Are Payment Card Contracts Unfair?

Steven J. Murdoch[1], Ingolf Becker[1], Ruba Abu-Salma[1], Ross Anderson[2], Nicholas Bohm[3], Alice Hutchings[2], M. Angela Sasse[1], and Gianluca Stringhini[1]

[1] University College London (UCL)
[2] Computer Laboratory, University of Cambridge
[3] Foundation for Information Policy Research

Abstract. Fraud victims are often refused a refund by their bank on the grounds that they failed to comply with their bank's terms and conditions about PIN safety. We, therefore, conducted a survey of how many PINs people have, and how they manage them. We found that while only a third of PINs are ever changed, almost half of bank customers write at least one PIN down. We also found bank conditions that are too vague to test, or even contradictory on whether PINs could be shared across cards. Yet, some hazardous practices are not forbidden by many banks: of the 22.9% who re-use PINs across devices, half also use their bank PINs on their mobile phones. We conclude that many bank contracts fail a simple test of reasonableness, and 'strong authentication', as required by the Payment Services Directive II, should include usability testing.

1 Introduction

Many research papers on payment security focus on the technical mechanisms used to prevent fraud. Yet, these often fail, and consumer confidence in payment systems depends on whether fraudulent transactions can be reversed, or the victim reimbursed. If a customer disputes a transaction, and there is no evidence that the merchant colluded, the question may be simply whether the bank gives the customer a refund. Will the bank be able to hide behind its contract terms in theory, and will it do so in practice?

Fifteen years ago, Bohm, Brown and Gladman surveyed the terms and conditions that banks were imposing on customers in the rush to put banking services on-line [2]. They found some bank contracts said that a customer who accepted a password for on-line banking would be liable for any transaction the bank claimed was made with that password, regardless of whether she had actually made it. This was a huge change from the law on cheques, where a forged signature is null and void, so banks cannot make customers liable for forged cheques by their terms and conditions. The new electronic banking contracts subtly shifted the burden of proof to the customer.

So, where are we fifteen years later? In the US, regulations require that disputed consumer transactions be refunded, unless the bank can show that the customer actually performed the transaction, or authorised someone else to do

J. Grossklags and B. Preneel (Eds.): Financial Cryptography 2016, Barbados, February 2016. Springer LNCS.

so. In the EU, the 2007 Payment Services Directive ruled that customers are entitled to a refund unless they have been "grossly negligent" in complying with the security procedures set out in the contract with their bank. Thus, banks may be permitted to refuse a refund if the customer fails to follow security guidelines correctly; and even in the USA, a bank might claim that a customer who had let a thief get hold of their card and PIN had authorised them to debit the account.

This might be a reasonable line to take, but only if the bank's contract terms are fair. So, have banks been able to cheat by setting unreasonable rules (e. g., 'choose a password you can't remember and don't write it down')? Or, are their security rules so vague that in the case of dispute, they can always claim that the customer is in breach? In this project, we try to find out.

We examine UK banking terms and conditions in the context of national and EU legislation. We focus on card-present payments and ATM withdrawals because the fraud risk of these transactions falls on the banks, maximising the incentive for customers to be refused a refund. The most reported cases involve a card being stolen (resulting in £59.7m fraud in the UK in 2014 [11]), counterfeited (£47.8m), or intercepted in the post (£10.1m). We exclude card-not-present (e. g., Internet) transactions (£331.5m), as their fraud risk falls on the merchant.

The vast majority of card-present transactions in the EU now require a PIN. In these cases, the bank may claim that the customer must have been grossly negligent in protecting it. Hence, we study how people actually use cards and PINs. We are interested in whether customers can practicably comply with typical bank contract terms, and whether they actually do in reality.

2 Legal and Regulatory Context

Banking contract terms are regulated everywhere. In the US, Federal Reserve regulations E and Z limit consumer liability for fraudulent debit and credit transactions at $50 (unless for debit transactions the customer did not promptly notify the bank of a lost or stolen card, in which case the limit is $500). Liability does not depend on whether the customer was negligent, and the only way to refuse a refund is to argue that the customer actually authorised the transaction or authorised someone else to perform it. In practice, fraud victims are generally refunded unless the bank suspects they are in cahoots with the merchant.

Practice in the EU was harmonised in 2007 by the Payment Services Directive (PSD), which states that customers are not liable for unauthorised transactions when their card is not stolen, and liability would be capped at €150 if it was. However, these limitations do not apply if the customers "failed with intent or gross negligence to fulfil one or more of his obligations under Article 56", which requires that customers comply with banking terms and conditions and, in particular, to "take all reasonable steps to keep its personalised security features safe". So, what counts as 'reasonable'?

European banks typically use the "gross negligence" exception when they choose to deny a refund, but its definition is left to national rules and practices.

As an example, banks commonly state that it is gross negligence to write down a PIN and keep it with the card. However, in practice, for a customer to be held liable, it is only necessary for the adjudicator to believe that gross negligence is, on the balance of probabilities, the most likely explanation.

The PSD requires that there be a means of adjudicating disputes without going to court. This was considered necessary because many European countries practice 'costs shifting', whereby the loser of a civil case pays the winner's costs, which could far exceed the sums in dispute.

The UK adjudicator is the Financial Ombudsman Service, from whose decisions we can see what they consider to be gross negligence. For example, in one case [5], a stolen debit card was used, and while the customer denied writing down the PIN, the bank records showed that the correct card and PIN had been used. The adjudicator observed that the customer had not used the card on the day (reducing the likelihood of shoulder-surfing), and concluded that the most likely explanation for the transactions was that the PIN was kept with the card. The customer was, therefore, held liable.

In one of the few UK cases to get to court [7], the judge also found that the most likely explanation for disputed ATM transactions was that either the customer had made the transactions, or the customer allowed them through intent or negligence. This decision was based on expert witness testimony from the bank, stating that there had never been a breach of the Chip and PIN system at an ATM, the disputed transactions were near the customer's home, and the total disputed amount did not exceed the available balance of the account. The customer was refused a refund and ordered to pay £15,000 of the bank's costs.

Of course, there are other explanations for how the PIN could have been obtained in both of these cases; the same PIN could have been used on another card or on the customer's mobile phone, or the PIN check could have been bypassed technically [8]. The outcome may turn on whether the adjudicator believes the bank or the complainant, which in turn may depend on their access to independent expertise.

The facts that people tend to choose PINs that are easy to guess, and that they tend to set the same PIN on multiple cards, mean that guessing a PIN is possible for about 1 in 11 stolen wallets [3], but a bank could argue that this is only a result of poor PIN choice and still amounts to gross negligence. Therefore, we examine guidance given to customers, to see if customers are set sufficiently clear and consistent rules with which they can reasonably be expected to comply.

3 Review of Banking Terms and Conditions

We surveyed the terms and conditions of a number of banks. We looked for instructions or advice on how users should handle the PINs associated with their cards. As an example, we consider HSBC [6], one of the big British banks.

PIN memo clauses. Banks' terms of service often provide guidance on writing down and recording PINs. HSBC forbids its users from writing PINs down anywhere, except in an "obfuscated" fashion that others cannot easily reconstruct.

It stipulates: "*Never writing down or otherwise recording your PINs and other security details in a way that can be understood by someone else*". It is not specified whether it is the PIN that should not be understood, or the connection between the PIN and the card.

PIN change clauses. Some banks tell customers whether they can change their PINs, and how to choose a PIN. HSBC's rules are concise, but general: "*These precautions include ... not choose security details that may be easy to guess*".

PIN re-use clauses. Many banks have rules on whether a customer can re-use a PIN for multiple cards. HSBC states that customer precautions include "*keeping your security details unique to your accounts with us ...*". This is actually in conflict with the advice given earlier by the UK banks' trade association, which recommends customers to change all their PINs to the PIN issued for one of their cards. The UK banks have also taken the necessary technical measures to ensure that cardholders from any bank can change their PIN at any ATM.

PIN advice clauses. Common conditions include not telling the PIN to any third party. HSBC stipulates that the PIN advice letter must be destroyed immediately after receipt: "*Safely destroying any Card PIN advice we send you immediately after receipt, e. g., by shredding it ...*".

4 Survey of Payment Card PIN Usage

We conducted an on-line questionnaire study of how people use payment cards, and, in particular, how many PINs they have, and how they are remembered. We also investigated their behaviour towards storing, resetting and sharing PINs.

4.1 Questionnaire Setup

The questionnaire was set up using LimeSurvey[4], and the participants were recruited using Prolific Academic[5]. We restricted submissions to British residents aged 18 or over. Participants were paid £1.50 for successfully completing the questionnaire. The questionnaire took five minutes on average to complete. We received 241 (out of 250) valid responses, and verified that the IP address used was from the UK in all but 5 cases[6].

Questions that required categorical responses by the participants had a set of predefined choices as well as a free text response field. The predefined choices were sourced from a small qualitative preliminary study. In nearly all cases the participants did not make use of the free text response field.

[4] `www.limesurvey.org`

[5] `www.prolific.ac`

[6] IP address geo-location has a non-trivial error rate, but this still confirms that our sample is predominantly from the UK, as intended.

4.2 Results

Of the participants, 61% are female and 39% are male. The age of the participants spans 18 to 71 years, with a mean of 31.2. Our participants are better educated than average bank customers: 38% have at least an undergraduate degree (BSc, BA or similar), while a further 17% have postgraduate education. 30% did not attend higher education, and a third of these (10%) have a General Certificate of Secondary Education (GCSE) as their highest qualification. 49% of the participants are employed; a further 13% are self-employed; 24% of participants are students; only 13% are unemployed.

Table 1. Distribution of participants' PINs

	0	1	2	3	4	5	6	7	8	9	mean
4 digits	1	88	65	41	31	8	5	1	1	0	2.28
5 digits	233	5	3	0	0	0	0	0	0	0	0.05
6 digits	228	8	4	1	0	0	0	0	0	0	0.08

The participants report having 1 to 9 payment cards (mean = 2.53). This contrasts with the number of 4-digit, 5-digit, and 6-digit PINs each participant has in Table 1. The vast majority of customers have only 4-digit PINs, but the mean number of PINs is 2.28 – statistically significantly lower than the mean number of cards per customer (dependent t-test, $t = -4.38$, $p < 0.0001$).

Table 2. Frequency of usage of participants' PINs

	4-digit PINs									5-digit PINs			6-digit PINs			
	#1	#2	#3	#4	#5	#6	#7	#8	Sum	#1	#2	Sum	#1	#2	#3	Sum
Every day	34	0	0	1	0	0	0	0	35	0	0	0	1	1	0	2
Several times a week	117	30	3	3	0	0	0	1	154	1	0	1	5	2	1	8
Once per week	59	35	12	3	0	0	0	0	109	2	1	3	0	0	0	0
Once per month	21	37	24	8	3	0	0	0	93	4	2	6	3	2	0	5
Several times a year	6	24	24	12	2	2	1	0	71	1	0	1	3	0	0	3
Once a year or less	1	14	10	10	4	1	0	0	40	0	0	0	1	0	0	1
Never	2	12	14	9	6	4	1	0	48	0	0	0	0	0	0	0

Table 2 analyzes how often participants use their PINs. No participant had more than eight 4-digit PINs, or more than two 5-digit ones or three 6-digit ones. We see at once that as the number of PINs increases, their usage drops. Only one participant uses more than one unique PIN on a daily basis. About half (48%) of the PINs are used at most once a month, and PIN #4 is used on average around twice a year. This supports the bank industry 'folk wisdom' that if you want customers to use cards other than their main card you must let them change their PINs.

Table 3. Source of 4-digit participants' PINs

	#1	#2	#3	#4	#5	#6	#7	#8	Sum
I chose it myself	75	56	28	15	3	3	1	0	181
Assigned to me, I decided not to change it	161	94	56	31	11	3	1	0	357
Assigned it to me, I am not allowed to change it	4	2	3	0	1	1	0	1	12

Table 3 documents PIN change, and we see that two-thirds of PINs are left as their default. Interestingly, there is no correlation between frequency of PIN use (Table 2) and PIN origin (Table 3). Virtually all participants are allowed to change their PINs in the UK. The details for 5- and 6-digit PINs have been omitted here for brevity. We also investigated the reasons for PIN change. Of the participants that set their own PIN, 61% reported changing their PIN on first receipt, a further 23% stated they changed their PIN because they felt it was compromised, but only 6% claimed to change their PIN on a regular basis.

Our participants keep their PINs for a long time: Only 13% of PINs were changed in the last year, with over 39% having been in use for over 5 years.

Remembering PINs. A quarter of the participants reported forgetting a 4-digit PIN at least once. Of these, 48% remembered or retrieved their PIN themselves, 24% were issued with a new PIN, and 15% used the bank's services to retrieve their PIN. Finally, 10% did not bother retrieving the forgotten PIN; half of these said they transferred their money to a different account.

Table 4. Location of written down PINs by participants. 79 (32.9%), 4 (50.0%), and 0 (0.0%) wrote down their 4-, 5-, and 6-digit PINs, respectively.

	4-digit	5-digit	6-digit	Sum
On the card	1%	0%	0%	1%
I kept the original PIN slip	0%	0%	0%	0%
On paper – kept in desk	16%	25%	0%	17%
On paper – kept in wallet	10%	0%	0%	10%
In a notebook/diary/planner, etc.	41%	25%	0%	40%
File on computer	10%	25%	0%	11%
File on phone	42%	25%	0%	41%

As many banks insist that PINs must not be written down, we decided to investigate this in reality. Table 4 describes our participants' strategies towards writing down PINs. Not a single participant kept the original PIN mailer. The prevailing method of PIN storage is on mobile phones – typically disguised as a phone number. 13% of the participants use a mnemonic for 4-digit PINs, the most common technique being the derivation of the PIN from a specific date. (This was also reported by Bonneau et al. [3].)

Table 5. A variety of locations where participants' PINs are re-used. 55 (22.9%), 0 (0.0%), and 1 (7.7%) re-used their 4-, 5-, and 6-digit PINs, respectively.

	4-digit	5-digit	6-digit	Sum
Unlocking mobile phone	49%	0%	0%	48%
Burglar alarm	2%	0%	0%	2%
Voicemail	15%	0%	0%	14%
SIM card unlock	7%	0%	0%	7%
Unlocking computer	5%	0%	100%	7%
On-line Banking	25%	0%	0%	24%

PIN re-use. 16% of our participants stated they use the same PIN on many payment cards; when a PIN was re-used, it was used on 2.8 payment cards on average, with the maximum being 9 cards! PINs were also used in a variety of other locations (Table 5): 22.9% of participants are re-using their 4-digit payment card PINs, half of whom use a payment card PIN to unlock their mobile phone.

Table 6. Sharing of PINs by participants. 102 (42.5%), 2 (25.0%), and 1 (7.7%) shared their 4-, 5-, and 6-digit PINs, respectively.

	4-digit	5-digit	6-digit	Sum
Stranger	0%	0%	0%	0%
Family member	37%	0%	100%	37%
Flatmate (if accommodation shared)	3%	0%	0%	3%
Spouse/partner	75%	100%	0%	74%
Casual acquaintance	1%	0%	0%	1%
Close friend	14%	0%	0%	13%

PIN sharing. Finally, an impressive 42.5% of our participants share their PINs, in many cases with more than one person (Table 6). Sharing predominantly occurs with a spouse or partner (32% of participants) or other family members (16%), but also, in some cases, close friends (6%).

5 Conclusion

In general, it is difficult for customers to be certain whether they are complying with bank rules, as these rules lack detail and can even be contradicted. For example, HSBC prohibits PIN re-use, whereas the UK bank trade body recommends this [4]. Vague and contradictory guidance puts customers in a weak position should a bank claim that a disputed transaction must have been caused by a failure to comply with its rules.

Our survey of PIN use confirms the practical difficulty of remembering PINs. Customers are commonly asked to remember four or more PINs, some of which they only use every month at most. The combined effect of forgetting over time [10], as well as interference between the different PINs remembered [1], makes unaided recall of these PINs a difficult task. In one study after 3 weeks, the majority of participants were unable to remember a PIN, and even after 1 week 45% had forgotten it [9]. In current usage scenarios, customers can only cope by re-using PINs or writing them down.

The 4-digit PIN system worked adequately in the environment for which it was originally designed: a single regularly-used ATM card. Today's usage scenarios are different, but the mechanism, and terms and conditions, remain unchanged. Not considering the usability implications pushes customers towards insecure PIN practices banned by the banks' contracts. Each PIN re-use allows a thief another 6 guesses, and mobile phone touchscreens can give away PIN digits directly. Not all customers can be expected to disguise PINs securely, but remembering an infrequently-used PIN is impractical without some kind of assistance. Customers who do not comply with their banking contract are then blamed for security failures that are actually caused by a system that is not fit for purpose.

The successor to the PSD – PSD II – adds a requirement that banks must use strong authentication for payments. This is defined as "authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent". The European Banking Authority is responsible for evaluating proposed solutions. Our study shows that an authentication technique must be evaluated in the context of normal use (e. g., multiple payment instruments, some used infrequently) and only considered strong if real people can use it in the course of their normal life. Otherwise, it risks becoming just another excuse for some banks to shift fraud liability to their customers.

Banks want customers to use multiple cards, so they can earn more fees. Regulators want people to use multiple cards to enhance competition. Secure methods for using a single PIN (or two-factor authentication technique) over all devices would remove the need for the ad-hoc coping mechanisms we see in the survey. Alternatively, to take the US approach, enshrine strong consumer protection in law; expect banks to use fraud detection to manage risks and absorb the residual fraud; and by increasing trust, increase transaction volumes and, thus, increase revenues and profits overall.

Data availability. The survey data used in this paper can be downloaded from `http://dx.doi.org/10.14324/000.ds.1473489`.

Acknowledgements. We are grateful to Adam Beautement, Brian Glass, Boris Hemkemeier and Kat Krol for helpful discussions. Steven J. Murdoch is supported by The Royal Society [grant number UF110392]; Ingolf Becker is supported by the Engineering and Physical Sciences Research Council [grant number EP/G037264/1].

References

1. Anderson, M.C., Neely, J.H.: Interference and inhibition in memory retrieval. In: Memory. Handbook of Perception and Cognition, pp. 237–313. Academic Press, 2 edn. (1996)
2. Bohm, N., Brown, I., Gladman, B.: Electronic commerce: Who carries the risk of fraud. Journal of Information, Law and Technology (2000)
3. Bonneau, J., Preibusch, S., Anderson, R.: A birthday present every eleven wallets? The security of customer-chosen banking PINs. In: Financial Cryptography and Data Security. pp. 25–40. Springer. (2012)
4. Bowerman, M.: Radio interview with APACS spokesperson. BBC Radio Merseyside. (19 February 2007)
5. Financial Ombudsman Service: Ombudsman news (March/April 2014), case 116/2, `http://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/116-disputed-transactions.html`
6. HSBC, UK: General, current accounts and savings accounts terms and conditions. (accessed on 1/9/2015)
7. Kelman, A.: Job v Halifax PLC (not reported) case number 7BQ00307. In: Digital Evidence and Electronic Signature Law Review. vol. 6. (2009)
8. Murdoch, S.J., Drimer, S., Anderson, R., Bond, M.: Chip and PIN is broken. IEEE Symposium on Security and Privacy. pp. 433–446 (May 2010)
9. Renaud, K., Ramsay, J.: How helpful is colour-cueing of PIN entry? arXiv:1407.8007 [cs]. (Jul 2014)
10. Squire, L.R.: On the course of forgetting in very long-term memory. Journal of Experimental Psychology: Learning, Memory, and Cognition. 15(2), 241–245. (Mar 1989)
11. UK Cards Association: Plastic fraud figures (2015), `http://www.theukcardsassociation.org.uk/plastic_fraud_figures/index.asp`