Reporting on Insights Gained into UK Citizens' Perceptions of Contactless Card Risks

Lukas Aldag*, Karen Renaud†, Benjamin Berens*, Reyhan Duezguen*, Mattia Mossano*, Melanie Volkamer*

* SECUSO - Security, Usability, Society, Karlsruhe Institute of Technology
† Division of Cyber Security, Abertay University
* firstname.lastname@kit.edu, † k.renaud@abertay.ac.uk

Abstract. Contactless debit cards are widely used in the UK, slowly becoming popular in other countries as well. The feature that distinguishes these cards from regular ones is that they can be used without entering a PIN if the transaction amount is below a predetermined limit. This is undeniably convenient, but introduces a risk: cards could be lost or stolen, and the new holder could make purchases without providing a PIN. European banking regulations (PSD2) mandate that customers be fully refunded by their banks in these cases (as long as no negligence can be proven). While the law is clear regarding liability and citizens' actual contactless card risks, we wanted to explore UK citizens' perceptions in this respect. We conducted an online survey, specifically exploring the perceptions of *liability, severity* and *likelihood* of contactless card fraud. We discovered that participants' risk perceptions were not aligned with their actual risk. In particular, most participants assumed that they themselves would be liable for any contested transactions. There are clear lessons to be learned – also valid for other EU countries – emphasising the need to ensure that consumers are aware of their rights in this respect.

Keywords: contactless cards · liability · severity · likelihood · perceptions

1 Introduction

Shoppers can pay for their purchases in a number of ways. Over the last few decades, the number of card purchases in the UK has gradually overtaken cash, with contactless purchases dominating, as can be seen in Figure 1. Given that the UK is considered to be "*a mature CHIP and PIN nation*" [30], we chose to focus on UK card users to understand the risk perceptions of regular users.

Perceptions of the risks of traditional payment methods (debit/credit cards, cash) have been investigated [20, 13, 15], but contactless debit card mental models have received less attention. European banking regulations require banks to refund contested transactions, as long as no negligence can be proven and the PIN was not entered. The implications for the customer are that use of these cards, contactlessly, is liability free.

Do contactless card holders know this? We carried out a study to gain insights into UK consumer perceptions of contactless card risks.

Section 2 reviews the risks of card usage. We designed an online study (Section 3) to gain insights into UK contactless card users. Participants were presented with a

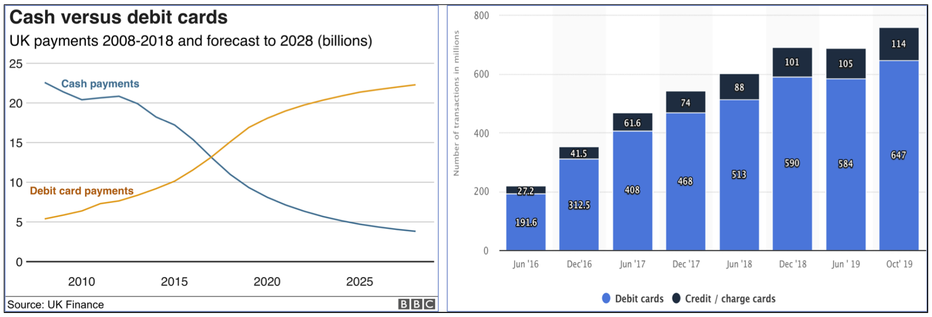

Fig. 1. UK Cash vs. Debit Cards [4], Contactless Usage growth since 2016 (https://www.statista.com/statistics/748192/number-of-contactless-transactions-in-the-uk/)

pickpocketing scenario where the victim subsequently notices a number of unauthorised transactions on his account. We then asked the participants a range of questions related to this scenario, with particular focus on *liability, severity* and *likelihood* perceptions. We present our findings in Section 4 and discuss them in Section 5. We review the literature related to contactless payments in Section 6 before concluding in Section 7.

2 Background

When debit cards were introduced in the UK in 1987, they were a very attractive alternative to cash. It was only during the mid 1990s that they spread throughout UK society[1]. The cards themselves were easy to carry and had no intrinsic value. They offered bank account holders ready access to their cash reserves, protected by using a secret PIN, allowing users to safely pay at most *points of sale* (POS).

Initially, to mitigate the risks of cashless payments, banks required customers to replicate the signature that appeared on the back of their card every time they used it. The card's information was stored on a magnetic stripe that could easily be read and counterfeited. This vulnerability was quickly exploited by criminals [30]. Embedded CHIP & PIN cards replaced magnetic stripes to prevent counterfeiting, thus reducing fraud[2].

In 2008, contactless cards, also referred to as Near Field Communication (NFC) cards, emerged in the UK [23]. These could be used to pay for purchases with a mere tap on the terminal, without entering a PIN. Although they undeniably enhanced convenience, they also heightened the risk of fraud. Those who carry a card requiring a PIN risk losing money only if both the card and PIN are stolen. However, if someone steals or finds a contactless card, they can use it at a POS without a PIN for transactions under a specific threshold.

[1] http://www.theukcardsassociation.org.uk/history_of_cards/index.asp
[2] http://www.theukcardsassociation.org.uk/news/10yearsChipandPINnews.asp

The contactless limits are different across the world. In the UK, it is £30 and in Germany it is €25 while in the USA it is $100[3]. Note that these limits were in place before the UK COVID-19 pandemic lockdown, during which the contactless transaction limits were adjusted upwards.

Contactless payments offer people the maximum amount of convenience at the POS where transaction amounts are small. In 2016, Jones [14] reported that the average transaction in the UK was under £10, which appears to be a good match for contactless payments.

What about the risks? Jones [14] reported on research by the Nationwide Building Society, which found that in 2016 more than half of UK citizens were "wary" of the new contactless payment cards. They reported on people wrapping their cards in tinfoil to prevent fraudsters from taking payments from their pockets. Yet in 2019, de Best [5] reported that 46% of point of sale (POS) transactions in the UK were contactless. UK citizens had clearly become less worried in the interim.

Financial Fraud Action UK [11] notes that fraud on contactless cards and devices remains low, equivalent to 2.7p in every £100 spent using contactless technology, accounting for only 1% of overall card fraud.

The Real Risks: According to article 73 of the PSD2 [10], the payment service provider is liable for all unauthorised transactions. In combination with article 74, the payer's liability for unauthorised payment transactions can be a maximum of €50, or approximately £50. Even so, banks have introduced a less secure contactless system, which makes it harder to detect unauthorised transactions.

The everyday consumer might well not be aware of the regulations, but UK consumer rights group "Which", a trusted source of advice, published the outcome of their own investigation into contactless cards in the UK. Their findings can be summarised as follows [32]:

Customer Perceptions: 73% liked the convenience afforded by contactless cards but 69% were worried about the cards being stolen.

Liability: banks say they will refund fraudulent purchases, but they found cases where refunds were delayed or refused. The onus is on the bank to prove negligence and they are obliged to refund if they cannot do this. Customers can contact the financial *ombudsman* if their bank refuses to refund contested transactions.

Severity per Transaction: The transaction limit during this study was £30.

Opt Out: They provide a list of contactless card providers in the UK, and at least six did not allow customers to opt out of using these cards at time of writing.

Which's report provides an excellent overview of the actual liability and severity related to contactless payments. The question is whether the millions of UK contactless card users are aware of these facts.

3 Methodology

We carried out a mixed-methods study, as detailed below, because we were seeking to reveal insights. As such, we were not aiming to demonstrate significant statistical

[3] https://merchantmachine.co.uk/contactless-limits/

differences, only to reveal risk perceptions and knowledge of such risk parameters by UK contactless card users.

3.1 Research Questions

Our overall goal is to reveal people's mental models related to contactless debit card risk perception in the UK. To do so, we derived the following three research questions:

RQ1: Liability: *Who* does the contactless cardholder think is liable if a thief steals a card and uses it?

RQ2: Severity: *How severe* does the contactless cardholder perceive the consequences of card theft to be?

RQ3: Likelihood: *How likely* does the contactless cardholder perceive the risk of a thief stealing their card and using it to be?

3.2 Study Procedure

We conducted an online survey, with six sections (Figure 2), to explore UK citizen mental models. The survey was created with *SoSci Survey*.

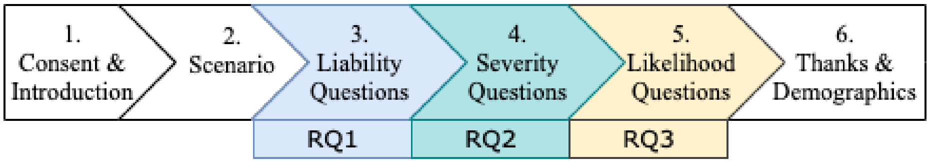

Fig. 2. Study Procedure

1. Consent & Introduction: We obtained informed consent and presented general information. Participants were informed that they were only permitted to participate if they had a bank account and paid for goods contactlessly with their debit cards.

2. Scenario: Participants were presented with a contactless card fraud scenario. We specifically chose a scenario where negligence was not a contributing factor. It is thus necessary for the victim to be unaware of the card theft and subsequent fraud. Hence the scenario makes it clear that there was no opportunity for the victim to report the theft and thereby prevent subsequent fraudulent use of their card.

Mister A. is walking down a street when a stranger approaches him and asks for directions. Later that day Mister A. realises that his purse went missing. He realises that he was pickpocketed by the stranger asking for directions. Mister A. goes to his bank and sees that the fraudster has used his card several times to make purchases, using the contactless payment option and staying below the limit, so that he does not need to enter the PIN.

3. Liability Questions:
We asked participants to provide an open text response:

- Who would be liable in the scenario above? *Open text response.*

Liability Experience Questions:
To assess personal or vicarious experience, we also asked a number of questions (reasoning that such experience might have made them aware of actual liability). We asked them to select one of the options for each question.

- Has something like this ever happened to you? *Yes/ No/ Don't know.*
- Has something like this ever happened to someone close to you? *Yes/ No/ Don't know.*
- Has something like this ever happened to an acquaintance? *Yes/ No/ Don't know.*

4. Severity Questions:
These questions focused on the potential severity related to the scenario. The questions related to severity were modified from a study by McClenahan *et al.* [18]. Severity questionnaires can be found in many academic disciplines, but most commonly in health studies [21]. Miles [21] refers to the survey formulated by Champion [7], which introduced the questions that we used for our study and those that the McClenahan *et al.* study [18] is based on. Not all of the questions are strictly tied to severity (pure severity questions are marked with an *). The other questions measure fear, which is part of assessing the severity of the consequences. These models are also connected to protection motivation theory, which we refer to in our discussion.

We modified the questions for our context and presented them to the respondents in random order. For instance, the original question was "*The thought of testicular cancer scares me*". We changed the specific reference to testicular cancer to "*the scenario happening to me*". We made the same changes for each question, respectively. The options ranged from strong disagreement to strong agreement on a seven-point Likert scale [16].

- The thought of the scenario happening to me, scares me.
- When I think about this scenario happening to me, I feel nauseous.
- If this scenario happened to me, my career would be endangered.*
- When I think about this scenario, my heart beats faster.
- This scenario happening to me, would endanger my marriage (or significant relationship).*
- This scenario happening to me, would leave me hopeless. *
- My feelings about myself would change if I would experience the mentioned scenario.*
- My financial security would be endangered if the scenario would happen to me.*
- I am afraid to even think about the mentioned scenario.
- Problems I would experience by such a scenario would last a long time.
- If I experienced such a scenario, it be more serious than other events.*
- If I had experienced such a scenario, my whole life would change.*

Severity Knowledge Questions:

We included two questions to assess knowledge of the actual severity. These could be answered by choosing an option and providing an open text response.

- Do you know how much money Mister A. could lose in the given scenario? *Yes, it is: open text / No, but I guess it is: open text.*
- Do you know how much you can spend per contactless transaction with your contactless debit card, without entering your PIN? *Yes, it is: open text/ No, but I guess it is: open text.*

5. Likelihood Questions:

We asked the participants questions related to the perceived likelihood of the scenario occurring. These questions were inspired by Brugger *et al.* [6], who introduced the concept of psychological distance to study likelihood perception. When looking into the literature regarding likelihood, several questionnaires exist but most of them are very specific to their own contexts. We thus chose a broader concept that can be applied to our context. We could have also chosen to ask a simple question to explore how likely they felt it was that the event could happen to them. With the current approach, we attempted to gain insights into multiple factors that would influence their likelihood calculus. Once again, we adapted their questions our context. For instance,the third question, "*To me, climate change feels like tomorrow...like thousands of years away*" was changed to "*it could happen to me tomorrow...couple years from now*". These changes resulted in the following questions:

- To me, the mentioned scenario feels: *very close (left) ... very distant (right).*
- To me, the mentioned scenario feels as if it could happen : *here (left) ... at the other end of the world (right).*
- To me, the mentioned scenario feels like it could happen to me: *tomorrow (left) ... couple years from now (right).*
- To me, the mentioned scenario feels like it could affect me: *(left) ... affecting distant strangers (right).*
- To me, the mentioned scenario feels: *very real (left) ... very hypothetical (right).*

Attention Check:

We included the following question to this list as an attention check:

- *This question will test your attention. Please tick the second answer from the right.*

Participants who failed the test were redirected to the end of the survey and no payment was given. Note that this was explicitly stated in the survey introduction (Survey Section 1).

Participants responded on a seven-point scale. The questions were presented in random order to minimise ordering effects.

6. Demographics and Thanks:

The questionnaire concluded with demographic questions (gender, age range). We concluded by providing a code so that they could claim their remuneration, and thanked them.

3.3 Analysis, Ethics & Recruitment

The quantitative data was analysed descriptively using SPSS statistics software. For the qualitative part, we used open coding. Two researchers read through the answers and created codes independently. Afterwards, one codebook was jointly created, and then used by both researchers to code all of the answers. The researchers achieved an inter rater reliability of $\kappa = .80$, which can be interpreted as strong agreement, according to [8, 19].

Ethics. We informed participants that their responses would be published anonymously, so that individual respondents could not be identified. We also informed them that their answers might be quoted in subsequent publications. We also explicitly stated that, to be remunerated, the participants had to answer the attention question correctly and that they had to engage in using contactless payments in their everyday lives. They were given the opportunity to exit the survey at any time without any negative consequences. The SoSci service is GDPR compliant and therefore conforms to the requirements of the University of [Anonymised]'s ethical commission.

Recruitment. We recruited participants from the UK via Clickworker's participant panel, commencing on 11.11.2019 and terminating on 30.11.2019. Having piloting the survey, we expected the participants to complete it in 15 minutes. Therefore, participants received €2.40 which corresponded to 1/4 of the UK minimum wage in 2019.

4 Results

In this section, we introduce the codes, as well as their frequencies, and the responses to all the questions asked in the survey. Finally, we explore further aspects that might have influenced the given answers.

4.1 Demographics

A total of 56 participants completed the survey. We excluded 11 participants from further analysis: three because of obvious nonsense answers, two because they had never used contactless debit cards, and six because they did not answer the attention question correctly. Of the remaining 45, 24 were male and 21 female. Age ranges were 21 under 35s, 10 between 35 and 45, and 15 over 45s.

Table 1. Coded answers to the question, "Who would be liable in the scenario?"

Code	#	%
Mr. A	15	33.3
Bank	18	40.0
Stranger	10	22.2
Other/NA	2	4.4

4.2 Codes and Total Responses

The first question asked participants whether they had experienced an incident such as the one described in the scenario, or whether it had happened to someone close to them or to an acquaintance. Two of the 45 participants had fallen victim to such an incident. Twelve participants knew someone close to them who had been a victim of such a fraud, and three knew it had happened to an acquaintance. Altogether this had happened to a total of 14 people. Note that we only counted people once, even if they knew of victims in multiple categories.

For the question related to who is liable, we created four different codes, '*Mr. A/me*', '*The Bank*' or '*The Stranger*'. Note that for the code *'Mr. A'*, we also counted everyone saying *me*, because a few participants imagined being in the scenario, even though we did not ask them to. We coded an answer to a certain category if the answer contained the code itself, or any variation thereof. Examples of how answers were coded:

- '*Mr. A/ Me*': Mr A., You individually.
- '*Bank*': The banks would be liable, The bank.
- '*Stranger*': Thief, The person who took the card.

Severity and likelihood were measured using multiple scale questions. To support comparison, we computed the average of all the answers, as suggested by [18]. The participants rated the severity with a mean score of 3.38 and a *SD* of 1.2. Note that '1' is trivial and '7' is extremely severe. The mean score for likelihood was 5.17 with a *SD* of 1.37. Note that we use the inverse value to enhance readability, meaning that '7' maps to highly likely and '1' maps to unlikely.

The participants were asked if they knew how much they could spend with each contactless transaction without having to enter their PIN. 33 participants said they knew and 12 guessed. We coded the answer using three codes, either '*Exactly £30*', '*More than £30*' or '*Less than £30*'. These were chosen to be either the correct contactless transaction amount, more or less than the amount. The answers were all provided in numerical format. In the following, we provide some examples of each of the codes.

- '*£30*': £30 max, £30
- '*More than'*: £40, £250
- '*Less than*': £20-£25, £20

All 33 participants who said they knew the answer gave the correct answer of £30. Seven of the 12 participants who guessed the answer also gave the correct answer. Only two guessed more than £30 and 3 less than £30.

The participants were asked how much Mr A might lose in the given scenario. We created eight codes for this question, more than £135, full amount on card, up to a specific limit, less than £135, up to £30 per transaction, nothing, and other/NA. According to the PSD2, after five contactles payments or cumulative £135 the bank has to prove the owner of the card by asking for a PIN. We asked them if they knew the answer or needed to guess. Twelve participants said they knew the answer and 33 guessed. Here, we provide some examples of each of the codes:

- *'Full amount':* All the money in his bank account., All his money

Table 2. Coded answers to the question, "Do you know how much you can spend per contactless transaction with your contactless Debit Card, without entering your PIN?"

Code	Know the Answer	%	Guess the Answer	%
£30	33	100	7	58.3
More than	-	-	2	16.7
Less than	-	-	3	25

- *'Up to a specific limit':* A proportion of his balance up to certain limit, maybe 25%
- *'More than £135':* £300? Is there a daily limit on contactless payments?, A few hundred pounds.
- *'Less than £135':* £100, £30
- *'Up to £30 per transaction':* £30 per transaction, Any amount of transaction under 30
- *'Nothing':* 0
- *'Other/NA':* The amount stolen

Table 3. Coded answers to the question, "Do you know how much money Mr A. could lose in the given scenario?"

Code	Know the Answer	%	Guess the Answer	%
Full amount	-	-	1	3
Up to a specific limit	1	8.3	2	6.1
More than £135	2	16.7	11	33.3
Less than £135	1	8.3	14	42.4
Up to £30 per transaction	5	41.6	2	6.1
Nothing	3	25	2	6.1
Other/NA	-	-	1	3

With respect to severity, 20 participants estimated the loss as being less than the actual limit of £135 and 24 estimated an amount over the actual limit. To calculate these numbers, we allocated the code '*nothing*' to "less than the limit" and "full amount", *certain amount*, and *up to £30 per transaction* to 'more than the limit'.

We explored the influence of answers to specific questions, e.g. who is liable on the one hand, to estimated likelihood and severity, on the other.

4.3 Impact of Experience:

Experiencing an incident ought to influence likelihood perceptions. 31 of the 45 participants had never heard of, nor experienced, such an incident, while 14 had. We see a difference in severity ratings for each of these groups.

No Experience: Participants who had not experienced the scenario, either personally or vicariously, had a mean score of 3.19 for severity and a mean score of 5.04 for likelihood.

Had Experience: Those who had had personal or vicarious experience had a mean score of 3.73 for severity and a mean score of 5.46 on likelihood. This shows that a lived fraud experience leads to an increased estimation of likelihood as well as severity.

4.4 Impact of Liability Attribution:

The next aspect to explore is liability attribution. We had three groups to distinguish (1) *'Bank*', (2) '*Mr. A/me*', and (3) '*The stranger*'.

- **Bank**: The mean score for severity was 2.85 and for likelihood 5.3.
- **Mr A./me**: The mean score for severity was 3.53 with a mean likelihood score of 5.12.
- **Stranger:** The mean scores were 4.15 for severity and 4.88 for likelihood.

In summary, participants who thought '*The Bank*' was liable estimated the lowest severity, followed by '*Mr. A/me*', and then by '*The Stranger*'. The likelihood estimation slopes in the same direction.

Considering the influence of liability attribution, we again distinguished between three categories: (1) '*more than the actual limit*' (>£135), '*less than the limit*' (<£135) , or '*the actual limit' (£135).* See Table 4.

Table 4. Coded answers for "Who is liable and how much can Mr A. lose in the presented scenario?"

Who is liable	**More than £135**	**Less than £135**	**Other**	**Total**
Bank	8	8	1	17
Mr A/me	8	5	1	14
Stranger	7	4	-	12
Other/NA	1	1	-	2

Finally, we considered liability attribution and separated participants based on direct or vicarious experience of such an incident. The results show that the severity, for each of the liability attributions, is higher for those with experience than for the uninitiated. Interestingly, those who fell into the group that attributed liability to the bank, and had had no experience of such a scenario, estimated the scenario as being most likely to occur. See Table 5.

5 Discussion

We can now return to our three research questions:

Table 5. Coded answers for who is liable and if ever heard/experienced such a scenario or not

Who is Liable	Heard/experienced incident			Not heard/experienced incident		
	#	Severity	Likelihood	#	Severity	Likelihood
Bank	7	3.30	6.26	11	2.57	4.69
Mr A./me	2	4.04	3.90	13	3.45	5.31
Stranger	5	4.2	4.60	5	4.1	4.80
Other/NA	-	-	-	2	2.67	5.80

RQ1: Liability: *Who does the contactless cardholder think is liable if a thief steals a card and uses it?*

We discovered that 60% of the participants did not realise that the bank was liable for contested transactions. The general lack of awareness we detected is beneficial to banks because if people assume they cannot challenge transactions, they will accept the liability, and they will do so seemingly for large amounts of money. Are banks telling their customers that they are not liable for fraudulent contactless transactions?

We visited the corporate finance institute to find the names of the top banks in the UK[4]. For each bank we did a Google search on 31 March 2020 for *contactless card fraud* appended to the bank's name. We then visited each of these banks to ascertain whether they did indeed provide accurate information related to liability. Table 6 shows what we discovered.

Table 6. UK Banks' Information about Contactless Liability

Bank	URL	**Liability**
Bank of Scotland	bankofscotland.co.uk	Bank is liable
Barclays	barclays.co.uk	Bank is liable
HSBC		—
Lloyds	lloydsbank.com	Fraud protection is the same as for Chip&PIN
Nationwide	nationwide.com	—
RBS	www.rbs.com	—
Santander	www.santander.co.uk	Fraud protection is the same as for Chip&PIN

The UK Card Association [29] explains that "*You are fully protected against fraud, so you get all of your money back and will never be left out of pocket.*" With respect to the amount a person can spend without entering a PIN, they say "*Every card has an in-built security check which means from time-to-time you have to enter your PIN to verify that you are the genuine cardholder.*"

Only two of the banks provide accurate information. The others either say that people have the same protection as for CHIP & PIN cards or require people to contact the bank to report fraud (so that they do not admit that they are liable for contactless

[4] https://corporatefinanceinstitute.com/resources/careers/companies/top-banks-in-the-uk/

card fraud).

RQ2: Severity: *How severe does the contactless cardholder perceive the consequences of card theft to be?*

88.9% of the participants knew how much they can spend per transaction, but were not aware of the limit of £135, which is encoded in article 42 of the PSD2 regulations. We expected participants to rate the incident as being less severe when the bank is liable, which was confirmed by our findings. Interestingly enough, the highest severity score was achieved by participants stating that the stranger would be liable. This finding might be explained by the uncertainty that comes with the stranger being liable. It might be nearly impossible to apprehend the stranger, and Mr. A might need to write off his losses.

RQ3: Likelihood: *How likely does the contactless cardholder perceive the risk of a thief stealing their card and using it to be?*

Participants rated the scenario at least likely if they thought a stranger would be liable. They rated severity lowest when the bank would be liable. This makes sense, because they personally would not lose anything, except for the effort involved in reporting the incident. We have to ask why the severity is not highest when Mr. A is liable? The participants might believe that it is Mr. A's own fault and that he should accept the consequences.

We can now explore some possible explanations for the mental models perception we revealed.

5.1 Possible Explanations

The mental models we uncovered are not due to a lack of information being offered by banks or consumer rights organisations. The conclusion we have to make is that people are not looking for the information. They are using the contactless cards without really being aware of the risks related to their use. There are a number of possible explanations for this.

Optimism Bias: Van Pligt [24] highlighted a general human tendency to underestimate risk, especially with respect to the impact on yourself. Moreover, our perception of risk is based on severity and likelihood, the intention being to avoid loss as much as possible. That means that, to minimize the sense of loss, people might underestimate the potential losses that might result from an adverse event. Doing this would help them to justify their usage of a system that they believe to be more risky given that they consider themselves to be liable for any associated losses.

Focus on Reward: Protection Motivation Theory [22] suggests that people weigh up likelihood and severity, on the one hand, against rewards, on the other, to make a threat appraisal. Our study suggests that reward (convenience) is greater than participants' perceptions of severity and liability. If people are aware of the fact that banks are indeed willing to refund them, then severity will never be an issue. At the moment, based on the responses, likelihood perceptions are not high either. It might be that the small amount of money spent in each contactless transaction leads them to discount the risk. That being so, the anticipated reward becomes far more salient than the perceived unlikely liability.

Avoidance: People might be engaging in avoidance behaviour, i.e. fear control rather than danger control [26]. If this is happening, it means that they prefer not to think about the risks because it makes them feel uncomfortable. This might explain why people don't make any effort to find out about personal liability. This might dovetail with Zipf's [33] suggestion that people will choose the path of least resistance i.e. minimising effort.

Social Conformance: There might be an element of social conformance [27]. People might think that "everyone else is happily using these cards, so it must be ok". This was found to be a predictor of non-protective behaviour in another study [31] and might also be the case here. A variety of different ways of paying contactlessly are emerging (e.g. Apple Pay) and their diffusion might be convincing people that the risks *must* be acceptable.

5.2 In Summary

It is unlikely that one of these explanations, in isolation, explains what we observed. There are probably elements of these that come together, and each respondent will be influenced to different degrees. We are aware of both the positive and possible negative consequences of making the costumers more aware of their rights. Still, we argue as it is their right, they should know about it and get the information in an easy and understandable manner.

5.3 Consequences

Banks might have poor motivation to ensure that the contactless card usage liability is clear. Without clarity, customers might be less interested in asking for a refund for contested transactions, especially since the amount is likely to be to small in comparison to the required effort to make a claim. This might change if banks were to state the zero liability legislation. On the other hand, this might well encourage customers to engage in fraudulent behaviors by claiming refunds for non-fraudulent transactions. It is indeed possible for customers to abuse their rights to claim refunds. However, banks have improved their fraud detection systems over the last few years to prevent such fraudulent actions. This means that the risks of such behaviors, in comparison to the profits, are relatively low. Another side effect of more accurate liability knowledge might be that the customers would exercise less care to secure their cards, as they know any contested transactions will be refunded. Even so, we argue that the effort required to get a new card and reporting anomalous incidents is currently too high. If incidents of stolen debit cards increase it is likely that banks would engage in more intensive investigations when people attempt to claim for contested transactions. They might well be biased in favour of claiming gross negligence instead of refunding money as the legislation mandates.

5.4 Limitations:

There are a number of limitations in this study. The first is the small number of participants. This made it impossible for us to carry out statistical analyses of the results. Yet we did gain valuable insights from our qualitative analysis. The second limitation is that we only surveyed UK participants. This was a deliberate choice because we wanted to maximise our chances of getting enough participants for our study, and the UK is a major user of contactless payment cards.

6 Related Literature

A number of changes are occuring in the European financial landscape, due to the introduction of PSD2, which further strengthens customer rights related to different payment methods. Steenot [28] reviewed changes relating to liability and concluded that liability has been reduced, especially in cases of payments that do not require strong authentication. Strong, in this case, refers to the need for two factor authentication. This will not only change online shopping, but also the liability related to unauthorised contactless transactions, because no second factor is required.

This situation will create more competition and leave the banks to respond. Cortet *et al.* [9] suggest four possible strategies to react to this situation: (1) comply, (2) compete, (3) expand, and (4) transform. Whichever way, it will influence the financial landscape. It is important to keep customers' trust during this period of change. The introduction of new payment systems such as the contactless one clearly provide greater levels of convenience but might also trigger suspicion. Polasik *et al.* [25] demonstrated that contactless payment is faster than any other payment methods and people do indeed favour convenience.

Lumpkins and Joyce [17] and Akinyokun and Teague [1] explored NFC systems that enable the transfer of money. Lumpkins and Joyce [17] created a collection of payment methods, what they are and how they work. Their opinion is that NFC is the next step into the future and will eliminate paper currency and plastic credit cards. The ultimate goal of rolling out this new method, based on these papers, is the eventual replacement of hard cash across society. It is likely that this will be pushed even harder now that COVID-19 related concerns are discouraging the use of cash[5].

An interesting study by Brett [3] investigated how the adoption of contactless payment affects and their impact on our spending behaviours. The main findings were a reduced sense of guilt and more purchases of smaller goods, as it is easier to pay for them contactlessly. The main reason is that spending this way does not quite feel like spending real money.

[5] https://forum.thaivisa.com/topic/1152818-covid-19-could-cash-be-helping-to-spread-the-coronavirus/

Research has also been undertaken to investigate making the method more secure by exploring further ideas for verification [2, 12]. Alhothaily *et al.* [2] introduced a new verification method for cardholder by using a multi possession-factor authentication with an integrated distance bounding technique. This adds an additionallayer of security and prevents many different attacks. Gunson *et al.* [12] studied the perception of single and two-factor authentication methods in automated telephone banking. They used a one-time pass code generated using a hardware security token to add additional security level. The user perceived the two-factor authentication as more secure, but, on the downside, the usability reduced.

Akinyokun *et al.* [2] analysed NFC-enabled mobile wallets and contactless payment cards and also explored the EMV and ISO standards for contactless payments. Their examination highlighted inconsistencies between the two standards which, in their words, are disconcerting and might compromise the integrity of contactless transaction payments.

We were not able to find any other studies into the mental models of those who use contactless payment systems.

7 Conclusion

Contactless payments are the ultimate convenience in daily shopping — allowing a shopper to pay with a tap of a card. Yet it also seems risky because the holder of the card does not necessarily need to be the owner of the bank account. Cards get misplaced and stolen, and contactless cards appear, at first, to be the thief's greatest enabler. However, this has been anticipated and the latest legislation forces banks to accept liability when fraudulent transactions occur.

We carried out this research to determine whether UK citizens, as one of the countries with the longest history of contactless card usage, are aware of their zero liability in this respect. We discovered that there was generally a low level of awareness of who carried the liability for fraudulent transactions. It seems that people will use contactless cards, even if they think they themselves are liable if other people use their cards to defraud them.

We suggest a few explanations for our findings. We believe that consumer rights organisations in all countries where PSD2 applies ought to do more to highlight the actual liability attribution so that customers are more aware of their rights and can claim the money from their banks if they are defrauded.

References

1. Akinyokun, N., Teague, V.: Security and privacy implications of NFC-enabled contactless payment systems. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. p. 47. ACM, Reggio Calabria, Italy (2017)
2. Alhothaily, A., Alrawais, A., Cheng, X., Bie, R.: Towards more secure cardholder verification in payment systems. In: International Conference on Wireless Algorithms, Systems, and Applications. pp. 356–367. Springer (2014)

3. Aljawder, M., Abdulrazzaq, A.: The effect of awareness, trust, and privacy and security on students' adoption of contactless payments: An empirical study. International Journal of Computing and Digital Systems **8**(6) (2019), http://dx.doi.org/10.12785/ijcds/080614
4. BBC: UK's cash system 'will collapse without new laws' (2020), https://www.bbc.co.uk /news/business-51550061 Last accessed: 07 July 2020)
5. de Best, R.: Payment methods in Europe - Statistics & Facts (Mar 8, 2019), https://www.statista.com/topics/3946/digital-payment-methods-in-europe/ Last accessed 08 July 2020
6. Brügger, A., Morton, T.A., Dessai, S.: "Proximising" climate change reconsidered: A construal level theory perspective. Journal of Environmental Psychology **46**, 125–142 (2016)
7. Champion, V.L.: Instrument development for health belief model constructs. Advances in Nursing Science **6**(3), 73–85 (1984). https://doi.org/https://doi.org/10.1097/00012272-198404000-00011
8. Cohen, J.: A coefficient of agreement for nominal scales. Educational and Psychological Measurement **20**(1), 37–46 (1960)
9. Cortet, M., Rijks, T., Nijland, S.: Psd2: The digital transformation accelerator for banks. Journal of Payments Strategy & Systems **10**(1), 13–27 (2016)
10. European Parliament: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) (Dec 2015), http://data.europa.eu/eli/dir/2015/2366/oj/eng Code Number: 337 Library Catalog: EUR-Lex
11. Financial Fraud Action UK: Fraud the facts 2017 (2017), https://www.financialfraudaction.org.uk/fraudfacts17/ Last accessed 17 March 2020
12. Gunson, N., Marshall, D., McInnes, F., Morton, H., Jack, M.: Usability evaluation of dialogue designs for voiceprint authentication in automated telephone banking. International Journal of Technology and Human Interaction (IJTHI) **10**(2), 59–77 (2014)
13. Hancock, A.M., Jorgensen, B.L., Swanson, M.S.: College students and credit card use: The role of parents, work experience, financial knowledge, and credit card attitudes. Journal of Family and Economic Issues **34**(4), 369–381 (2013)
14. Jones, R.: Once it was touch and go, now contactless is a new-wave revolution (2016), https://www.theguardian.com/money/2016/sep/10/contactless-cards-wave-pay-oyster-london-use Last accessed 08 July 2020
15. Kosse, A.: The safety of cash and debit cards: a study on the perception and behaviour of Dutch consumers. International Journal of Central Banking **9**(4), 77–98 (2013)
16. Likert, R.: A technique for the measurement of attitudes. Archives of Psychology **22**(140), 55 (1932)
17. Lumpkins, W., Joyce, M.: Near-Field Communication: It Pays: Mobile payment systems explained and explored. IEEE Consumer Electronics Magazine **4**(2), 49–53 (2015)
18. McClenahan, C., Shevlin, M., Adamson, G., Bennett, C., O'Neill, B.: Testicular self-examination: a test of the health belief model and the theory of planned behaviour. Health Education Research **22**(2), 272–284 (2006)
19. McHugh, M.L.: Interrater reliability: the kappa statistic. Biochemia Medica: Biochemia Medica **22**(3), 276–282 (2012)
20. Mendes-Da-Silva, W., Nakamura, W.T., Moraes, D.C.d.: Credit card risk behavior on college campuses: evidence from brazil. BAR-Brazilian Administration Review **9**(3), 351–373 (2012)
21. Miles, A.: Perceived severity (2008)
22. Norman, P., Boer, H., Seydel, E.R.: Protection motivation theory. Predicting Health Behaviour **81**, 126 (2005)

23. Payments News: First Fully Integrated Contactless Payment System in UK (2008), https://web.archive.org/web/20140302142640/http://www.paymentsnews.com/2008/03/first-fully-int.html Last accessed 08 July 2020
24. Van der Pligt, J.: Risk perception and self-protective behavior. European Psychologist **1**(1), 34–43 (1996)
25. Polasik, M., Górka, J., Wilczewski, G., Kunkowski, J., Przenajkowska, K., Tetkowska, N.: Time efficiency of point-of-sale payment methods: Empirical results for cash, cards and mobile payments. In: International Conference on Enterprise Information Systems. pp. 306–320. Springer, Wroclaw, Poland (2012)
26. Renaud, K., Dupuis, M.: Cyber security fear appeals: unexpectedly complicated. In: Proceedings of the New Security Paradigms Workshop. pp. 42–56. ACM, Costa Rica (2019)
27. Sarbin, T.R., Hardyck, C.D.: Conformance in role perception as a personality variable. Journal of Consulting Psychology **19**(2), 109 (1955)
28. Steennot, R.: Reduced payer's liability for unauthorized payment transactions under the second payment services directive (psd2). Computer Law & Security Review **34**(4), 954–964 (2018)
29. The UK Cards Association: How secure are contactless card payments? (2015), http://www.theukcardsassociation.org.uk/contactless_consumer/ContactlessSecurity2015.asp Last accessed 08 July 2020
30. The UK Cards Association: 10 Years of Chip and PIN: 2006 to 2016 (2016), http://www.theukcardsassociation.org.uk/news/10yearschipandpinnews.asp Last accessed 08 July 2020
31. Volkamer, M., Gutmann, A., Renaud, K., Gerber, P., Mayer, P.: Replication Study: A Cross-Country Field Observation Study of Real World PIN Usage at ATMs and in Various Electronic Payment Scenarios. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS). pp. 1–11. ACM (2018)
32. Which: Contactless cards (2019), https://www.which.co.uk/money/banking/banking-security-and-new-ways-to-pay/new-ways-to-pay/contactless-cards-ah1q15s797hb Last accessed 08 July 2020
33. Zipf, G.K.: Human behavior and the principle of least effort. Addison-Wesley Press (1949)