International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms

Ingolf Becker* Alice Hutchings† Ruba Abu-Salma*
Ross Anderson† Nicholas Bohm‡ Steven J. Murdoch*
M. Angela Sasse* Gianluca Stringhini*

Abstract

We set out to investigate how customers comprehend bank terms and conditions (T&Cs). If T&Cs are incomprehensible, then it is unreasonable to expect customers to comply with them. An expert analysis of 30 bank contracts across 25 countries found that in most cases the contract terms were too vague to be understood; in some cases they differ by product type, and advice can even be contradictory. While many banks allow customers to write PINs down as long as they are disguised and not kept with the card, 20% of banks do not allow PINs to be written down at all, and a handful do not allow PINs to be shared between accounts. We test our findings on 151 participants in Germany, the US and UK. They mostly agree: only 35% fully understand the T&Cs, and 28% find that sections are unclear. There are strong regional variations: Germans find their T&Cs particularly hard to understand, but Americans assume harsher T&Cs than they actually are, and tend to be reassured when they actually read them.

1 Introduction

The ability to revoke fraudulent bank payments, or at least reimburse the victims of fraud, is presented as one of the primary selling points of the consumer banking system and, particularly, for payment cards. This consumer-friendly feature is also used as a justification for the higher transaction fees that accompany card payments compared with payment systems where transactions are final, such as cash and cryptocurrencies. However, whether a fraud victim actually gets their money back will depend on bank practices and ultimately the contract between the bank and its customers, which may in turn depend on national or international legislation. In order to get a refund, a fraud victim may need to demonstrate that they have followed security practices set out in their contract with the bank, but these terms may be hard to understand and may only

*University College London (UCL)
†University of Cambridge
‡Foundation for Information Policy Research

Workshop on the Economics of Information Security (WEIS), 13–14 June 2016, Berkeley, CA, USA

partially match (if not conflict with) the understanding that customers have developed from the bank's more prominent promotional material, as well as the affordances of its system.

This paper builds upon previous research into the fairness of bank terms and conditions, particularly how the rules adapt to changes in technology. The first study, by Bohm, Brown and Gladman [21], reviewed the terms and conditions of online banking services, which at the time were still in their infancy. They found that some bank contracts stipulated that a customer accepting an online banking password also accepted liability for any transactions that the bank claimed were made with that password, regardless of whether the customer had actually made them. Bohm et al. pointed out that the liability had shifted; a forged handwritten signature is null and void in most countries, so a bank cannot make customers liable for forged cheques using its terms and conditions. The banks took advantage of the technology change to escape nineteenth-century consumer-protection law. In some countries, such as the US, pressure by consumer-rights advocates led to regulations that require disputed transactions to be refunded.

More recent research [41] found that many bank customers do not comply with bank terms and conditions on PIN security: they regularly share, reuse, and write down PINs. Bank rules were also found to lack detail, and in some cases were contradictory. Adapting the concept of a 'security budget' from Beautement, Sasse and Wonham [20], the cost of compliance with terms and conditions (such as the cognitive effort required to remember PINs, the embarrassment of being unable to complete transactions, and the inability to get relatives to run errands) may be so high that millions of customers write down or share PINs anyway, regardless of what the bank contract says.

There is also the issue of affordances; if banks permit customers to change PINs, then they will often change them to the PIN on the most frequently-used account. This may conflict with a contract term specifying that PINs should not be shared across banks. It is technically straightforward for a bank to set the same random PIN on every card issued to a customer, and not let them change it. But, if the card is not the customer's primary card, they may well just not use it. By letting customers change PINs but forbidding some likely PIN changes in the small print, the banks are externalising this tension (and the associated risks) on to their customers. At the regulatory level, there is a tension between direct consumer protection (which might limit PIN change facilities), and the promotion of competition (for which PIN changes are a good thing, otherwise people will be less likely to start using different cards). But to what extent are such issues hidden from the public behind the obscure contract language?

In this research, we first compare bank terms and conditions around the world. We then ask participants if the rules are sufficiently clear, and if they understand the customers' obligations. Adams and Sasse [1] demonstrate, in relation to security practices in the workplace, that ill-conceived and misunderstood policies can result in security breaches. If banking rules similarly cannot be understood, then it is unreasonable to expect customers to comply with them. Furthermore, as disputes are often a matter of the customer saying they did not write down a PIN and keep it with a stolen card, against the bank saying that they must have done so, requiring customers to demonstrate compliance with rules that many people break is an unfair burden of proof. Finally, if the liability shifts to the customer, banks face a less than socially optimal incentive to detect and prevent fraudulent activity on their systems.

2 Review of Banking Terms and Conditions Internationally

2.1 Methodology

In the first stage of this project, we surveyed the terms and conditions of 30 banks operating in 25 countries. The study's scope included Europe (Cyprus, Denmark, Germany, Greece, Italy, Malta, and the United Kingdom), the United States, Africa (Algeria, Kenya, Nigeria, and South Africa), the Middle East (Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, UAE and Yemen), and East Asia (Singapore). No banks were found operating online in Libya or Syria.

Major banks were selected for the study. These are not always the largest banks, as some make their terms and conditions available only to account holders. The types of documents reviewed also differed for each bank, as some had separate terms and conditions for telephone and Internet banking, as well as credit and debit cards and current accounts. All the documents reviewed were downloaded from the banks' websites and related to personal (not business) accounts.

The terms and conditions were reviewed to identify instructions or advice on security. This included how users should handle the PINs associated with their cards, as well as telephone and Internet banking credentials. The documents reviewed were in English, German, Italian, Arabic, and Greek. The authors include native speakers of these languages, who coded and translated the relevant sections. The documents were coded in accordance with the categories set out in table 1. The terms and conditions for accounts that adhere to Sharia Law, which prohibits the charging of interest or making money on savings, were found to have identical security clauses to other personal accounts held within the same bank.

2.2 Results

The terms and conditions relating to PIN, telephone banking and Internet banking are considered in turn. A summary of the findings relating specifically to customer obligations to secure PINs is shown in table 2.

2.2.1 PIN Writing Clauses

It is very common for banks' terms of service to provide guidelines to their customers on writing down their PIN – 26 banks out of 30 have them. The most common instruction is to keep the written PIN in a different place from the card, and not to write it on the card itself – 15 banks have such a requirement. Only six banks forbid their users from writing the PIN down anywhere. Vague statements are not uncommon: five banks instruct the customer to keep the PIN in a "safe" place. These banks include Ahli United Bank [2], Bank Audi [14], Bank of Baghdad [17], Nedbank [52] and Zenith Bank [57]. Furthermore, three banks (Arab Banking Corp. [11], HSBC [37] and National Bank of Kenya [44]) allow PINs to be written down in an "obfuscated" fashion that others cannot easily reconstruct. In contrast, National Bank of Greece explicitly states that "the Bearer

Category	Description
PINWrite	References to writing down PINs
PINChange	References to changing PINs
PINReuse	References to reusing PINs, whether it be within the same or across different banks
PINAdvice	What to do with the written letter from the bank that contains the PIN
ReceiptsStatements	What to do with the receipts and statements
TelephoneWrite	References to writing down telephone banking access codes
TelephoneChange	References to reusing telephone banking access codes, whether it be within the same or across different banks
TelephoneAdvice	What to do with the written advice from the bank that contains the telephone banking access code
OnlineWrite	References to writing down online banking access codes
OnlineChange	References to changing online banking access codes
OnlineReuse	References to reusing online banking access codes, whether it be within the same or across different banks
OnlineAdvice	What to do with the written advice from the bank that contains the online banking access code
OnlineSecuritySoftware	Requirements to install and keep up to date security software
OnlineNetwork	Use of the network that the customer can access online banking from, including public access points
OnlinePassword	Requirements relating to the use of password managers or saving passwords in the browser
OnlineDevice	Requirements relating to the type or status of devices (e.g., not shared/public access, jailbroken/rooted)

Table 1: Description of coding categories used.

Bank (country)	W	C	R	A	Bank (country)	W	C	R	A
HSBC (United Kingdom)	●	●	●	●	The Association of Banks (Singapore)	●	●	○	●
OCBC (Singapore)	○	●	○	○	Nedbank (South Africa)	●	●	○	○
Zenith Bank (Nigeria)	●	●	○	○	National Bank of Kenya (Kenya)	●	○	○	○
APS Bank Limited (Malta)	●	○	○	●	Danske Bank (Denmark)	●	○	●	●
Monte dei Paschi (Italy)	○	○	○	○	Unicredit (Italy)	●	○	○	○
Sparkassen (Germany)	●	○	○	○	Deutsche Bank (Germany)	●	○	●	○
Volksbank (Germany)	●	○	○	○	Citibank (United States)	●	●	○	○
Ahli United Bank (Bahrain)	●	●	●	○	Commercial International Bank (Egypt)	●	○	○	○
Bank of Baghdad (Iraq)	●	○	○	○	Arab Bank (Jordan)	●	●	○	○
National Bank of Kuwait (Kuwait)	●	●	○	○	Arab Banking Corp. (Algeria)	●	○	●	○
Bank Audi (Lebanon)	●	●	○	○	Bank Muscat (Oman)	●	○	○	○
Bank of Palestine (Palestine)	○	●	○	○	Qatar National Bank (Qatar)	●	●	○	●
National Commercial Bank (Saudi Arabia)	●	○	○	○	National Bank of Abu Dhabi (UAE)	○	○	○	○
Arab Bank (Yemen)	●	●	○	○	National Bank of Greece (Greece)	●	●	○	○
Co-operative Central Bank (Cyprus)	●	○	○	●	Bank of Cyprus (Cyprus)	●	●	○	●

Table 2: Summary of banks' T&Cs related to PIN security. "W" indicates clauses related to writing down and storing a written PIN, "C" indicates clauses related to changing the PIN, "R" indicates clauses related to reusing it, and "A" indicates clauses related to the destruction of the letter from the bank advising of the PIN. A ● indicates that such a clause is present in the terms of service, while a ○ indicates its absence.

is required to: memorize the PIN, not write it down – even in an obscured fashion – on the Card or on any other document . . . " [43].

There are considerable variation in how PINs may be written down, and where recorded PINs may be kept. For example, Arab Banking Corp. in Algeria, HSBC in the United Kingdom, and National Bank of Kenya stipulate the following:

> Never writing the Customer's password or security details down in a way that someone else could easily understand, or allowing anyone to observe the Customer inputting the Customer's password details on any electronic media [11].
>
> Never writing down or otherwise recording your PINs and other security details in a way that can be understood by someone else . . . [36].
>
> If the Customer makes a written record of any PIN Code or security procedure, the Customer must make reasonable effort to disguise it and must not keep it with the card for which it is to be used [44].

It is not specified whether it is the PIN that should not be understood by someone else (such as by using a code to disguise the numbers), or whether it is the connection between the PIN and the card that should not be understood.

In Singapore, OCBC does not appear to specify how customers might record PINs [54], even though its trade association has a Code of Practice which stated that customers should be told that "they should never write the PIN on the card . . . " [13], and the Code of Consumer Banking Practice which states that "you should . . . never write and/or keep record of your PIN together with your card" [12].

A number of other banks are similarly vague about proximity of PIN and card. Here are more examples from Nedbank in South Africa, and Zenith Bank in Nigeria:

> The client must . . . ensure that any record of the PIN is kept separate from the card and in a safe place [52].
>
> The customer . . . undertakes . . . not to write down the Passcode, Accesscode/Password in an open place to avoid third party coming across . . . [57].

Bank Audi [14], Bank of Baghdad in Iraq [17], Bank of Cyprus [18], Deutsche Bank [29], Sparkassen and Volksbank in Germany [31, 26], and UniCredit in Italy [56] state that the PIN should not be stored with or on the payment card. Moreover, Bank of Cyprus [18] states that the PIN should not be recorded or stored on an electronic device that allows it to be identified with the card.

Qatar National Bank provides vague advice [55]: it requested from its customers to only memorize their PINs. On the other hand, a number of banks, including Ahli United Bank in Bahrain [2], Citibank in the United States [22] and National Commercial Bank in Saudi Arabia [50], provide more specific advice. The following appeared under the heading "Security Tips" of Citibank, so is perhaps not binding:

> Keep your Personal Identification Number (PIN), Telephone Personal Identification Code (TPIC) and other codes used to access your accounts secret. Do not tell them to anyone. Do not write them on your Citibank Banking Card or keep them in your wallet or purse ...

The advice from the National Bank of Kenya differs by the type of account. For credit cards, there is only the following vague advice:

> The Card member shall exercise due care to ensure the safety of the Card and the Secrecy of the PIN at all times ... [44].

In contrast, the following requirements are set out for current accounts:

> If the Customer makes a written record of any PIN Code or security procedure, the Customer must make reasonable effort to disguise it and must not keep it with the card for which it is to be used ... [45].

Arab Bank in Jordan and Yemen [6, 8], Bank Muscat in Oman [15], APS Bank in Malta [4], Co-operative Central Bank of Cyprus [18], National Bank of Greece [43], and National Bank of Kuwait [47] forbid customers from writing down the PIN anywhere at all. For example, the following is from APS Bank:

> Not writing down the PIN on the Card or anywhere, or disclosing it to anyone else including the Police officers and/or the Bank's personnel ... [4].

Danske Bank in Denmark does not allow the PIN to be kept with the card. It does offer "PIN memorisers" for recording obfuscated PINs:

> Do not keep your PIN with your card or write it on your card. For security reasons, you should memorise your PIN. If you are unable to do so, keep it in a safe place, preferably a PIN memoriser. PIN memorisers are available free of charge from any of our branches ... [27].

Finally, a few banks do not provide guidelines to customers on how PINs might be written down, such as the Bank of Palestine [19], Monte dei Paschi di Siena in Italy [39], and the National Bank of Abu Dhabi in the United Arab Emirates [42].

2.2.2 PIN Change Clauses

Half of the banks (15 out of 30) specifically indicate whether they allow users to change their PIN, or provide advice on how to choose a PIN. The rules varied across banks, with HSBC being concise, but general:

> These precautions include ... not choosing security details that may be easy to guess ... [36].

One bank (Nedbank in South Africa) requires customers to change their PIN on receipt of a payment card, with no stated restrictions on PIN choice:

> The client shall ... immediately change any temporary PIN and password allocated by the bank for the purpose of allowing the client to access the services for the first time ... [52].

One other bank (Bank of Cyprus [18]) mandates customer PIN change, but also provides advice on how to select a PIN. The Ahli United Bank in Bahrain [2], and OCBC in Singapore [54], as well as the Association of Banks in Singapore [13] set out requirements for selecting a strong PIN, telling users not to use telephone numbers, birthday dates, personally identifiable information, or certain sequences of numbers as their PINs. For example:

> The Customer may change the Customer's ATM-PIN from time to time. The Bank shall be entitled at the Bank's absolute discretion to reject any number selected by the Customer as the Customer's substitute ATM-PIN without giving any reason ... When selecting a substitute ATM-PIN, the Customer shall refrain from selecting any series of consecutive or same or similar numbers or any series of numbers which may easily be ascertainable or identifiable with the Customer ... [54].

It is odd to see such a requirement in a contract, as ATM systems support a "denied PIN list" and the bank could simply add PINs such as 1234, 2345, ..., 9999 to this list to block them completely, along with commonly-blocked values such as 0000.

Seven other banks (Ahli United Bank [2], Arab Bank [6], Bank Audi [14], Bank of Palestine [19], Citibank [22], National Bank of Kuwait [47], and Zenith [57]) suggest their users change their PINs periodically. Finally, National Bank of Greece states that the "Bearer can replace [the PIN] with another number of his choice at any of the Bank's ATMs, following the on-screen instructions" [43].

Citibank tells its customers not to choose PINs that begin with a zero:

> The PIN you select must consist of four numbers and cannot begin with a zero ... [22].

We have not been able to test whether this condition is enforced by Citibank ATMs on their own customers. We also do not know if the banks that do not set PIN-change conditions (including banks in Algeria, Cyprus (Co-operative Central Bank) Denmark, Egypt, Germany, Iraq, Italy, Kenya, Malta, Nigeria, Oman, Saudi Arabia and the UAE) offer a PIN change facility or not.

2.2.3 PIN Reuse Clauses

Even fewer banks provide advice on not reusing a PIN for multiple cards – only five out of 30. For example, HSBC states that customer precautions include "keeping your security details unique to your accounts with us ..." [36]. This is actually in conflict with the advice given earlier by the UK banks' trade association which recommended customers to change all their PINs to the PIN issued for one of their cards. The UK banks allow cardholders from any bank to change their PIN at any ATM.

Danske Bank allows customers to have a unique PIN sent to them, or to use a PIN for a personal card that has already been issued by the same bank [27]. The bank does

not stipulate whether the PIN has to be unique to them, and in any case it does not appear to offer a PIN change facility. Arab Banking Corp. explicitly specifies that the PIN chosen has to be unique to the bank, while Ahli United Bank only states that the PIN used must be unique, under the heading "Security Information" [2].

2.2.4 PIN Advice Clauses

Seven banks stipulate that the original letter containing the PIN (the PIN advice letter) must be destroyed. HSBC demands this "immediately after receipt":

> Safely destroying any Card PIN advice we send you immediately after receipt, e.g., by shredding it ... [36].

In Cyprus (Co-operative Central Bank [23]), Malta (APS Bank Limited [4]), and Qatar (Qatar National Bank [55]), the banks allow customers to memorise the PIN before destroying the advice:

> Memorise the PIN and immediately destroy the document ... [23].

> Destroying the PIN notification sent to him by the Bank immediately after memorising the PIN ... [4].

> Upon receiving your credit/debit card, memorise the PIN and destroy the PIN mailer ... [55].

The customers of Danske Bank [27] have no set time limit:

> You must also remember to destroy the letter containing your PIN [27].

2.2.5 Clauses Relating to Bank Statements and Receipts

Fourteen of the 30 banks include clauses relating to bank statements and/or receipts. Overall, these banks have notably differing requirements regarding the retention of bank statements and receipts. Only HSBC in the UK and the National Bank of Kuwait insist that customers shred their bank statements if they dispose of them:

> Keeping card receipts and other information about your account containing personal details (such as statements) safe and disposing of them safely. People who commit fraud use many methods such as searching in dust bins to obtain this type of information. You should take simple precautions, such as shredding paper containing such information [36].

> Save receipts: Remember to take your receipts and shred them before discarding. It is best not to ask for receipts at all [46].

The advice from the National Bank of Kuwait that receipts should not be asked for differs with other banks, which requires customers to retain receipts for reconciliation with bank statements [2, 14, 15]. The Qatar National Bank specifically states:

> Ensure that you received a copy of the receipt and keep it safe . . . Never throw away your transaction receipts [55].

This requirement regarding the retention of records also differs across banks. The Arab Bank in Jordan requires customers to "ensure that your account records are properly disposed" [5], while at the other extreme, the Arab Banking Corp. in Algeria recommends that "the customer prints off and keeps or electronically saves all electronic statements" [11]. Three banks (Monte dei Paschi di Siena [39], Unicredit [56] and National Bank of Kenya [44]) provide vague statements, such as inviting their users to apply "common sense" when dealing with card transactions, or using "due care".

2.2.6 Clauses Relating to Telephone Banking Security

Clauses relating to telephone banking security are found for 13 of the 30 banks. Some are found in contracts specifically for telephone banking, while others include this in their general terms and conditions, or combined the two. Until July 2015, HSBC's general UK contract set out requirements for safeguarding security details, including "PINs, security numbers, passwords or other details including those which allow you to use PIB [Personal Internet Banking] and TBS [Telephone Banking Service]" [37]. Further requirements for telephone banking were found in a document called *Banking Made Easy*. These documents were later revised, with the duplication removed. Now, the terms and conditions specify that customers are required to follow the advice in the separate *Banking Made Easy* brochure. Some of HSBC's requirements for PINs also apply here: the credentials cannot be written down in a way that can be understood by someone else, and they must be unique to the bank. The security code for telephone banking is a 6- to 10-digit number created by the customer registration, so there is no advice letter to destroy.

The OCBC [54] and Monte dei Paschi di Siena [40] do not specify whether telephone banking credentials may be written down, or whether the credentials have to be unique. However, customers are permitted to change their telephone banking PIN. The OCBC specifies that:

> When selecting a substitute T-PIN, the Customer shall refrain from selecting any series of consecutive or same or similar numbers of any series of numbers that may easily be ascertainable or identifiable with the customer [54].

As stated earlier, Citibank specifies that the 'Telephone Personal Identification Code (TPIC)' should not be written on the card or kept in the customer's wallet or purse. It also volunteers that the customer could set up a TPIC by calling the bank [22]. No limits on code selection are discussed, and no demand found for the TPIC to be unique.

Many banks' terms and conditions relating to safeguarding PINs are also applicable to telephone banking, including that credentials should not be written in an 'open place' [57], should not be kept with the card for which they are to be used [45], and should be changed periodically and be kept confidential and private [7, 19, 9, 51].

2.2.7 Clauses Relating to Internet Banking Security

As with telephone banking, some banks have specific contracts for Internet banking, whilst others include this in general contracts. Some go still further to impose conditions on the security of the network, the security of the device including the use of security software, and the use of online password managers or browsers to store credentials.

The most onerous conditions are set out by HSBC in the UK. Under its Personal Internet Banking Terms and Conditions [38], credentials for Internet banking must not be written down in a way that can be understood by someone else, they cannot be easy to guess, and they have to be unique to the bank. The customer must always access Internet banking by typing the address into the web browser and use antivirus, antispyware and a personal firewall. If accessing Internet banking from a computer connected to a LAN or a public Internet access device or access point, they must first ensure that nobody else can observe, copy or access their account. They cannot use any software, such as browsers or password managers, to record passwords or other security details, apart from a service provided by the bank. Finally, all security measures recommended by the manufacturer of the device being used to access Internet banking must be followed, such as using a PIN to access a mobile device.

The OCBC, in Singapore, insists that the card and PIN must not be kept together, yet elsewhere that PINs must be memorised and not recorded anywhere. Customers were advised not to repeat any digits in the 6-digit PIN more than once, that it should not be based on the User ID, telephone number, birthday or other personal information, that it should not be used for different websites, applications or services, and that it should be changed 'regularly'. Customers of the Singapore bank also have to install antivirus, antispyware and firewalls, and ensure they were updated and patched. File and printer sharing also have to be disabled, and customers cannot use public or Internet cafe computers. Browsers cannot be used to store credentials. What's more:

> 10. Do not install software or run programs of unknown origin ...
> 14. Do not use a computer or device which cannot be trusted ...
> 16. You are advised not to access Online Banking using 'jailbroken' or 'rooted' mobile devices (ie the phone Operating System has been tampered with), as it poses potential risk of malicious software infection [53].

The other banks reviewed do not impose such aggressive restrictions. Clauses specific to online banking include: using a firewall, antivirus and/or antispyware software [2, 3, 5, 9, 10, 14, 16, 24, 25, 30, 32, 42, 43, 48, 50]; using a modern browser [10, 40]; patching the browser and/or operating system [2, 10, 16, 24, 25, 30, 32, 42, 43, 50]; not saving passwords in password managers or browsers [11, 16, 24, 42, 48, 50]; not using public-access computers [2, 7, 9, 16, 24, 42, 49, 50]; encrypting wireless networks [24]; clearing the cache after each banking session [16]; using a password to access the computer [50]; and disabling file and printer sharing capabilities [50]. The National Bank of Kuwait [48] and the Commercial International Bank in Egypt refers to particular firewalls and antivirus programs:

> Common commercial examples include Zone Labs, www.symantec.com and Computer Associates. The leading free firewall is "Zone Alarm" from Zone

> Labs and there are many others to choose from. Zone Alarm is now used on over 20,000,000 PCs and has been awarded the PC World 2003 "World Class Award" for Best Firewall [48].
>
> There are many effective programs to choose from, but the most common commercial products include McAfee, Symantec (Norton) and Sophos. It is also possible to obtain free anti-virus protection. A search for 'free anti-virus' on Google will provide a list of the most popular [24].

Danske Bank stipulates that customers should not leave the mobile phone on which they receive codes and their payment card number with others, including members of their household [28].

3 Survey

The second contribution of this research is a cross-cultural study of the understanding and interpretation of banking terms and conditions (T&Cs). As we have previously seen, there are significant differences in the legal background of banking between countries. However, these may appear rather theoretical. In order to distill out the practical effects of the banks' contracts, we conduct a survey with participants from Germany, the United Kingdom and the United States. Consumer protection for fraudulent transactions in Germany and the UK is governed by the same law, the EU Payment Services Directive (PSD), whereas US disputes are governed by the more consumer-friendly federal regulations E and Z. The PSD allows banks to refuse refunding a customer if the most likely explanation for the fraud is considered to be that the customer was grossly negligent in complying with bank security rules. Regulations E and Z require that customers be refunded in almost all circumstances, and demonstrating gross negligence is not sufficient to refuse a refund. The aims of this survey are threefold:

1. identify the perceptions and prejudice of participants towards banking terms and conditions;
2. measure the ability of our participants to understand the banks' terms and conditions and act on them;
3. on a country specific basis and as a cross-cultural study.

3.1 Survey Design

The survey is divided into four stages. We begin with some demographics on the participants as well as some statistics on the payment methods our participants use. This is followed by two scenarios on the conflicts between the T&Cs and customers. The scenarios are sourced from the UK Financial Ombudsman newsletter [33, 34, 35]. The Financial Ombudsman is an arbitration service that was set up by the UK banks as an alternative to using the court system to resolve disputes between financial institutions and customers, and later became the dispute resolution service designated under the PSD. Its quarterly newsletter publishes examples of its recent dispute resolutions. After

a number of questions regarding the scenarios has been asked, we introduce a section of relevant terms and conditions on payment safety and fraud (see section 3.3). We ask the participant a number of questions to gauge their understanding of the terms and conditions on a following page, without allowing access to the terms.

We then reintroduce the two scenarios and again enquire on their interpretation of the outcome of the scenario, but this time giving the participant access to the relevant terms and conditions.

Most of the responses in the survey are collected using free-text responses. There are several reasons for choosing this method: As we are interested in the perceptions of the participants and their understanding of the terms and conditions, we had to remove any form of prompts in order to get the unbiased responses. These free-text responses are then manually grouped using Thematic Analysis. The raw counts are normalised, in most cases by the number of participants per country. As each participant may have mentioned multiple themes, each theme may range between 0% and 100%.

The participants for this study were recruited using Prolific Academic[1]. The survey took on average 18 minutes to fill out, and we paid each participant £2.50. We trialed the study on German, British and American native speakers and ran an initial online pilot that helped us resolve some minor ambiguities.

Conducting the survey in two languages across three countries posed several challenges. Firstly, the financial legislation is very different between the EU and the US (the US being significantly more consumer-friendly). This had a direct impact on the responses, but we were nevertheless able to measure the impact of the treatment of the terms and conditions on the two scenarios. Second, there are significant cultural differences regarding privacy and data protection between the three countries.

The survey and the two scenarios were translated into German by a native speaker, and checked by a second native speaker in order to ensure that the intent of the questions was preserved as closely as possible. Minor changes were also made between the British English and American English version in order to aid comprehension.

3.2 The Scenarios

Our two scenarios were presented in a random order to the participants. The order they were shown in did not lead to any statistically significant variations in answers. The scenarios shown below are those shown to the participants in the UK.

3.2.1 Scenario 1: Card Loss

The first scenario is based on a typical story of theft [33]. The scenario reads as follows:

> Miss K travels to work on the Tube. When leaving the Tube at the destination station, Miss K notices that her purse is missing. In the Tube station is a police office, where she reports her purse as stolen. When she gets to work, she phones her bank to cancel her debit card. But, by this time, the thief has made several large cash withdrawals using the card.

[1] `https://www.prolific.ac/`

In the original article, the Financial Ombudsman decided that the most likely reason the thief could withdraw cash is that Miss K stored her PIN with the card. The Ombudsman concluded that Miss K had likely been grossly negligent and is denied a refund. We do not tell the participants this outcome.

3.2.2 Scenario 2: Phone Scam

The second scenario is based on a combination of Ombudsman News stories [34, 35]. The scenario reads as follows:

> Mr L received a phone call from his bank. The person he spoke to said there had been some "suspicious activity" on his account, and asked him if he had made certain purchases. When Mr L said he hadn't, the person on the phone said that he should call a different department at the bank straight away to sort the problem. Mr L called the number on the back of his debit card. The person he spoke to asked him some security questions and then confirmed that suspicious activity had taken place. They said that Mr L should immediately transfer all the money from his account to a different account, and he gave him the details of that account over the phone. Mr L transferred the money straight away.
>
> When Mr L told his partner what had happened, she was worried. She suggested he call his bank to check he'd done the right thing. It turned out that Mr L had been the victim of a scam. The fraudster had put a technical fix in place so that when Mr L ended the first call and rang the number for his bank, he'd actually just reconnected with the fraudster.

In this scenario, the Ombudsman ruled that Mr L should not be reimbursed, as he was deemed to have authorised the transaction. There is a large number of similar cases, which all vary slightly on the exact manner the fraudulent transaction is processed. In some cases, the Ombudsman decides in favour of the customer; in many others, she does not.

3.3 The Terms and Conditions

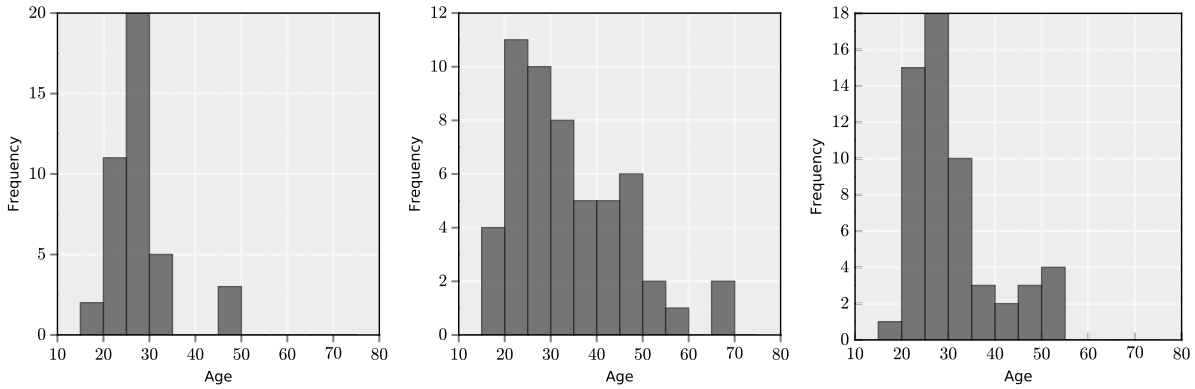
It is infeasible to have our participants work through an entire document of Terms and Conditions as part of a study, as these documents range from 20 to 40 pages. In order to get a realistic assessment of the ability of our participants, we avoided presenting only the passages most relevant to the study, but left whole paragraphs intact. For the UK, we chose HSBC's General Terms and Conditions [37], and in particular Section *9. Important Security Information*, and Section *27.5 Liability for Unauthorised Transactions*. As discussed previously, HSBC's T&Cs are representative of T&Cs in the UK.

For the American participants, the survey focused on Citibank's Client Manual Consumer Accounts [22]. In particular, we chose the sections on *Lost or Stolen Banking Cards or Other Access Devices and Unauthorised Electronic Transactions* and *Security Tips*. Again, our choice of the bank followed from our analysis in section 2.

Following the same argument, we chose the Terms and Conditions for Debit Cards of Deutsche Bank [29] for Germany. Here, we focused on Section *6. Geheimhaltung der*

persönlichen Geheimzahl (PIN) (Keeping your PIN secret), Section *12. Erstattungs- und Schadensersatzansprüche des Kontoinhabers* (Reimbursments and claims for damages of the account owner), and Section *13. Haftung des Kontoinhabers für nicht autorisierte Kartenverfügungen* (Liability of the account owner for unauthorised card charges).

3.4 Demographics



(a) Country: DE (b) Country: UK (c) Country: US

Figure 1: Histogram of our participants' age

Gender	DE	UK	US
Female	24%	52%	27%
Male	73%	48%	71%
Other	2%	0%	2%

Table 3: Gender of our participants

We recruited 151 participants in total: 41, 56 and 54 participants from the DE, UK and US respectively. An overview of the age and gender of all recruited participants can be found in figure 1 and table 3. There are some surprising differences in these demographic distributions between the three countries, considering that all participants were sourced from the same platform. There is a strong gender bias of around 3:1 in Germany and the US. The participants in the UK are, however, gender-balanced.

Figure 1 highlights the age distributions between the participants from the three countries. We checked the participants' location by geo-locating their IP address used to access the survey. IP geo-location is far from accurate, however, all but 3 participants' IP addresses matched their declared country. We decided to include the answers from these participants, as the answers were well-written and showed no other anomalies.

The mean ages across the three countries are 27.0, 33.7 and 30.4 years for the DE, UK and US respectively. The variance varies widely with 43.2, 160.6 and 95.5 respectively. In general, Prolific Academic seems to have the most representative demographics for the UK.

Employment Status	DE	UK	US
Employed	22%	48%	57%
Student	63%	30%	14%
Unemployed	2%	4%	12%
Self-employed	7%	13%	16%
Retired	2%	6%	0%
Prefer not to say	2%	0%	0%

Table 4: Employment demographics of our participants

Highest Qualification	DE	UK	US
GCSE Level education (e.g., GCSE, O-Levels or Standards) or lower	7%	15%	0%
A-Level education (e.g., A, AS, S-Levels, Highers)	24%	11%	12%
Some undergraduate education (e.g., No completed degree)	10%	19%	18%
Degree/Graduate education (e.g., BSc, BA)	32%	35%	43%
Postgraduate education (e.g., MSc, MA, MBA, PhD)	22%	19%	16%
Vocational education (e.g., NVQ, HNC, HND)	5%	0%	5%
Other	0%	2%	4%

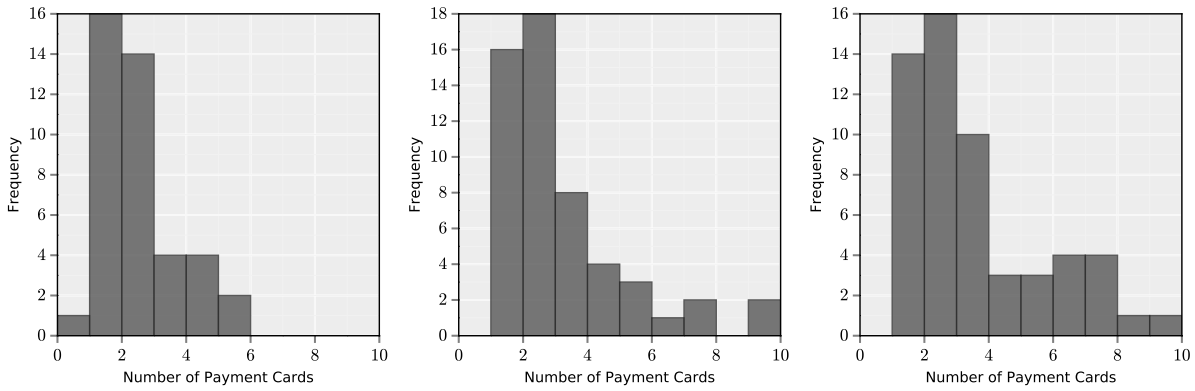
Table 5: Educational demogprahics of our participants

There are distinct differences in employment across the US, DE and UK, as can been seen in table 4. Almost all our participants claim to be native speakers in our study; 100%, 92% and 92% for the DE, UK and US respectively. There is an above-average distribution of educational statistics, which shows over 50% of our participants from each of the countries have finished at least a bachelor's degree of equivalent (see table 5). The translation of education levels is not straightforward, which may explain the 0% value for GCSE level education in the US. Two participants revealed that they had learning disabilities.

It is obvious that our participants' demographics could be better aligned for a cross-cultural study. Unfortunately Prolific Academic does not offer the functionality to sample participants to a specific demographic distribution. However, while there are strong differences in the employment demographics (table 4) and gender, the age and educational demographics (figure 1 and table 5) are fortunately similar.

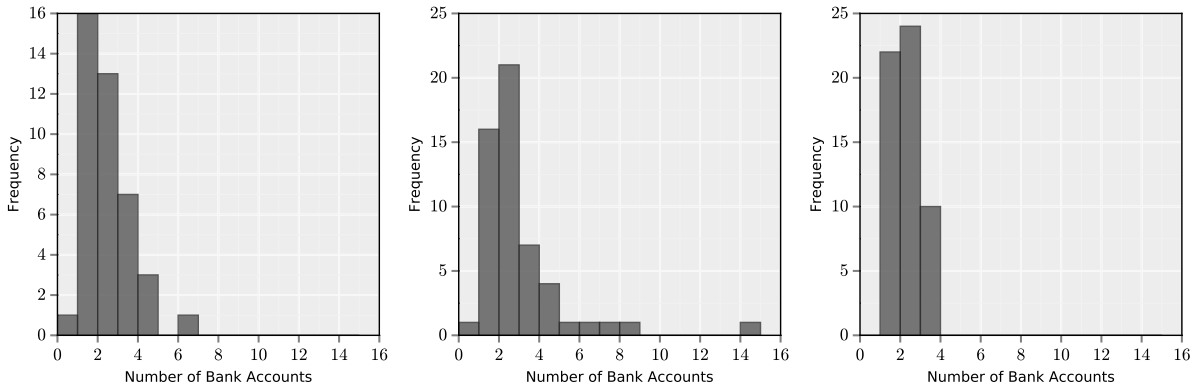
3.5 Payment Demographics

In order to meaningfully compare the responses to our questions, we have to check that the participants have similar levels of financial development. One measure is the number of bank account and payment cards. Figure 2 shows 3 histograms for the number of payment cards our participants have in the DE, UK and US respectively. The means are here 2.0, 2.7 and 3.1 respectively. Similarly, figure 3 displays the distribution of bank accounts of our participants with means 2.0, 2.5 and 1.8 respectively. While many credit cards are prevalent in the US, our participants there also have the smallest number of bank accounts.



(a) Country: DE (b) Country: UK (c) Country: US

Figure 2: Participants' number of payment cards



(a) Country: DE (b) Country: UK (c) Country: US

Figure 3: Participants' number of bank accounts

Frequency	DE	UK	US
Every day	0%	19%	20%
Several times a week	63%	65%	55%
Once per week	22%	13%	20%
Once per month	5%	2%	4%
Several times per year	7%	2%	0%
Once per year or less	0%	0%	2%
Never	2%	0%	0%

Table 6: Frequency of use of any of our participants' payment cards

Furthermore, we investigate the frequency of payment card use. Here, the UK participants use their cards the most, followed by the Americans. No participant in Germany uses a payment card on a daily basis (table 6), yet payment card penetration rates are still high. Virtually, no participant manages a week on average without using a card.

3.5.1 Fraud Experience

Frequency	DE	UK	US
No	88%	72%	66%
Yes	12%	28%	34%

Table 7: Have you ever experienced fraudulent transactions or incidents on any of your payment cards or bank accounts?

We hypothesise that people who have been a victim of fraud previously are more likely to pay attention to the details of payment contracts. We ask the participants if they have been victims of payment fraud, and to explain the experience to us. In table 7, we list the frequency of fraud experiences of our participants.

Code	DE	UK	US
Fraud identified at a later stage	28.6%	55.0%	60.7%
Transaction before card blocked	0.0%	0.0%	3.6%
Transaction after card blocked	0.0%	5.0%	0.0%
Transaction blocked by bank	42.9%	30.0%	21.4%
Other/No idea where fraud occurred	42.9%	30.0%	42.9%
Offline transaction	14.3%	15.0%	17.9%
Online transaction	14.3%	40.0%	14.3%
Cash withdrawal	0.0%	0.0%	7.1%
Card stolen	0.0%	5.0%	7.1%
Online account hacked	0.0%	5.0%	0.0%
New card	28.6%	30.0%	32.1%
Full refund	14.3%	80.0%	82.1%

Table 8: Thematic analysis of the description of fraud experienced by participants. The first four codes describe the identification of fraud, the next six codes describe the type of fraud, and the last two describe the follow-up actions that happened.

In order to get a complete description of the events, we solicited free-text responses. We analysed these responses using Thematic Analysis, and the results can be seen in table 8. The table is divided into three sections: fraud identification, type of fraud, and resolution. As these were manually annotated free-text responses, the absolute percentages are approximate, but the relative differences are worth noting. There is a clear trend in the stage where fraud is identified: in Germany, more fraud is identified automatically than noticed by the customers at a later stage. This is reversed for the UK and the US, where almost two thirds of fraud is identified by the customer. For American customers, this may be an annoyance, but a minor one: Federal Regulations E & Z ensure that the customer will get his money back. In the UK, this may be a greater worry as the refund is dependent on whether the bank considers you to have been 'grossly negligent'.

3.6 Scenario Overview

Question	DE	UK	US
Scenario 1: Card Loss	41.5%	81.5%	76.8%
Scenario 1: Card Loss after T&Cs	70.7%	66.7%	96.4%
Scenario 2: Phishing	31.7%	37.0%	35.7%
Scenario 2: Phishing after T&Cs	43.9%	46.3%	42.9%

Table 9: Percentage of participants that say that the money should be returned in each of the scenarios. McNemar's test is significant with $p < 0.05$ for both Scenario 1: Card Loss and Scenario 2: Phishing.

In the following sections 3.7 and 3.8, the participants consider the two scenarios in two different combinations: once before seeing the relevant terms and conditions, and once afterwards. Each time they are asked if they think the protagonist should be reimbursed by the bank and why they think so. The results of the binary question can be found in table 9. We find that in all but one case, the participants are more likely to have the protagonist reimbursed after reading the terms and conditions. This is statistically significant with $p < 0.05$ for both scenarios using the McNemar's test for binary variables. We will now consider each of these four conditions in isolation, and analyse the qualitative responses.

3.7 Scenario 1: Card Loss

For each of the two settings, there are two sets of answers to consider: those that argue for the reimbursement of the protagonist, and those against it.

3.7.1 Prior to Revealing Terms and Conditions

Code	DE	UK	US
Banks have good security that should have prevented fraud	0.0%	4.5%	0.0%
Depending on the T&C of the bank	0.0%	0.0%	9.3%
Insurance will compensate her	0.0%	2.3%	14.0%
People are protected from fraud by the bank	35.3%	38.6%	48.8%
She did not authorise the transaction	17.6%	6.8%	2.3%
The theft was reported swiftly	52.9%	50.0%	41.9%
Yes, because the bank can prove it wasn't her, due to CCTV at ATM	5.9%	11.4%	7.0%

Table 10: Thematic analysis of the answers in support of reimbursement in Scenario 1: Card Loss.

Tables 10 and 11 show the results of the "Card Loss" scenario before revealing the terms and conditions. The respondents who supported reimbursement gave a wide range of reasons (table 10). The most recurring reasons across the German, UK and US surveys are: (1) the theft was reported immediately, cited by 52.9%, 50.0% and 41.9% of respondents respectively, and (2) banks are expected to protect their customers from fraud, with 35.3%, 38.6% and 48.8%. Additionally, some of the UK respondents (4.5%) were more specific, and said that good security measures are deployed by banks to defend against fraud. 17.6% of the German respondents said that Miss K did not authorise the transaction and, hence, she should be reimbursed; only 6.8% and 2.3% mentioned the same reason in the UK and US surveys. Another interesting reason for reimbursing Miss K is that it can be easily proven that she did not make the transaction because CCTV cameras are widely deployed at ATMs; this reason was mentioned in all three surveys. Only 2.3% of the UK respondents believe that the insurance company is responsible for compensating Miss K, whereas 14.0% provided the same reason in the US survey. Interestingly, only US participants, with about 9%, mentioned that reimbursement depends on Miss K's bank terms and conditions.

Code	DE	UK	US
Common perception that the customer loses	4.2%	20.0%	23.1%
Debit, as opposed to credit, cards do not have fraud protection	0.0%	10.0%	23.1%
Don't know/unsure	4.2%	0.0%	0.0%
Her mistake	25.0%	20.0%	30.8%
Her purse is not insured, thief must be caught	0.0%	20.0%	0.0%
Money cannot be retrieved once it leaves someone's account	4.2%	20.0%	23.1%
She may have been grossly negligent	29.2%	10.0%	0.0%
She waited too long before notifying her bank	58.3%	10.0%	0.0%

Table 11: Thematic analysis of the answers not in support of reimbursement in Scenario 1: Card Loss.

Table 11 presents the reasons provided by the respondents who did not support the reimbursement across all three surveys. About 58% of the German respondents mentioned that Miss K waited too long before reporting the incident to her bank; only 10.0% of the UK respondents provided the same reason, whereas this reason was not mentioned by any of the Americans. Some of the German (29.2%) and UK (10.0%) respondents believed she was grossly negligent without explaining what "gross negligence" means. Another reason given is that it was her mistake because she forgot her purse in the train; this reason was shared by many respondents, namely 25.0% (DE), 20.0% (UK) and 30.8% (US). Interestingly, only 4.2% of the German respondents believed that a bank customer is destined to lose, but a much higher percentage provided the same reason in the UK (20.0%) and US (23.1%) surveys. Also, the same distribution was found for another reason: that once the money leaves someone's account, it cannot be retrieved. Another interesting perception is that debit, as opposed to credit, cards are not protected against fraud; this reason was given by 10.0% of the English surveyed and 23% of the US ones. Finally, 20.0% of the Brits mentioned that since Miss K's purse is not insured, the only way to retrieve her money is to catch the thief (as if they simply assumed that the bank

would not bear the loss). About 4.0% did not know (or were not sure about) whether Miss K should be reimbursed or not.

3.7.2 After Revealing Relevant Terms and Conditions

Code	DE	UK	US
However, it's hard for debit, as opposed to credit cards	0.0%	0.0%	1.9%
Insurance will reimburse her	0.0%	0.0%	1.9%
She reported the card stolen within the time limits	31.0%	61.1%	98.1%
She used the landline to report the incident	0.0%	2.8%	0.0%
The card was stolen, the transaction was unauthorised, it's fraud	86.2%	63.9%	7.4%
Yes, if it can be proved that the card was stolen	0.0%	16.7%	0.0%

Table 12: Thematic analysis of the answers in support of reimbursement in Scenario 1: Card Loss, after the participants have seen the T&Cs.

After revealing the terms and conditions to our participants, we were interested in their comprehension. Table 12 presents the reasons provided by the respondents who believed that Miss K should be reimbursed (after reading the terms and conditions). About 86% of the German respondents and 64% of the UK ones believed that the victim should get a refund because the card was stolen, and the transaction was unauthorised; only 7% of the Americans provided this reason. On the other hand, 98.1% of the Americans mentioned that Miss K reported the incident within the time limits specified by the Terms and Conditions; this reason was given by 31.0% and 61.1% of Germans and Brits. No other reasons were mentioned in the German survey. In contrast, 16.7% of UK respondents believed that it can be proved that the card was stolen. One of the Brits reported that Miss K used the land-line to report the incident (2.8%). Another was unsure whether Miss K would be reimbursed or not. One American said that insurance can actually reimburse Miss K, and another believed it would be possible to retrieve the money if the stolen card was a credit card, and not a debit card.

Code	DE	UK	US
It is difficult to recover the money	0.0%	11.1%	100.0%
PIN might have been written down in her purse	16.7%	66.7%	0.0%
She was grossly negligent as she lost her card and failed to immediately cancel it	83.3%	38.9%	0.0%

Table 13: Thematic analysis of the answers not in support of reimbursement in Scenario 1: Card Loss, after the participants have seen the T&Cs.

In contrast, table 13 displays the reasons mentioned by the participants who said that Miss K should not be reimbursed, after seeing the terms and conditions. Most Germans (83%) said Miss K was grossly negligent because she lost her card and failed to cancel it swiftly. The same reason was provided by 39% of Brits. In contrast, most Brits (67%)

believed that Miss K must have written her PIN down on a piece of paper, and left that in her purse; only 17% of Germans reasoned this way. All the Americans who opposed reimbursement said that it is difficult to recover the money; only 11.1% of the Brits gave this as their reason for refusing a refund.

3.7.3 Analysis

The arguments from both sides are interesting, considering that the protagonist's claim in the UK was denied due to the Ombudsman deciding that the most likely explanation for the fraud was that she had stored her PIN with her card and hence was grossly negligent. Only 10% of the UK participants who argued against the protagonist being reimbursed gave this reason. This changes drastically after the participants have read the terms and conditions: now two thirds of those against reimbursement give the same reason as the Ombudsman.

We do not know how this case would have been decided in Germany and the US, but we can analyse the change in their perceptions, nevertheless. In the case of Germany and the UK, the perceptions in favour of reimbursement did not change with the revelation of the terms and conditions. In the US, however, there was a significant shift to 'She reported the card stolen within the time limits' from 41.9% to 98.1%. This strongly suggests that our participants read the the terms and conditions carefully.

In contrast to the American T&Cs, the German terms do not give a definite time frame as to when a transaction has to reported as fraudulent. This may have motivated the high response rate in table 13.

3.8 Scenario 2: Phone Scam

3.8.1 Prior to Revealing Terms and Conditions

Code	DE	UK	US
Banks have good security that should have prevented fraud	53.8%	50.0%	55.0%
Don't know/unsure	0.0%	0.0%	5.0%
He was tricked into phoning the number on the back of his card	30.8%	35.0%	15.0%
If the fraud can be proven	15.4%	10.0%	10.0%
The bank should be be insured/reverse the transaction/be ethical	30.8%	35.0%	25.0%
The scammer can be someone working in the bank	0.0%	0.0%	10.0%

Table 14: Thematic analysis of the answers in support of reimbursement in Scenario 2: Phone Scam.

Table 14 presents the reasons provided by the participants who initially supported reimbursing Mr L in the "Phone Scam" scenario. A common theme across all three surveys is that banks should secure their systems properly; this was the view of 53.8%,

50.0% and 55.0% of DE, UK and US respondents. Second, banks should be insured, should be ethical, and should be able to reverse any unauthorised transaction; support was 30.8%, 35.0% and 25.0%. Third, Mr L was tricked, but did the right thing by phoning the number on the back of his debit card (30.8%, 35.0% and 15.0%). Additionally, 15.4% of the Germans said that as long as fraud can be proven, Mr L should get his money back; this reason was mentioned by 10% of Brits and Americans each. Only Americans (with 10.0%) said that Mr L should be reimbursed because the scammer might have been a bank employee.

Code	DE	UK	US
Banking accounts have no protection	7.1%	11.8%	16.7%
Banks tend not to care about customers	3.6%	8.8%	5.6%
Difficult to recover the money	7.1%	5.9%	16.7%
Don't know/unsure	0.0%	0.0%	2.8%
His own fault, he was scammed	75.0%	8.8%	19.4%
May have acted fraudulently	17.9%	64.7%	33.3%
No one can tell the difference between the fraudster and the real customer	0.0%	17.6%	30.6%

Table 15: Thematic analysis of the answers not in support of reimbursement in Scenario 2: Phone Scam.

Table 15 shows the reasons given by the respondents who initially opposed reimbursing Mr L. Three quarters of Germans believed that it was his fault because he fell for a scam; in contrast, most Brits (64.7%) said that Mr L had most probably acted fraudulently; this reason was given by one-third of the Americans but only one tenth of the Germans. Another one-third of the Americans said that Mr L cannot be reimbursed because no one can differentiate between him and the scammer. Some other reasons were mentioned as well across all surveys, such as bank accounts are generally not protected, banks do not tend to care about their customers, and it is hard to recover the money.

3.8.2 After Revealing Relevant Terms and Conditions

After revealing the relevant terms and conditions, the respondents who supported reimbursement provided the reasons shown in table 16. 27.8% in the DE survey said that Mr L would not have thought that a technical fix was in place; this reason was given by almost one-half of the UK participants but only 8.3% of US ones. Another 22% of DE respondents said the Mr L followed the security procedures documented for a phone call, a view shared by 28.0% and 4.2% in the UK and US surveys. Most of the US respondents believed Mr L should be reimbursed because he was not the one who authorised the transaction, a view shared by only 16.7% of Germans but 28.0% of Brits.

Finally, table 17 documents the reasons for why Mr L should not be reimbursed. About 60% and 50% in the DE and UK surveys believed that Mr L was grossly negligent; 28% of the US participants who opposed reimbursement provided the same reason. Another common reason is that Mr L transferred the money himself, given by 35% (DE), 38% (UK) and 44% (US). Other reasons included that Mr L was the one who gave his de-

Code	DE	UK	US
Don't know/unsure	16.7%	0.0%	4.2%
He could not have been aware that there was a technical fix in place	27.8%	48.0%	8.3%
He followed the security procedures as documented for telephone calls	22.2%	28.0%	4.2%
He was not grossly negligent	22.2%	20.0%	0.0%
If the fraud can be proven	0.0%	4.0%	0.0%
It is not an authorised transaction	16.7%	28.0%	75.0%
Phishing not covered by the T&C	16.7%	8.0%	8.3%
The bank can retrieve the money	0.0%	4.0%	4.2%

Table 16: Thematic analysis of the answers in support of reimbursement in Scenario 2: Phone Scam, after the participants have seen the T&Cs.

Code	DE	UK	US
Difficult to recover the money	8.7%	3.4%	12.5%
Don't know/unsure	4.3%	0.0%	3.1%
He gave his details out on the phone to the fraudsters	13.0%	10.3%	3.1%
It is gross negligence	60.9%	48.3%	28.1%
Mr. L transferred the money himself	34.8%	37.9%	43.8%
Phishing not covered by the T&C	8.7%	0.0%	9.4%

Table 17: Thematic analysis of the answers not in support of reimbursement in Scenario 2: Phone Scam, after the participants have seen the T&Cs.

tails out to the fraudsters, that it is hard to recover the money, and that social engineering attacks, such as phishing are not covered by the bank terms and conditions.

3.8.3 Analysis

In the UK, the Ombudsman decided that the protagonist was not to be reimbursed as he was deemed to have authorised the transaction and has, hence, been grossly negligent. While the majority of participants from the UK shared the view that he should not be reimbursed (table 9), the majority of participants were unable to give the same reason after reading the terms and conditions, they only decided that he had been grossly negligent. There was a significant shift in the opinion of the German participants after reading the T&Cs: Previously the majority had reasoned that 'it was his own fault', but this changed to the more vague but more consistent with the T&Cs view of 'gross negligence' (tables 15 and 17). Interestingly, even though 'gross negligence' is not mentioned in the terms and conditions shown to the American customers, still 28.1% gave this reason (or one to that effect). But, only in the US did the majority of participants gave the same reason as the Ombudsman – although it is uncertain if the decision would have been the same in the US.

Those participants that decided that the protagonist should be reimbursed changed

their reasoning significantly after reading the T&Cs. In Germany and the UK, the previously most frequent response – that the bank should have prevented the fraud (table 14) – does not appear as a reason in favour at all in table 16. Instead, the reason has shifted towards the fact that the customer acted with best intentions, and could not have known that he had been reconnected to the fraudsters after following the prescribed security procedure by calling the number on the back of his card. While the participants in the US initially gave the same reasons as those from the UK and Germany, after reading the terms and conditions the vast majority (75.0%) agree that the protagonist did not authorise the transactions. This must have been a clear feature of the terms and conditions presented to the participants from the US.

3.9 Understanding of Terms and Conditions

The terms and condition documents are by no means accessible, and to be sure that our participants actually spend some time reading them rather than glossing them over, they were shown the terms on a separate page and were instructed to read carefully because they would be asked questions on these terms on the following page. Participants were unable return to the terms page once they had left. On average, the participants spend 204 seconds on reading the T&Cs.

Code	DE	UK	US
Don't know	2.4%	7.4%	7.1%
Notified not quickly enough	19.5%	13.0%	80.4%
Shared details	7.3%	27.8%	3.6%
Violate T&Cs	7.3%	18.5%	1.8%
Fraudulently	0.0%	16.7%	0.0%
Always	7.3%	5.6%	3.6%
If you notice something suspicious	0.0%	0.0%	1.8%
Not kept details safe	19.5%	9.3%	3.6%
Been phished	2.4%	1.9%	0.0%
Gross negligence	53.7%	27.8%	0.0%

Table 18: Thematic analysis of the answers to the comprehension question: "When are you liable for an unauthorised transaction?"

A set of comprehension questions followed on the next page. It seems that many of the participants had never read their bank's terms and conditions before. One comments: "Why am I responsible for closing the door to an ATM lobby as I leave? Why am I being told as a customer to not let people into banks after hours?"

Each of the comprehension questions solicited a free-text answer, and we subjected the responses to Thematic Analysis. In table 18, the participants analyse liability. The responses clearly represent the peculiarities of the contracts: For American customers, the only reason to get a non-fraudulent claim turned down is to miss the deadlines. In contrast, in Germany and the UK, the focus is on gross negligence, with 54% of participants from Germany correctly stating that gross negligence is the reason for becoming liable.

Code	DE	UK	US
Don't know	4.9%	3.7%	12.5%
Carelessness	4.9%	31.5%	46.4%
Not being careful with details	53.7%	48.1%	8.9%
Your fault	2.4%	11.1%	5.4%
Ignoring warnings	2.4%	1.9%	0.0%
Not informing your bank of loss	7.3%	14.8%	14.3%
Negligence beyond reasonable practice	17.1%	9.3%	10.7%
Harmful misconduct	7.3%	0.0%	3.6%
Not following the T&Cs	7.3%	5.6%	0.0%

Table 19: Thematic analysis of the answers to the question: "What is gross negligence?"

Table 19 follows through by diving into the participants' understanding of 'gross negligence'. British and German participants agree that 'gross negligence' is mostly about *being careful with details*, where details may be any form of credentials or cards. Conversely, the participants resident in the US equate it with the more traditional meaning of carelessness – clearly because their T&Cs do not mention 'gross negligence' at all. The more legally correct version of 'harmful misconduct' is mentioned only infrequently.

Code	DE	UK	US
Write down	17.1%	11.1%	26.8%
Change periodically	0.0%	0.0%	21.4%
Memory technique	36.6%	14.8%	16.1%
Use existing/memorable numbers	9.8%	31.5%	14.3%
Choose unique	4.9%	1.9%	0.0%
Just remember it	26.8%	27.8%	25.0%
Write down encrypted	4.9%	3.7%	1.8%
Don't know	7.3%	11.1%	5.4%

Table 20: Thematic analysis of the answers to the question: "What can you do to remember your PIN?"

Next, we asked how one was supposed to remember PINs (table 20). Writing down PINs is more accepted in the US than in Germany or the UK with over a quarter of participants stating that the terms and conditions allowed them to do so. Unfortunately, it was difficult here to find sample terms and conditions whose intentions were actually made clear in the extract. Still further insights can be gained: there is a tendency in the US to change PINs frequently, something that was only mentioned in the extract for the American participants. Interestingly, PIN reuse is seen favourably in the UK with 32% of participants noting it as acceptable – an even higher proportion than we found in previous research [41]. We also note that Germans tend to use memory techniques (36.6%) while Brits are more likely to change their PIN to an existing or memorable number (31.5%). We already noted that the UK banks' association encourages PIN changes, and all banks

provide the facility. However, some banks in Germany do not allow customers to change their PINs at all.

Level	US	DE	UK
Understood nothing	0%	0%	0%
Understood the minority	2%	7%	6%
Understood half of it	4%	12%	2%
Understood the majority	50%	59%	54%
Understood everything	45%	22%	39%

Table 21: How confident are you that you have understood the T&Cs?

In contrast to these tables, we asked the participants to self-judge their own understanding of the terms and conditions. Table 21 shows that the vast majority of participants claimed to understand the majority of the terms although less than a quarter of participants from Germany claimed to understand them fully. Given that our participant pool has above average education, it is likely that most bank customers do not fully understand the contract terms of their bank accounts. However, it should be noted that the subject pool from the US thought they understood their terms to a much greater extent (although they are about equally well-educated). Perhaps the better consumer protection makes them less cautious. It is also noteworthy that after reading the T&Cs, participants actually realised that they had even stronger rights than they thought.

Code	DE	UK	US
Tips useful	0.0%	0.0%	1.8%
All ok	36.6%	51.9%	73.2%
Complicated	29.3%	13.0%	17.9%
Unclear	51.2%	13.0%	19.6%
Abbreviations, special terms	24.4%	25.9%	1.8%
Gross negligence	0.0%	13.0%	0.0%
Negligence limits unclear	0.0%	0.0%	5.4%

Table 22: Thematic analysis of understanding issues of the T&Cs of the participants.

Diving into more detail, table 22 lists the broad themes that the participants were struggling with. What most stands out is that in Germany the T&Cs were branded as unclear, needlessly complicated and full of special terms and abbreviations. One participant noted: "Everything is overcomplicated. The terms actively avoid using clear, simple language." We concur; German T&Cs do actually appear much more difficult to understand than the UK's.

4 Discussion

Fifteen years ago, when online banking was in its infancy, many banks sought to shift liability explicitly by making customers liable for any transaction where they said the

customer's password was used. This led to complaints about liability shifting. The situation now is for banks to give instead a variety of different advice, much of it so waffly that it is unclear how customers are to set about complying with it, or indeed whether their behaviour is likely to be changed by it at all. In some cases, advice given by banking trade associations is contradicted by member banks' small print. In the case of the most aggressive banks (in the UK and Singapore), it is probably infeasible for customers to comply with the stated contract terms, and later work will test this on a panel of representative users.

The more general picture is that banks set out many different ways of blaming the customer in the event of dispute, and create a climate of expectation in which a court or Ombudsman will be tempted to run through the checklist, in effect asking the customer to prove they were not careless. But, rather than a blanket assertion to this effect, the actual argument will usually be one based on the facts of the case where the bank says "Your password was used so you must have been negligent." In the US, where consumer laws are held to discourage such an argument, the bank can argue instead "As your password was used, you authorised this transaction." The exceedingly onerous UK bank terms and conditions are particularly worrisome in this context.

Most developed countries have unfair-contract laws, so the question to ask may be: "are bank contracts fair?" Our initial investigation shows that in many cases they are too vague for a firm view to be taken one way or another, and so an assessment will come down to a study of actual dispute resolution practice. However, where contract terms require user behaviour that is far from normal, a usability assessment may provide an answer; and where a banking association advises customers to change all their cards to the same PIN, while some of its member banks have small print forbidding the practice, that is clearly unfair. The unfairness that results from obfuscation does vary, however. Americans tend to be reassured when they actually read their bank contract terms and conditions, while most Germans find them too hard to understand. Overall, the data we have collected gives a number of insights into the effects that the differing approaches to bank regulation have had on consumer expectations between countries. There is much more work to be done here, by researchers and regulators alike.

Data Availability

The survey data used in this paper can be downloaded from:
`http://dx.doi.org/10.14324/000.ds.1489747`.

Acknowledgements

We are grateful to Tristan Caulfield, 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]. Alice Hutchings is supported by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSSandT/CSD) Broad Agency Announcement 11.02, the Government of Australia, and SPAWAR Systems Center Pacific [contract number N66001-13-C-0131]. The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not reflect those of the aforementioned agencies.

Bibliography

[1] Anne Adams and M. Angela Sasse. Users are not the enemy. In *Communications of the ACM*, pages 40–46, 1999.

[2] Ahli United Bank, Bahrain. Security Information – (Accessed on 01/9/2015).

[3] APS Bank, Malta. APS 365 Online Service – Terms and Conditions Agreement – Personal Customers (Accessed on 1/9/2015).

[4] APS Bank, Malta. Cards – Terms and Conditions (Accessed on 1/9/2015).

[5] Arab Bank, Jordan. Privacy Statement (Accessed on 02/9/2015).

[6] Arab Bank, Jordan. Ways to Bank – ATM – Security Tips (Accessed on 02/9/2015).

[7] Arab Bank, Jordan. Ways to Bank – Internet Banking Services (Arabi Online) – Terms and Conditions (Accessed on 02/9/2015).

[8] Arab Bank, Yemen. Ways to Bank – ATM – Security Tips (Accessed on 02/9/2015).

[9] Arab Bank, Yemen. Ways to Bank – Internet Banking Service – Terms and Conditions (Accessed on 02/9/2015).

[10] Arab Banking Corp. (ABC), Algeria. Online Security (Accessed on 01/9/2015).

[11] Arab Banking Corp. (ABC), Algeria. Terms and Conditions – (Accessed on 01/9/2015).

[12] Association of Banks, Singapore. Code of Consumer Banking Practice (Accessed on 1/9/2015).

[13] Association of Banks, Singapore. Code of Practice for Banks – Credit Cards (Accessed on 1/9/2015).

[14] Bank Audi, Lebanon. Privacy and Security – Information Security Tips (Accessed on 03/9/2015).

[15] Bank Muscat, Oman. Cards – Good Practices (Card Usage) (Accessed on 03/9/2015).

[16] Bank Muscat, Oman. Internet Banking – Security (Accessed on 03/9/2015).

[17] Bank of Baghdad, Iraq. Electronic Services – Visa Card Service (Accessed on 01/9/2015).

[18] Bank of Cyprus, Cyprus. Cards Terms and Conditions (Accessed on 7/9/2015).

[19] Bank of Palestine, Palestine. Terms and Conditions (Accessed on 03/9/2015).

[20] Adam Beautement, M. Angela Sasse, and Mike Wonham. The compliance budget: Managing security behaviour in organisations. In *NSPW*, pages 47–58. ACM Press, 2008.

[21] Nicholas Bohm, Ian Brown, and Brian Gladman. Electronic commerce: Who carries the risk of fraud. *Journal of Information, Law and Technology*, 3, 2000.

[22] Citibank, USA. Client Manual Consumer Accounts (Accessed on 1/9/2015).

[23] Co-operative Central Bank, Cyprus. Bank Card Agreement (Accessed on 7/9/2015).

[24] Commercial International Bank, Egypt. Online Security (Accessed on 01/9/2015).

[25] Dachverband der Volksbanken und Raiffeisenbanken, Germany. Sonderbedingungen für das Online-Banking (Accessed on 18/9/2015).

[26] Dachverband der Volksbanken und Raiffeisenbanken, Germany. Sonderbedingungen für die VR-BankCard (Accessed on 18/9/2015).

[27] Danske Bank. Conditions Cheque and Cash Card Accounts (Accessed on 1/9/2015).

[28] Danske Bank. Terms and Conditions for Access Agreement – Danske eBanking – Consumers (Accessed on 1/9/2015).

[29] Deutsche Bank Privat- und Geschäftskunden AG, Germany. Bedingungen für Debitkarten (Accessed on 6/9/2015).

[30] Deutsche Bank Privat- und Geschäftskunden AG, Germany. Bedingungen für den Zugang zur Deutsche Bank AG über elektronische Medien (Accessed on 6/9/2015).

[31] Deutscher Sparkassenverlag, Germany. Allgemeine Geschäftsbedingungen (Accessed on 4/9/2015).

[32] Deutscher Sparkassenverlag, Germany. Bedingungen für das Online-Banking (Accessed on 4/9/2015).

[33] Financial Ombudsman Service. Ombudsman News, March/April 2014. case 116/02 `http://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/116-disputed-transactions.html`.

[34] Financial Ombudsman Service. Ombudsman News, March/April 2014. case 116/08 `http://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/116-disputed-transactions.html`.

[35] Financial Ombudsman Service. Ombudsman News, March/April 2014. case 116/09 `http://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/116-disputed-transactions.html`.

[36] HSBC, UK. Banking Made Easy (Accessed on 1/3/2016).

[37] HSBC, UK. General, Current Accounts and Savings Accounts Terms and Conditions (Accessed on 1/9/2015).

[38] HSBC, UK. Personal Internet Banking Terms and Conditions (Accessed on 1/9/2015).

[39] Monte dei Paschi di Siena, Italy. Terms and Conditions for "Mondo Carta" – Electronic Debit Card (Accessed on 7/9/2015).

[40] Monte dei Paschi di Siena, Italy. Terms and Conditions for "Multicanalita Integrata" – Internet and Phone Banking (Accessed on 7/9/2015).

[41] Steven J. Murdoch, Ingolf Becker, Ruba Abu-Salma, Ross Anderson, Nicholas Bohm, Alice Hutchings, M. Angela Sasse, and Gianluca Stringhini. Are payment card contracts unfair? In *Financial Cryptography and Data Security*. Springer, 2016.

[42] National Bank of Abu Dhabi (NBA), UAE. General Terms and Conditions (Accessed on 03/9/2015).

[43] National Bank of Greece, Greece. Unified Booklet of Terms for Deposits by Individuals (Accessed on 7/9/2015).

[44] National Bank of Kenya. Terms and Conditions Credit Cards (Accessed on 1/9/2015).

[45] National Bank of Kenya. Terms and Conditions Personal Account Openings (Accessed on 1/9/2015).

[46] National Bank of Kuwait (NBK), Kuwait. ATM Safety Tips (Accessed on 02/9/2015).

[47] National Bank of Kuwait (NBK), Kuwait. Support – Security – Card Security Tips – General Tips (Accessed on 02/9/2015).

[48] National Bank of Kuwait (NBK), Kuwait. Support – Security – Online Safety Tips – Prevention Checklist (Accessed on 02/9/2015).

[49] National Commercial Bank (NCB), Saudi Arabia. Consumer Protection Code (Accessed on 03/9/2015).

[50] National Commercial Bank (NCB), Saudi Arabia. Personal Banking – AlAhli Online – Security Awareness Tips (Accessed on 03/9/2015).

[51] Nedbank, South Africa. e-Banking Service Terms and Conditions (Accessed on 1/9/2015).

[52] Nedbank, South Africa. Terms and Conditions of Transactional Current Accounts (Accessed on 1/9/2015).

[53] OCBC, Singapore. Online Banking Security (Accessed on 1/9/2015).

[54] OCBC, Singapore. Terms & Conditions – Electronic Banking Services (Accessed on 1/9/2015).

[55] Qatar National Bank (QNB), Qatar. Personal Banking – Credit Cards – Credit Card Safety (Accessed on 03/9/2015).

[56] Unicredit, Italy. Terms of Service – Carte di Debito Internazionali A Doppia Tecnologia – Debit Cards (Accessed on 10/9/2015).

[57] Zenith Bank, Nigeria. e-Banking Service Terms and Conditions (Accessed on 1/9/2015).