barrier to customers making claims for unauthorised transactions
- governance, oversight and measuring outcomes

1 Payment Services Regulations (PSRs) and Consumer Credit Act 1974 (CCA)

1.5 In each of these areas we saw a range of behaviours with many positive findings and some areas where performance was more mixed. Section three of this report sets out our findings in more detail along with examples of good practice.

1.6 The research[2] we commissioned identified that consumers recognise that protections are in place in the event of an unauthorised transaction. But consumers do not always know how the protections apply to them and tend to make assumptions about what their basic rights are. They also face obstacles when remembering multiple PINs (Personal Identification Numbers) and/or passwords in relation to their account(s), which may lead to them storing or sharing them. The research also identified that consumers who have experienced an unauthorised transaction value their provider immediately adopting and maintaining a supportive stance, as well as dealing with their claim promptly.

Who should read this paper?

1.7 We focused on current accounts and credit cards provided to consumers, but this report should interest all regulated firms offering payment services – including banks, building societies, credit card providers, authorised payment institutions and e-money issuers. Trade bodies representing these firms, as well as organisations that represent consumer interests and individual consumers may also wish to read this report.

Next steps

1.8 Based on our findings, we do not believe further thematic work is required at this stage.

1.9 Relevant firms should consider our findings and how they apply to their own approach to dealing with unauthorised transactions, taking action where needed.

2 Qualitative consumer research undertaken by Strictly Financial

2. Background

Why did we undertake this review?

2.1 Consumers are protected in the event of fraudulent or other unauthorised transactions by provisions in the Payment Services Regulations 2009 (PSRs),the Consumer Credit Act 1974 (CCA) and, in some cases, our Handbook.

2.2 Our work focused on current accounts and credit cards as these are core services used by consumers to undertake regular, day-to-day transactions. It is particularly important that consumer confidence is maintained in the security of everyday banking. To support this, the protections in place must be operating effectively, including the requirement to provide a refund in the event of fraud or other unauthorised transactions.

What is an unauthorised transaction?
An unauthorised transaction is 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[3])

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

3 www.fca.org.uk/news/continuous-payment-authorities-your-right-to-cancel

2.3 We wanted to make sure that when retail customers experience an unauthorised transaction they receive a refund from their current account or credit card provider where due. We also wanted to ensure that firms were complying with the legal requirements and not placing unreasonable obstacles or responsibilities on their customers, or unfairly rejecting claims.

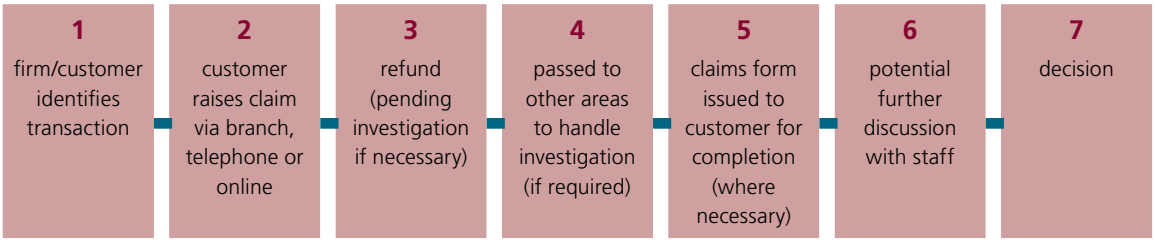
2.4 We assessed regulated firms, including banks, building societies and stand-alone credit card companies. In our approach, we recognised that there are some complex concepts for firms to consider, such as when a transaction is or is not made with the consent of the customer, and when a customer may be held liable for an unauthorised transaction due to their own gross negligence.

2.5 We were also interested in understanding more about the consumer perspective on unauthorised transactions. The experience of an unauthorised transaction can be both emotionally and financially stressful for consumers. For example, this could involve their accounts being cleared of funds, payments being refused due to insufficient funds and could also cause concerns regarding the security of personal information and potential impacts on credit ratings. As part of the review, we also looked at how firms handle claims made by vulnerable customers who, due to their personal circumstances, are especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.[4]

How big is this issue for consumers?
While comprehensive data on unauthorised transactions does not exist, the Crime Survey for England and Wales (CSEW) for the year ending December 2014 estimated that 4.8% of plastic card owners were victims of card fraud in the last year.[5]

Process for claiming a refund of an unauthorised transaction

2.6 While the process for a customer experiencing and claiming for an unauthorised transaction varied between firms, it generally took the following form:



4 FCA Occasional Paper No. 8, Consumer Vulnerability, February 2015, available online at: www.fca.org.uk/static/documents/occasional-papers/occasional-paper-8.pdf

5 Office for National Statistics, Crime in England and Wales, Year Ending December 2014, April 2015, available online at: www.ons.gov.uk/ons/dcp171778_401896.pd

What are the legal and regulatory responsibilities of firms?

2.8 Regulated firms, such as those who offer current accounts or credit cards, have a number of responsibilities in relation to unauthorised transactions. The relevant provisions are set out in Annex 1 and guidance is provided in our approach document.[6] There are differences between the requirements depending on whether there is consumer credit involved (as is the case with credit cards and overdrafts) or not.

2.9 When an unauthorised transaction is made using a payment service regulated by the PSRs[7], such as transfers from a current account or credit card payments, the responsibilities of both the payment service provider (PSP) and payment service user (customer) are detailed under regulations 55 to 62 of the PSRs.

2.10 The PSRs include regulations on:

- the consent and withdrawal of consent for payment transactions
- agreed spending limits on payment instruments (for example debit and credit cards)
- obligations of the payment service user and PSP in relation to use and safety of payment instruments
- evidence on the authentication and execution of payment transactions

2.11 For payment services provided under contracts that are not regulated credit agreements, the PSRs also cover:

- 'stopping' payment instruments
- notification of unauthorised transactions
- PSP and payers' (customers') liabilities for unauthorised transactions

2.12 For unauthorised transactions made under contracts that are regulated credit agreements, such as credit cards and current account overdrafts, provisions of the CCA apply in place of these provisions (see regulation 52 of the PSRs). These cover the responsibilities of both firms and customers in this respect, including:

- acceptance of credit tokens (such as a credit card or debit card when a current account is overdrawn[8])
- liability for misuse of credit facilities
- misuse of credit tokens

2.13 Certain provisions of the PSRs are also disapplied in the case of 'low value' payment instruments (see regulation 53).

6 *The FCA's role under the Payment Services Regulations 2009: Our Approach* FCA June 2013
7 The PSRs implement the Payment Services Directive (PSD) which will be updated when PSDII is implemented in 2017.
8 Section 14 of the Consumer Credit Act 1974 describes a credit token.

2.14 A PSP must generally refund unauthorised payments immediately[9] unless it has evidence that there is a reason to refuse a refund. It must also refund any charges and interest a customer has paid because of the unauthorised transaction.

2.15 If the transaction was on a credit card or overdrawn current account, firms are not required to provide a refund immediately, but cannot charge interest or ask for repayment of the amount unless it can prove the customer is liable to pay.

2.16 Under the PSRs, a PSP can only refuse a refund for an unauthorised payment if:

- it can prove the customer authorised the transaction – though a bank or building society cannot simply say that use of a password, card and PIN conclusively proves a customer authorised a payment
- it can prove the customer is at fault because they acted fraudulently or, because they deliberately, or with 'gross negligence', failed to use a payment instrument in accordance with the terms and conditions governing its use, failed to notify the PSP on becoming aware of its loss, or failed to protect the details of their card, PIN or password
- the customer told their bank or building society about an unauthorised payment more than 13 months after the date it left their account

2.17 Under the CCA, creditors such as credit card providers and banks and building societies in the case of overdrawn current accounts, can only refuse a refund for an unauthorised payment if:

- it can prove the debtor (the customer), or someone acting on their behalf, authorised the transaction – though a firm cannot simply say that use of a password, card and PIN conclusively proves a customer authorised a payment
- the loss was due to the use of a credit token by a person who acquired it with the debtor's consent

2.18 Creditors cannot hold customers liable for an unauthorised transaction on the basis of 'gross negligence.'

2.19 Under both the PSRs and CCA, customers may have to pay up to the first £50 of an unauthorised transaction if their card has been lost or stolen, or (in the case of the PSRs) their creditor or PSP can show they failed to keep the details of their password or PIN safe.

2.20 However, customers are not liable for any unauthorised payments made after they notified their provider of the loss, theft or unauthorised use of their card or password – unless the provider can prove they acted fraudulently. They can also not be held liable where the payment instrument or credit token has been used in connection with most distance contracts, that is those concluded without any face to face interaction, for example by internet, mail order, phone or television.

2.21 Where a retail banking service is not a payment service within the scope of the PSRs, provisions in the Banking: Conduct of Business Sourcebook (BCOBS) apply instead. BCOBS 5.1.11 and 5.1.12 contain provisions regarding firms' and customers' liability for unauthorised transactions.

9 Or within a reasonable period for non-payment accounts – see Banking: Conduct of Business Sourcebook (BCOBS) 5.1.11.

How did we carry out our review?

Firm assessment work

2.22 We assessed a sample of regulated firms offering current accounts and/or credit cards to understand their approach to unauthorised transactions. The sample included a variety of sizes and types of firms, including banks, building societies and credit card firms.

2.23 The assessment included a desk-based review of information submitted by firms in the sample. We carried out firm visits and met with key members of staff responsible for operations and oversight. Our key focus was to understand how firms ensure that customers receive refunds where due and how these judgements are reached.

2.24 We considered firms' communications to customers and their approach towards preventing unauthorised transactions, as well as how they make decisions and treat customers throughout the claims process. We also looked at firms' governance and oversight arrangements, including their management information (MI).

2.25 We focused on the overall approach taken by firms in the sample rather than reviewing customer files. We did not assess the detailed experience or final outcome of claims for individual customers.

2.26 We have given feedback to each of the firms in our sample and suggested appropriate follow-up actions.

Qualitative consumer research

2.27 We commissioned consumer research to look at the issue from a consumer perspective and understand more about customer experiences when they suffer unauthorised transactions. This involved four group discussions with people who had and had not experienced an unauthorised transaction on their accounts.

2.28 Screening interviews took place with 948 consumers who held current, savings and credit card accounts, covering a range of locations, ages and providers.[10] This allowed for qualitative research involving telephone interviews with 37 consumers who had experienced an unauthorised transaction experience on one of their accounts, with a further ten face-to-face in-depth interviews lasting one hour each with fraud victims.

10 Sample boosted to result in a minimum of 50 victims of fraud willing to progress to the qualitative stage.

3.
Findings – firm assessments

Customer communications and awareness

General approach

3.1 We set out to establish if firms' communications on unauthorised transactions deliver clear, consistent messages to customers and are accessible to all relevant customers.

3.2 Our approach included looking at firms' strategies and communications designed to raise general awareness of fraud, as well as those issued to individual consumers in the event of an unauthorised transaction. We reviewed whether relevant, up-to-date information regarding fraud and unauthorised transactions is easily accessible across a variety of channels, such as online, in branches and by post. We also considered whether this information is available at the most suitable time, for example following an experience of an unauthorised transaction.

3.3 We found that most firms made good efforts to educate their customers about how to protect themselves from unauthorised transactions. Some firms had invested substantially in communications strategies to improve consumer awareness and reduce the risk of fraud.

3.4 We identified evidence of useful information being made available in order to deliver a consistent message. This included messaging around the importance of consumers securing their account information, making clear that the firm will never ask customers for card details or PINs and online alerts to warn customers about fraud risks when making online payments. A number of firms shared details of current frauds and scams with their customers and provided content from or reference to other sources of helpful information such as law enforcement agencies. Effective approaches to the distribution of communications often involved the use of a range of channels, including account statement mailings, SMS messaging, online web pages and prompts using online banking.

Some firms ran local branch campaigns and encouraged their branch or call centre staff to talk to their customers about how to manage the risk of fraud and other unauthorised transactions while others were active in using radio and local newspaper coverage to share messages.

3.5 We also saw examples of firms frequently updating customer literature and information to make improvements and ensure it remained current. In some cases this was to update the content (for example, refreshing messages to reflect changing fraud models and risks) and in some cases to improve the clarity of messages (for example improving customer letters).

3.6 A number of firms told us that they wanted to include helpful material in their terms and conditions to educate customers on how to keep their accounts secure and raise their awareness of unauthorised transactions. However, we question whether terms and conditions are the right channel for customer education and, in general, firms were unable to evidence the effectiveness of this approach.

3.7 In the majority of firms, not all terms and conditions were fair and not-misleading. Examples of this include:

- Terms and conditions that did not mention the 13-month time limit in which a customer can make a claim for an unauthorised transaction.
- Terms for credit agreements placing a 13-month time limit on reporting an unauthorised transaction.
- Terms placing onerous responsibility on the part of the customer, which may deter them from making claims.
- Failure to explain that 'gross negligence' cannot be used as a reason to decline claims for unauthorised transactions made using an overdraft facility.
- Clauses that state where the law provides higher protection than the terms and conditions, the provider will apply the law. Whilst in theory this seems sufficient, it relies on consumers having a detailed knowledge of their legal rights and also raises questions regarding the legality of other clauses.

3.8 We saw evidence of a minority of firms restricting the availability of information to particular channels, such as making it available only online. This may make it difficult for some customers to access important information about fraud protection and the claims process. This is a particular concern for customers with no access to online services.

Communications approach following an unauthorised transaction

3.9 We explored how firms communicated with customers that had suffered a fraud or other unauthorised transaction. We saw examples of some firms providing tailored information to increase a customer's awareness following a claim, including advice on how to avoid fraud in the future.

3.10 One firm invited victims of unauthorised transactions to a workshop to understand their experiences and improve the firm's processes and communications.

We saw a small number of cases where firms lacked a clear strategy for communicating with customers about unauthorised transactions. We saw very limited evidence of firms checking the effectiveness of their messages. Examples of this included an absence of formal feedback to ensure that customers understand the guidance provided, as well as a lack of monitoring to track the use or effectiveness of the information provided.

Prevention of unauthorised transactions

3.11 Although not the main focus of our assessment, we looked at the approach taken by firms to prevent or proactively identify fraud and other unauthorised transactions.

3.12 We found that most firms in our sample took a proactive approach, including analysing risks, behaviours and trends, exploring new technology to detect fraud, such as voice recognition and ID scanning in branches. Most firms had structured approaches to sharing details of current frauds and potential risk areas with relevant staff in the firm, for example through staff briefing and training sessions.

3.13 Firms also shared details of collaborative work with other firms and industry bodies to help minimise risks to consumers. There are a number of panels and industry groups where intelligence on emerging risks and ideas is shared in a constructive way, including industry-led training workshops.

One example of collaboration in the industry is firms working closely with various card schemes (for example VISA and Mastercard) to report persistent merchants that cause difficulty when cancelling Continuous Payment Authorities (CPAs).

3.14 We found that all firms in our sample had monitoring mechanisms in place to allow them to identify and suspend suspicious transactions and subsequently contact the customer (either by phone or SMS) to confirm whether the transaction should be completed. Similarly, we saw evidence of firms encouraging consumers to pre-notify them of overseas travel to prevent any complications while abroad, where the risks of customers suffering unauthorised transactions might be higher.

3.15 Firms' estimates for the proportion of frauds that are prevented by their monitoring and fraud prevention systems ranged from 40-85%. A number of firms also told us that there is a delicate balance to be struck between identifying and preventing as many potential unauthorised transactions as possible and the risk of disrupting customers trying to carry out their everyday banking and credit card transactions.

How firms make decisions

3.16 We set out to assess firms' policies and how they make decisions when assessing claims for unauthorised transactions. We wanted to understand how firms manage the difficult challenge in a high volume area of considering the merits of each customer's claim while also achieving a level of consistency, i.e. that customers in similar situations are likely to experience a similar outcome.

3.17 This included a review of the approach taken towards decision making, the experience of staff and how firms confirm that decisions are made well. We looked at the approach to making routine decisions, as well as exploring the approach to more complex situations, for example decisions on transactions where a customer's PIN number may have been used or where the customer may have written down their PIN number. We also looked at how firms deal with claims from customers who may be vulnerable. We considered whether the firm's overall methods for dealing with unauthorised transaction claims were likely to support straightforward resolution or act as a barrier to the customer pursuing their claim.

Handling claims

3.18 We saw evidence that most firms were treating each unauthorised transaction claim on its own merits, supported by scenarios and challenge criteria for categorising different types of cases. While some firms take a manual approach towards handling claims, other, usually larger, firms use automated processes to uphold or refer cases. This included automatic decision making for claims under a certain amount. A number of firms also demonstrated the use of check points and controls for when customers' claims were likely to be rejected, such as the referral of cases to more senior or experienced members of staff before reaching a decision.

3.19 Firms told us that unauthorised transactions can be a challenging area requiring difficult judgements to be made. We saw a range of approaches to decision making. Some firms allowed frontline staff to decline cases, while others centralised decision making to more experienced

staff and ring-fenced teams, and had escalation processes for more complex cases. A number of firms used scenarios and other guidance to help staff reach a decision.

3.20 We saw examples where experienced staff and management spent time with new staff and monitored decision making to ensure that fair decisions were made, particularly when claims were declined. A number of firms told us that staff making decisions on unauthorised transactions were more experienced, having built up knowledge through significant length of service experience. In some cases this appeared to result in heavy reliance on a small number of key staff, where experience had not been passed on to other members of staff. Some firms also used different teams to handle different types of unauthorised transaction claims, such as those classed as fraud and those classed as disputed (for example cancelled CPAs), as well as more complex cases.

3.21 Most firms had internal discussions and escalation processes in place to share experiences and best practices, helping to support fair decisions for customers on what can be difficult judgements and situations. Our work identified that most firms undertake quality assurance (QA) testing to ensure confidence in the decisions being made, with some firms reviewing all declined cases while others used a sampling approach.

3.22 There were some concerns regarding the strategies some firms have adopted towards assessing unauthorised transaction claims, including different processes and misalignment between different business units within some larger firms, which may lead to inconsistent customer outcomes, in particular when dealing with customers across different locations.

Deciding the outcome of a claim

3.23 Generally, firms complied with the requirements of the PSRs and the CCA, although our work suggests that firms find the law complex, particularly when an unauthorised transaction debits an overdrawn current account.

3.24 The different approaches to decision making that we saw, demonstrated that firms are aware of their responsibility in determining liability for unauthorised transactions. Some firms treated all unauthorised transactions in the same way. Others identified how different provisions apply when determining liability for unauthorised transactions made using a current account with a credit balance (when the law permits the use of a 'gross negligence' test), and when the transaction was made using an overdrawn current account or credit card (when the law does not permit the use of a 'gross negligence' test).

3.25 We found that, in general, firms were not declining claims for unauthorised transactions purely on the basis of a customer's failure to comply with specific requirements in the account or card terms and conditions. We also did not find any evidence of firms holding customers liable for unauthorised transactions solely on the basis that the PIN was used to make the transaction.

3.26 Most firms told us that in complex, finely balanced cases the firm's approach will be to take a case-by-case approach and to err on the side of the customer. This included considering the circumstances of the case and the customer's actions and whether these were relevant to the decision before declining a claim. No evidence was identified to suggest that the amount of a claim has any bearing on the outcome of a case. We also did not see firms using financial or other incentives to influence decision making.

3.27 Some firms did not demonstrate that they have clear policies in place for staff when handling more complex cases, although the firms in question advised that this was sometimes counteracted by these cases being handled by highly experienced staff.

Continuous Payment Authorities (CPAs)

We did not set out to focus on firms' general approach towards CPAs. However, in the course of our work we noted that firms are making good efforts to comply with their regulatory requirements following our previous work in 2013.[11] Despite this, it was clear that merchant behaviour, such as frequently changing names, can make it difficult for firms to proactively identify and cancel a CPA once a customer has withdrawn their authorisation. Many firms took a collaborative approach with other industry bodies towards handling this risk, such as working with card schemes to report and monitor merchant behaviour.

Scams and vishing

Vishing is a scam that involves a fraudster using social engineering techniques over the telephone to fraudulently obtain personal and financial information.[12] 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.

These transactions can often be high in value and certain categories of customers are potentially more vulnerable or at risk of being targeted. We are aware the industry has been undertaking collaborative work to raise awareness of these types of scams (such as the British Bankers' Association[13]). While we did not specifically assess firms in this area we did see evidence of firms trying to support their customers before and after vishing attacks. This included some firms deciding to go beyond their legal requirements and treat vishing claims and other scams in the same way as unauthorised transactions, even where the customer had authorised the payment. UK banks, building societies and card issuers, with the support of the police, have published a Joint Declaration in respect of vishing type phone scams.[14] The Financial Ombudsman Service (FOS) published a Vishing report on 6 July 2015.[15]

11 www.fca.org.uk/news/continuous-payment-authorities-your-right-to-cancel
12 www.fca.org.uk/consumers/scams/banking-scams/banking-and-online-accounts
13 www.bba.org.uk/news-2/cold-calls-vishing-and-couriers/
14 www.financialfraudaction.org.uk/joint-declaration-phone-scams.asp
15 http://financial-ombudsman.org.uk/news/updates/vishing-report-2015.html

Credit brokers

In a policy statement on credit broking and fees[16], we reported in December 2014 that we have significant concerns about the practices of some credit brokers – particularly in the high-cost short-term credit (HCSTC) and other subprime credit markets – which charge upfront fees to consumers. We saw evidence of poor practice in the credit broking market, which is causing serious harm to consumers, with evidence of some payments being taken without the consent, or informed consent, of consumers.

While this was not the focus of our work on unauthorised transactions, firms raised the difficulties that such poor practice cause for them and their customers. We have since introduced new rules banning credit brokers from charging fees to customers and from requesting customers' payment details for that purpose, unless they ensure that customers are given clear information about who they are dealing with, what fee will be payable, and when and how the fee will be payable.[17]

Customer experience

3.28 Although not focused on customer service, we were interested in whether firms set out unreasonable expectations of customers, such as onerous security requirements. We were also interested in whether the forms and paperwork that customers complete in the event of an unauthorised transaction were likely to act as a barrier to customers making claims.

3.29 Firms' understanding of what consumers experience following an unauthorised transaction was in line with the findings of the consumer research undertaken as part of this work. We saw a number of examples of firms showing consideration for the needs of customers and how they are affected by an unauthorised transaction. We also saw evidence of approaches to help speed up the claims process, such as conference style telephone calls involving the firm, customer and merchant of the transaction in question.

3.30 One firm carried out research with customers who have suffered unauthorised transactions in order to understand their experiences and improve processes.

3.31 However, when looking at whether consumers face unreasonable obstacles in the claims process, we did find some evidence that process maps could be lengthy and complicated, raising concerns about whether the investigation methodologies in place help to deliver fair outcomes for customers. Independent reviews undertaken by some firms also identified this as an issue, echoing our concerns. While firms demonstrated that in certain cases a crime reference number is required to process a claim, we did not identify evidence to suggest that this was required in unreasonable circumstances.

3.32 A minority of firms made the refund of an unauthorised transaction contingent on the return of certain paperwork. This, along with examples of lengthy claims processes where customers are passed across multiple teams or business areas, could create a risk that they are put off or intimidated and do not complete their claim.

3.33 Our work identified some evidence of high volumes of claim decline rates, due to the non-return of customer disclaimer forms. In some cases this may be because customers have later

16 www.fca.org.uk/your-fca/documents/policy-statements/ps14-18
17 www.fca.org.uk/news/ps14-18-credit-broking-and-fees

remembered undertaking the transaction. However, this finding highlighted a lack of effort by some firms to follow up with customers. While in some cases particular card schemes may require the completion of disclaimer forms, it is important that this is managed effectively so it does not impact the customer's right to a refund for unauthorised transactions.

3.34 Other firms did have consumer friendly processes as well as robust chasing mechanisms to ensure customers complete and return their disclaimer forms. Effective examples included providing disclaimer forms electronically, such as by email, and providing online facilities where customers can log and manage claims for unauthorised transactions. Some firms did not mandate paperwork at all, or only in a minority of cases, such as when this is required by the card scheme rules.

How do firms treat customers in vulnerable circumstances?
We saw evidence of particular care being taken for customers in vulnerable circumstances. A number of firms used quite broad definitions of what might make a customer 'vulnerable' in relation to a claim for an unauthorised transaction and applied a flexible approach to deciding whether to pay a claim. Some firms also used different approaches to the treatment of cases for potentially vulnerable customers. This included the implementation of specialised tools to help customers with speech and hearing difficulties, as well as dedicated teams to handle claims made by vulnerable customers and providing customers with named case handlers to track their case.

Governance, oversight and measuring outcomes

3.35 We wanted to understand how firms' management oversee operations and decision making around unauthorised transactions. This included understanding how business operations and decisions were reviewed and challenged through day-to-day management and oversight structures and the work of control functions, such as compliance teams and internal audit.

3.36 We looked at how firms record case data and whether they were able to track the outcomes of unauthorised transactions claims. More generally we were interested in how management review the quality of their decision making, consider trends and emerging risks relating to unauthorised transactions. We looked for practical examples of how MI is used to inform risk management and support continuous improvement in the business. We did not review individual complaints, but we looked at the organisation of teams handling complaints on unauthorised transactions and how complaints are used to make business improvements.

3.37 When assessing governance and oversight arrangements we took into account the different sizes and types of firms reviewed.

Management oversight

3.38 In general, firms demonstrated good oversight arrangements and challenge of decisions on unauthorised transactions claims. A number of firms used 'independent' quality assurance (QA) functions. This normally involves someone independent from the main decision making area reviewing samples of cases, reporting back to management and providing training and making improvements as required.

3.39 Beyond the consideration of individual cases we saw good examples of senior management reviewing the output of QA and MI on customer experience and performance. Most firms regularly discussed risks to customers and trends around unauthorised transactions, particularly focused on fraud cases. Some firms also focused heavily on reviewing data on customer experience, for example looking at customer research to understand the experiences of fraud victims. In one firm senior management met regularly with claim handling staff to discuss trends and topics of interest, such as how to prevent fraud and learn from individual cases in order to drive business improvements.

3.40 We saw that the majority of firms used complaints teams or staff independent of the teams handling claims to review complaints on unauthorised transactions. While total volumes of complaints were generally fairly low, some firms were able to demonstrate the use of effective Root Cause Analysis of complaints to learn lessons to improve processes, communications and strategy. A number of firms were actively involved in cross-industry discussion groups, sharing findings of relevant cases and approaches.

3.41 Although oversight arrangements seemed to be working effectively in a number of firms, in a minority of cases we felt improvements were needed. For example, where firms were carrying out quite limited assurance of claims decision making or relying heavily on customer complaints as a form of MI, providing a very partial view.

Control functions including compliance and internal audit

3.42 A number of firms were able to provide evidence of ad hoc or regular reviews by control and assurance functions, such as compliance and internal audit, on areas relevant to unauthorised transactions. These were used to provide insight and challenge to senior management, leading to action and changes where required. For example, we saw audit reviews on fraud operations and compliance reviews on unauthorised transactions policy and processes.

One firm had commissioned a compliance review focusing specifically on whether the firm is making good decisions in relation to unauthorised transactions claims.

MI including data on customer outcomes

3.43 We saw mixed performance regarding MI, with some firms having particular challenges around the quality of data on the outcome of claims.

3.44 Some firms had clear, comprehensive MI, which provided relevant qualitative and quantitative information to management. Examples of the information provided included the outcomes and financial amount of claims, as well as the reasons for declining claims and trend analysis. This information can be used by management to support effective oversight.

One firm undertakes mystery shopping to check that customers who make a claim about an unauthorised transaction get a fair outcome.

3.45 However, in some firms we did not feel that MI was adequate or sufficiently granular to provide confidence that decisions for customers are correct. We saw examples where MI covers only a partial view of products (for example limited to compliance with some but not all relevant regulations) or was very process focused with no insight into customer outcomes. Some firms had already identified the need for improvements and were working to address gaps at the time of our assessment.

3.46 It was apparent that the categorisation of different types of unauthorised transaction can be a complex task for firms and it is therefore not surprising that varying approaches were taken towards this. We did not undertake quantitative analysis or outcome testing, either as a whole or in relation to subsets of unauthorised transactions. However, we have noted that in most firms, particularly those that provide both current accounts and credit cards, it would be difficult to do so due to the inconsistent categorisation of claims.

4.
Consumer research findings

4.1 We commissioned research to help better understand the impact of unauthorised transactions on consumers and their experiences of the claims process. We did not assess the outcome of cases or whether firms were complying with their legal and regulatory requirements. The key findings detailed below provide some useful insight into how consumers perceive unauthorised transactions and some lessons for firms.

Do consumers understand their rights and responsibilities?

4.2 The research suggested that, while consumers know there are some protections in place for unauthorised transactions, they tend to make assumptions about their basic rights. The common view among consumers was that they are entitled to their money back from their current account or credit card provider, as long as the unauthorised transaction is not their fault. Consumers had no detailed knowledge or understanding of their rights or obligations. They also widely noted that they did not read the detailed terms and conditions of their accounts, which may suggest that consumers face challenges with the amount and format of information presented to them by their account providers.

4.3 A number of consumers in the group discussion highlighted the obstacles they face with the number of PINs and passwords they are required to remember, admitting that they do not always keep their account security details as secure as they could. Examples of this included the sharing of PINs and, to a lesser extent, passwords. Participants expressed a view that it is unreasonable to expect people not to share their account details with loved ones. Some participants also stated that they write down PINs and passwords, often in disguised form in case they forget them. The majority viewed three to four PINs and passwords as the most they can remember and it is therefore fairly common for participants to duplicate PINs and passwords (or variations of them) across both financial and non-financial accounts, which could affect the security of their accounts.

What do consumers experience when making a claim?

4.4 Consumers typically reacted with a sense of shock and invasion upon discovering an unauthorised transaction on their account. It felt very personal and they wanted this to be reflected in the way their provider handled 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. Consumers 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. Consumers expected the provider to take their account history and previous behaviour into consideration when assessing a claim.

4.5 The claims experience varied from instant satisfaction to drawn out, frustrating experiences. While most consumers had been successful in making a claim, how they were treated played a greater part in their view of their provider than the outcome of the claim. Although not receiving a refund in circumstances where consumers felt they were entitled to one was clearly a source of both disappointment and frustration.

Positive experiences

4.6 Consumers characterised a positive experience as the provider immediately adopting and 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 that a refund would be provided. Knowing the timescale for the refund emerged as less important than having the reassurance that it would happen.

4.7 A good experience also included the staff asking questions in a gentle and sympathetic way and giving the impression that they could and would try to help. If the provider was unable to provide a refund, customers felt that expressions of sympathy and solidarity (at least in principle) by their provider helped them feel that they were being treated fairly. This also included the way in which the reason for not giving a refund was communicated. If the claims process started with a perceived lack of support, the consumers tended to retain this view of the provider, even if they subsequently received a refund.

Key concerns

4.8 Consumers viewed a lack of communication from the provider and being passed around between different departments during the course of a claim as a cause of frustration, even where the outcome was a refund. Claimants wanted to be kept up to date on the progress of the provider's investigation and were irritated if they felt they had to chase the provider for information and updates. The combination of unmet expectations and poor communication was seen as especially irritating.

4.9 While most of the victims 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 mostly to consumers who saw themselves as careful with their account security and were unsure about how the money had been taken from their account. They were left feeling exposed and wondering if there was more they could have done to protect themselves.

What impact do unauthorised transactions have on consumer behaviour?

4.10 The victims interviewed typically modified their attitudes and behaviours as a result of their experiences. 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 in future.

5.
Next steps – what should firms do?

5.1 Our work has identified that firms are generally making good efforts to reach fair judgements on whether to refund fraudulent or other unauthorised transactions. This is encouraging, and we saw some good practice in a number of areas, including fraud prevention, customer communications and oversight of unauthorised transactions.

5.2 However, we also recognise that this is an area that requires firms to make finely balanced judgements and implement complex legal requirements. We saw some less consistent practices in a number of areas. These included the content of terms and conditions, the development of effective MI that allows firms to track outcomes, sometimes lengthy claims processes and paperwork and some inconsistency around the application of the gross negligence test when determining liability in cases where the customer is overdrawn. It is likely that some firms will need to make improvements in a number of areas.

5.3 By publishing this report, we are sharing more details about the good and poor practices we observed.

Action for firms

5.4 It is important that all firms responsible for handling unauthorised transaction claims continue to focus on this area to support market confidence. In particular, consumers will continue to feel secure in using their everyday banking and payment services if they know that, in the event of an unauthorised transaction, their claim will be dealt with promptly and fairly.

5.5 We have given feedback to each of the firms in our sample about the good and poor practices we observed in their businesses regarding unauthorised transactions.

5.6 We encourage all relevant firms to read our findings and satisfy themselves that they are complying with their legal and regulatory requirements and have appropriate systems and controls in place to prevent harm to customers.

5.7 Firms may also wish to consider the consumer research and reflect on the experiences of consumers when suffering unauthorised transactions and throughout the claims process.

Future work

5.8 Based on our findings, we do not believe further thematic work on unauthorised transactions is required at this stage. Given the importance of the topic we will continue to maintain oversight of unauthorised transactions through our day-to-day supervision approach and may in future consider further focused work to ensure that consumers continue to experience fair outcomes.

Annex 1
Relevant provisions

Principles for Businesses

- PRIN 3 - Management and control
- PRIN 6 - Customers' interests
- PRIN 7 - Communications with clients

Senior Management Arrangements, Systems and Controls

- General requirements: BCOBS 4.1.1 R

Banking: Conduct of Business Sourcebook

- 5.1.11 - Firm's liability for unauthorised payments
- 5.1.12 - Banking customer's liability for unauthorised payments

Payment Services Regulations 2009

- Regulation 52: Disapplication of certain regulations in the case of consumer credit agreements
- Regulation 55: Consent and withdrawal of consent
- Regulation 56: Limits on the use of payment instruments
- Regulation 57: Obligations of the payment service user in relation to payment instruments
- Regulation 58: Obligations of the payment service provider in relation to payment instruments
- Regulation 59: Notification of unauthorised or incorrectly executed payment transactions
- Regulation 60: Evidence on authentication and execution of payment transactions
- Regulation 61: Payment service provider's liability for unauthorised payment transactions

- Regulation 62: Payer's liability for unauthorised payment transaction
- Regulation 63: Refunds for payment transactions initiated by or through a payee
- Regulation 64: Requests for refunds for payment transactions initiated by or through a payee

The FCA's role under the Payment Services Regulations 2009 - Our approach

- 8.86 – 8.91: Consent
- 8.92 – 8.94: Payment service provider's liability for unauthorised transactions (regulation 61)
- 8.95 – 8.97: Obligations of the customer in relation to payment instruments (regulation 57)
- 8.98 – 8.99: Obligations of the payment service provider in relation to payment instruments (regulation 58)
- 8.100 - 8.101: Notification of unauthorised or incorrectly executed payment transaction (regulation 59)
- 8.102 – 8.105: Evidence on authentication and execution of payment transactions (regulation 60)
- 8.106 – 8.113: Payment service provider's liability for unauthorised transactions (regulation 61)
- 8.114 – 8.119: Payer's liability for unauthorised payment transactions (regulation 62)
- 8.120 – 8.123: Refunds for payment transactions initiated by or through the payee (regulation 63)
- 8.124 – 8.125: Requests for refunds for payment transactions initiated by or through a payee (regulation 64)

Consumer Credit Act 1974

- Article 66 – Acceptance of credit-tokens
- Article 83 – Liability for misuse of credit facilities
- Article 84 – Misuse of credit-tokens

Unfair Terms in Consumer Contracts Regulations 1999

Financial Conduct Authority

PUB REF: 005061

25 The North Colonnade Canary Wharf
London E14 5HS
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk