JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 3(2), 2017, 109–125
doi: 10.1093/cybsec/tyx011
Research paper

Research paper

International comparison of bank fraud reimbursement: customer perceptions and contractual terms

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

[1]Computer Science Department, University College London, Gower Street, London WC1E 6BT; [2] University of Cambridge Computer Laboratory, 15 JJ Thomson Avenue, CB3 0FD; [3]Foundation for Information Policy Research

*Corresponding author: E-mail: i.becker@cs.ucl.ac.uk

Received 7 May 2017; accepted 17 November 2017

Abstract

The study presented in this article investigated to what extent bank customers understand the terms and conditions (T&Cs) they have signed up to. If many customers are not able to understand T&Cs and the behaviours they are expected to comply with, they risk not being compensated when their accounts are breached. An expert analysis of 30 bank contracts across 25 countries found that most contract terms were too vague for customers to infer required behaviour. In some cases the rules vary for different products, meaning the advice can be contradictory at worst. While many banks allow customers to write Personal identification numbers (PINs) down (as long as they are disguised and not kept with the card), 20% of banks categorically forbid writing PINs down, and a handful stipulate that the customer have a unique PIN for each account. We tested our findings in a survey with 151 participants in Germany, the USA and UK. They mostly agree: only 35% fully understand the T&Cs, and 28% find important sections are unclear. There are strong regional variations: Germans found their T&Cs particularly hard to understand, and USA bank customers assumed some of their behaviours contravened the T&Cs, but were reassured when they actually read them.

Key words: banking fraud; customer perceptions; international comparisons; PIN usage; terms and conditions

Introduction

The ability to revoke fraudulent bank payments, or at least reimburse the victims of fraud, is one of the main selling points of the consumer banking system and particularly payment cards. The additional security feature is also used to justify the higher transaction fees associated with card payments, compared with payment systems where transactions are final, such as cash and cryptocurrencies. However, whether a customer who becomes a victim of fraud actually is reimbursed depends on the contract between the bank and its customers (which may in turn depend on national or international legislation), and how a bank chooses to apply the Terms & Conditions (T&Cs) the customer has signed up to. In order to be reimbursed, a fraud victim may need to demonstrate that they have followed security practices set out in the T&Cs—and thus it is very important that customers (i) are able to understand them, and (ii) are able to comply with the behaviours stipulated in them.

This article builds on previous research into the fairness of bank T&Cs, particularly how the rules adapt to changes in technology. The first study, by Bohm, Brown and Gladman [1], reviewed the T&Cs 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 T&Cs. The banks took advantage of the technology change to escape 19th-century consumer protection law. In some countries, such as the USA, pressure by consumer-rights advocates led to regulations that require disputed transactions to be refunded.

Recent research [2] also found bank T&Cs did not have sufficient detail for customers to work out what they had to do to be compliant, and in some cases were contradictory. The same study also found that bank customers do not comply with conditions on Personal identification number (PIN) security: they regularly share, reuse, and write down PINs—because they are unable to manage the credentials otherwise. Adapting the concept of a 'security budget' from Beautement, Sasse and Wonham [3], the cost of compliance (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) with T&Cs may be so high that millions of customers act habitually in ways that break them because they simply could not manage otherwise.

There is also the issue of affordances; banks permit customers to change PINs 'so you can pick one that is memorable to you'. For infrequently-used accounts, however, customers will often change them to the PIN on the most frequently-used account, because they are afraid they will forget it, and consider re-using a PIN more secure than writing it down. Many T&Cs, however, stipulate that the PIN for the account must be unique. It is technically straightforward for a bank to set a random PIN on every card issued to a customer, and not let them change it. By letting customers change PINs, but forbidding changes most customers will make in order to cope with the small print, the banks are inducing their customers to break the rules—and thus create ground for not being reimbursed in case of a breach. 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 there inconsistencies between banks in a country (that may lead to confusion), what do customers understand of their obligations, and whether such issues are hidden from the public behind the obscure contract language? This research attempts to find out.

In the 'Review of banking T&Cs internationally' of this research, we first conduct an expert examination of bank T&Cs around the world, identifying consistency, or lack thereof, both within and between countries. We draw on our diverse research team to sample the major banks and translate relevant passages into English. We focus on security advice on PINs, bank statements and telephone and online banking.

In the second part of this article we conduct a cross-cultural study between 151 individuals in the USA, UK and Germany. We ask participants if the rules are sufficiently clear, and if they understand the obligation imposed on customers by the banks' T&Cs. We focus this study on two common cases of bank fraud and supply the participants with the relevant sections of bank T&Cs from their country.

We conclude in the section 'Discussion' that if banking rules similarly cannot be understood, then it is unreasonable to expect customers to comply with them. Indeed, they make matters worse: Adams and Sasse [4] demonstrated a long time ago that traditional password and PIN policies require humanly impossible memory tasks. A recent National Institute of Standards and Technology report [5] found that in a work context, over 50% of staff write their credentials down in some way. As disputes are often centered around the PIN being written down and kept with the card—with the customer saying they did not do this, and the bank saying that they must have done—we argue that stipulating a behaviour that we know most people cannot follow means the rules are out of date at best, and unfair at worst. 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.

Related literature

Financial fraud remains an area of concern. In the UK, payment card fraud increased by 6% to £618 million in 2016 [6]. In the USA about 2 million customers actively reported fraud in 2012 [7], and while it is difficult to accurately specify in the USA, Sullivan estimates the value of unauthorized third-party fraud transactions through debit and credit card transactions as $3.8 billion for 2012 [8]. While the direct monetary loss to customers is negligible in the USA thanks to strong consumer protection, major data breaches have further repercussions as more personal identifiable information is stolen because fraudsters use this very data to attack customer accounts. Sullivan also compares the loss due to fraud between (amongst others) the USA, UK and the Single Euro Payment Area (SEPA) [8, Chart 9]: On a per-transaction basis over the period of 2005–2012, SEPA had the lowest fraud loss, followed by the UK and the USA.

Despite the significant volume of payment fraud, research on understanding its implications is surprisingly limited. In the USA, the Federal Reserve Bank of Philadelphia regularly runs its own conference series on 'Consumer Credit & Payments' and the Federal Reserve Bank of Kansas City one on 'Payments'. Stanley discusses work by Hogarth and Hilgert (primary text unavailable) where 18% of households had complaints with their credit card provider, but fraud is not mentioned [9]. The focus of the article instead lies on maintaining a safe environment: improving banks' risk mitigation techniques, increased cooperation between banks and payment reversal—attempting to shift liability of consumers is 'not good politics'. Despite discussing the impact of consumer regulation in financial markets, most of the discussion focusses on the impact of disclosures. On the topic of credit cards, fraud is not considered to be an important regulatory aspect, compared to regulation limiting the creditors ability to change interest rates at short notice and levy fines, as banks stand to lose a large revenue stream. The report notes that customer complaint data (from the CFPB) relatively closely reflects overall consumer satisfaction with financial institutions. The conference also debated consumers' ability to understand financial disclosures. It concludes that consumers cannot be expected to read disclosures, but if a consumer is interested they should be easily accessible and comprehensible. The participants agree that further academic research on the understanding and comprehension of disclosures should be conducted—as indeed we do in this research.

When Sullivan considers payment fraud in the USA, his recommendations for reducing payment fraud are mostly technical [8]. In the short term the industry should focus on hardening systems to attack, followed by improving the security of payment cards themselves in the medium term. Only in the long term does he call for standardization of payment systems (and their security). Further he argues that the existing basic tort-law principle 'that the entity in the best position to deter check fraud will bear the losses for a check it processes' should be expanded to the rest of the payment industry as well.

This is in stark contrast with legislation in the UK and the European Union. Before the introduction of payment cards, consumer protection in the UK was comparable to the USA as consumers were not liable for forged signatures on cheques. This liability was reduced slightly with the introduction of payment cards, where the consumer was liable for the first £50 (or thereabouts, depending on the bank) of fraud [1].

The introduction of automated teller machines (ATMs) caused a significant shift in consumer liability, as the bank would claim a customer was negligent or collusive if their card and PIN appeared to have been used. This was sharpened with the move to Chip and PIN as chip cards are harder to forge [10], and by the Payment Services Directive which supported harmonisation of regulations across the EU for members of the Single Euro Payment Area (SEPA). Suddenly if the bank deems that a consumer has been negligent in handling their PIN the consumer is fully liable. This change in customer liability has caused banks to become careless and therefore caused a huge increase in fraud in the UK [11], as consumers are unable to fix the banks' numerous security issues [12, 10].

Yet academic study of the reasons and consequences of this shift in liability is limited. In a rare publication on payment fraud from the field of criminology, Jansen and Leukfeld apply Routine Activity and Protection Motivation theory in a study with 30 phishing and malware victims [13]. They find that to some degree everyone is susceptible to online banking fraud victimization, regardless of their knowledge and skill. They identify that victims had taken adequate steps to protect themselves yet recommend more safety training for customers as well as education about the fraud risks. However, if the risks apply to all customers who find that protecting themselves is difficult, it makes more economic sense to allocate the risks to the actor who can do most to reduce the fraud overall, and who can also implement a straightforward procedure for recovering the funds [10, 11 and 14].

Review of banking T&Cs internationally

Methodology

In the first stage of this project, we surveyed the T&Cs of 30 banks operating in 25 countries. The study's scope included Europe (Cyprus, Denmark, Germany, Greece, Italy, Malta, and the UK), the USA, 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). Also included in the analysis is the Code of Consumer Banking Practice for Singapore. No banks were found operating online in Libya or Syria. We selected these banks in order to get a good representation across different cultures and regions. There was some convenience sampling in the countries selected, according to the language skills available within the research team. The bank documents included in this survey, and the codes used to identify them, are outlined in Table 1. For example, for APS Bank in Malta there were two relevant documents—APS1 and APS2. For other banks three or more documents contained relevant information.

Major banks were selected for the study. These are not always the largest banks, as some make their T&Cs available only to account holders. In some cases, multiple documents were reviewed, as some banks had separate T&Cs for telephone and Internet banking, as well as credit cards, debit cards and current accounts. All the documents reviewed were downloaded from the banks' websites and were for personal (rather than business) accounts. We found that T&Cs for accounts that adhere to Sharia Law, which prohibits charging interest on loans or paying it on savings, had identical security clauses to other personal accounts at the same bank. There were no further differences found for other types of personal account customers, such as high-wealth individuals.

The T&Cs were reviewed to identify instructions of or advice on security. This included how users should handle the PINs associated with their cards, as well as credentials for telephone and Internet banking. The documents reviewed were in English, German, Italian, Arabic, and Greek. The authors include native speakers of these languages, who translated the relevant sections and coded them in accordance with the categories set out in Table 2. To ensure consistency, we developed written instructions outlining how to select banks for review, which types of document to access, and the types of data to extract (and translate) from the T&Cs, as set out in the coding categories.

Results

The T&Cs 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 3.

PIN write 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 (AUB1), Bank Audi (BAL1), Bank of Baghdad (BBI1), Nedbank (NSA1) and Zenith Bank (ZBN1). Furthermore, three banks (Arab Banking Corp. (ABC2), HSBC (HUK2), and National Bank of Kenya (NBKe1)) 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 is required to: memorize the PIN, not write it down – even in an obscured fashion – on the Card or on any other document . . . ' (NBG1).

There is considerable variation in how PINs may be written down, and where. For example, Arab Banking Corp. in Algeria, HSBC in the UK, 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 (ABC2).
>
> Never writing down or otherwise recording your PINs and other security details in a way that can be understood by someone else . . . (HUK1).
>
> 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 (NBKe1).

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.

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 (NSA2).

Table 1. Banking documents included in survey

Bank	Country	Document name	Reference	Access date
Ahli United Bank	Bahrain	Security Information	AUB1	1 September 2015
APS Bank	Malta	APS 365 Online Service—T&Cs Agreement—Personal Customers	APS1	1 September 2015
APS Bank	Malta	Cards—T&Cs	APS2	1 September 2015
Arab Bank	Jordan	Privacy Statement	ABJ1	2 September 2015
Arab Bank	Jordan	Ways to Bank—ATM—Security Tips	ABJ2	2 September 2015
Arab Bank	Jordan	Ways to Bank—Internet Banking Services (Arabi Online) T&Cs	ABJ3	2 September 2015
Arab Bank	Yemen	Ways to Bank—ATM—Security Tips	ABY1	2 September 2015
Arab Bank	Yemen	Ways to Bank—Internet Banking Service—T&Cs	ABY2	2 September 2015
Arab Banking Corp.	Algeria	Online Security	ABC1	1 September 2015
Arab Banking Corp.	Algeria	T&Cs	ABC2	1 September 2015
Association of Banks	Singapore	Code of Consumer Banking Practice	ABS1	1 September 2015
Association of Banks	Singapore	Code of Practice for Banks—Credit Cards	ABS2	1 September 2015
Bank Audi	Lebanon	Privacy and Security—Information Security Tips	BAL1	3 September 2015
Bank Muscat	Oman	Cards—Good Practices (Card Usage)	BMO1	3 September 2015
Bank Muscat	Oman	Internet Banking—Security	BMO2	3 September 2015
Bank of Baghdad	Iraq	Electronic Services—Visa Card Service	BB1	1 September 2015
Bank of Cyprus	Cyprus	Cards T&Cs	BCC1	7 September 2015
Bank of Palestine	Palestine	T&Cs	BPP1	3 September 2015
Citibank	USA	Client Manual Consumer Accounts	CUS1	1 September 2015
Co-operative Central Bank	Cyprus	Bank Card Agreement	CCB1	7 September 2015
Commercial International Bank	Egypt	Online Security	CIB1	1 September 2015
Dachverband der Volksbanken und Raiffeisenbanken	Germany	Sonderbedingungen für das Online-Banking	DVR1	18 September 2015
Dachverband der Volksbanken und Raiffeisenbanken	Germany	Sonderbedingungen für die VR-BankCard	DVR2	18 September 2015
Danske Bank	Denmark	Conditions Cheque and Cash Card Accounts	DBD1	1 September 2015
Danske Bank	Denmark	T&Cs for Access Agreement - Danske eBanking Consumers	DBD2	1 September 2015
Deutsche Bank Privat- und Geschaeftskunden AG	Germany	Bedingungen für Debitkarten	DBG1	6 September 2015
Deutsche Bank Privat- und Geschaeftskunden AG	Germany	Bedingungen für den Zugang zur Deutsche Bank AG über elektronische Medien	DBG2	6 September 2015
Deutscher Sparkassenverlag	Germany	Allgemeine Geschäftsbedingungen	DSG1	4 September 2015
Deutscher Sparkassenverlag	Germany	Bedingungen für das Online-Banking	DSG2	4 September 2015
HSBC	UK	Banking Made Easy	HUK1	1 March 2016
HSBC	UK	Current Accounts and Savings Accounts T&Cs	HUK2	1 September 2015
HSBC	UK	Personal Interest Banking T&Cs	HUK3	1 September 2015
Monte dei Paschi di Siena	Italy	T&Cs for 'Mondo Carta'—Electronic Debit Card	MPS1	7 September 2015
Monte dei Paschi di Siena	Italy	T&Cs for 'Multicanalita Integrata'—Internet and Phone Banking	MPS2	7 September 2015
National Bank of Abu Dhabi	UAE	General T&Cs	NBA1	3 September 2015
National Bank of Greece	Greece	Unified Booklet of Terms for Deposits by Individuals	NBG1	7 September 2015
National Bank of Kenya	Kenya	T&Cs Credit Cards	NBKe1	1 September 2015
National Bank of Kenya	Kenya	T&Cs Personal Account Openings	NBKe2	1 September 2015
National Bank of Kuwait	Kuwait	ATM Safety Tips	NBKu1	2 September 2015
National Bank of Kuwait	Kuwait	Support—Security—Card Security Tips	NBKu2	2 September 2015
National Bank of Kuwait	Kuwait	Support—Security—Online Safety Tips—Prevention Checklist	NBKu3	2 September 2015
National Commercial Bank	Saudi Arabia	Consumer Protection Code	NCB1	3 September 2015
National Commercial Bank	Saudi Arabia	Personal Banking—AlAhli Online—Security Awareness Tips	NCB2	3 September 2015
Nedbank	South Africa	e-Banking Service T&Cs	NSA1	1 September 2015
Nedbank	South Africa	T&Cs of Transactional Current Accounts	NSA2	1 September 2015
OCBC	Singapore	Online Banking Security	OSi1	1 September 2015
OCBC	Singapore	T&Cs—Electronic Banking Services	OSi2	1 September 2015
Qatar National Bank	Qatar	Personal Banking—Credit Cards—Credit Card Safety	QNB1	3 September 2015
Unicredit	Italy	Terms of Service—Carte di Debito Internatzionali A Doppia Tecnologica—Debit Cards	UIt1	10 September 2015
Zenith Bank	Nigeria	e-Banking Service T&Cs	ZBN1	1 September 2015

> The customer . . . undertakes . . . not to write down the Passcode, Accesscode/Password in an open place to avoid third party coming across . . . (ZBN1). . . .

Bank Audi (BAL1), Bank of Baghdad in Iraq (BBI1), Bank of Cyprus (BCC1), Deutsche Bank (DBG1), Sparkassen and Volksbank in Germany (DSG1, DVR2), and UniCredit in Italy (UIt1) state that the PIN should not be stored with or on the payment card. Moreover, Bank of Cyprus (BCC1) 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 (QNB1): it requests its customers to only memorize their PINs. On the other hand, a

Table 2. Description of coding categories used

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 3. Summary of banks' T&Cs related to PIN security

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)	●	●	○	●

'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.

number of banks, including Ahli United Bank in Bahrain (AUB1), Citibank in the USA (CUS1) and National Commercial Bank in Saudi Arabia (NCB2), 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 . . . CUS1.

The advice from the National Bank of Kenya differs by the type of account. For credit cards, there is only a requirement to keep the PIN secret:

> The Card member shall exercise due care to ensure the safety of the Card and the Secrecy of the PIN at all times . . . (NBKe1).

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 . . . (NBKe2).

Arab Bank in Jordan and Yemen (ABJ2, ABY1), Bank Muscat in Oman (BMO1), APS Bank in Malta (APS2), Co-operative Central Bank of Cyprus (BCC1), National Bank of Greece (NBG1), and National Bank of Kuwait (NBKu2) 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 . . . (APS2).

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 . . . (DBD1).

In Singapore, OCBC does not appear to specify how customers might record PINs (OSi2), even though its trade association has a

Code of Practice which states that customers should be told that 'they should never write the PIN on the card …' (ABS2), 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' (ABS1).

Finally, a few banks do not provide guidelines to customers on how PINs might be written down, such as the Bank of Palestine (BPP1), Monte dei Paschi di Siena in Italy (MPS1), and the National Bank of Abu Dhabi in the United Arab Emirates (NBA1).

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 … (HUK1).

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 … (NSA2).

One other bank (Bank of Cyprus (BCC1)) mandates customer PIN change, but also provides advice on how to select a PIN. The Ahli United Bank in Bahrain (AUB1), and OCBC in Singapore (OSi2), as well as the Association of Banks in Singapore (ABS2) set out requirements for selecting a strong PIN, telling users not to use telephone numbers, birth 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 … (OSi2).

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 (AUB1), Arab Bank (ABJ2), Bank Audi (BAL1), Bank of Palestine (BPP1), Citibank (CUS1), National Bank of Kuwait (NBKu2), and Zenith (ZBN1)) 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 … (NBG1).

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 … (CUS1).

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.

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 …' (HUK1). 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 bank-operated 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 (DBD1). 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' (AUB1).

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 … (HUK1).

In Cyprus (Co-operative Central Bank), Malta (APS Bank Limited), and Qatar (Qatar National Bank), the banks allow customers to memorize the PIN before destroying the advice:

> Memorise the PIN and immediately destroy the document … (CCB1).
>
> Destroying the PIN notification sent to him by the Bank immediately after memorising the PIN … (APS2).
>
> Upon receiving your credit/debit card, memorise the PIN and destroy the PIN mailer … (QNB1).

The customers of Danske Bank have no set time limit:

> You must also remember to destroy the letter containing your PIN (DBD1).

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 (HUK1).
>
> Save receipts: Remember to take your receipts and shred them before discarding. It is best not to ask for receipts at all (NBKu1).

The advice from the National Bank of Kuwait that receipts should not be asked for differs from other banks, which require

customers to retain receipts for reconciliation with bank statements (AUB1, BAL1, BMO1). 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 (QNB1).

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' (ABJ1), 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' (ABC2). Three banks (Monte dei Paschi di Siena (MPS1), Unicredit (UIt1) and National Bank of Kenya (NBKe1)) provide vague statements, such as inviting their users to apply 'common sense' when dealing with card transactions, or using 'due care'.

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; others are in general T&Cs; and yet others in a combination. Until July 2015, HSBC's general UK contract set out requirements for safeguarding all credentials, including 'PINs, security numbers, passwords or other details including those which allow you to use PIB [Personal Internet Banking] and TBS [Telephone Banking Service]' (HUK2). Further requirements for telephone banking were found in a document called *Banking Made Easy*. These documents were later revised; now, the T&Cs simply require customers to follow the advice in the *Banking Made Easy* brochure. Some requirements for PINs also apply here: 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 number of 6–10 digits created by the customer during registration, so there is no advice letter to destroy.

The OCBC (OSi2) and Monte dei Paschi di Siena (MPS2) do not specify whether telephone banking credentials may be written down, or whether they 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 (OSi2).

Citibank customers can set up a 'Telephone Personal Identification Code (TPIC)' by calling the bank (CUS1); the online instructions do not discuss limits on code selection, or demand that the TPIC be unique.

Many banks' T&Cs for PINs also apply to telephone banking, including that credentials should not be written in an 'open place' (ZBN1), should not be kept with the card for which they are to be used (NBKe2), and should be changed periodically and be kept confidential and private (ABJ3, BPP1, ABY2, NSA1).

Clauses relating to Internet banking security

As with telephone banking, some banks have specific contracts for Internet banking, while 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 T&Cs (HUK3), 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 third-party software, such as browsers or password managers, to record passwords or other security details. 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 or biometric to lock 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 (OSi1).

The other banks reviewed do not impose such aggressive restrictions. Clauses specific to online banking include: using a firewall, antivirus and/or antispyware software (AUB1, APS1, ABJ1, ABY2, ABC1, BAL1, AMO2, CIB1, DBR1, DBG2, DSG2, NBA1, NBG1, NBKu3, NCB2); using a modern browser (ABC1, MPS2); patching the browser and/or operating system (AUB1, ABC1, BMO2, CIB1, DVR1, DBG2, DSG2, NBA1, NBG1, NCB2); not saving passwords in password managers or browsers (ABC2, BMO2, CIB1, NBA1, NBKu3, NCB2); not using public access computers (AUB1, ABJ3, ABY2, BMO2, CIB1, NBA1, NCB1, NCB2); encrypting wireless networks (CIB1); clearing the cache after each banking session (BMO2); using a password to access the computer (NCB2); and disabling file and printer sharing capabilities (NCB2). The National Bank of Kuwait 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 (NBKu3).
>
> 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 (CIB1).

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 (DBD2).

Discussion

This review of bank T&Cs demonstrates that banks take a variety of approaches to the security advice they offer to, and the demands they make of, customers. The approach varies not just between jurisdictions but between banks in each jurisdiction. Advice on writing down PINs ranges from a strict 'no' to 'yes, but', with requirements on obscuring the PIN and safekeeping. About half the banks allow users to change PINs; but there's a range of advice on PIN choice. The PIN advice letter may have to be destroyed at once, or eventually, or not at all; and a similar range of advice is given for bank statements and receipts. The clauses regarding the safekeeping of authenticating information for telephone banking and internet banking are no different, except in that different banks take the different extreme positions. Internet banking security is just as diverse, but much more complex; there are many more kinds of advice that banks can and do give about preventing malware infection of devices used for online banking, many of which are outdated and difficult to follow.

While some of the advice is drafted so as to be helpful, many of the instructions are demands. It is not clear from the present survey which of these demands are also designed to minimize the risk to the customer, and which are there to minimize the risk to the bank, by enabling it to ask a whole series of hard questions of customers who complain of fraud, and reject many claims on the basis of non-compliance. Such behaviour will be discussed further in the final 'Discussion' section below. Surveying how banks in different countries actually treat fraud victims and how this relates to local banking regulation would be a fascinating research project, but a very much larger one than the work reported here.

Limitations

There are number of limitations of our methodology that should be mentioned. Primarily, our scope is limited to languages that our diverse range of authors speak. We did use search engines and site maps when searching for T&C documents, so while care was taken to retrieve the T&Cs documents of the banks studied, there were a number of banks which did not seem to publicly list their T&Cs.

Furthermore, banks regularly update their T&Cs. Our research here presents a snapshot. We have made our dataset publicly available (see the final 'Discussion' section), as outdated T&Cs can be hard to retrieve.

In the following section, we explore how individuals interpret and understand these differences.

Survey

The second contribution of this research is a cross-cultural study of the understanding and interpretation of banking T&Cs. As we have described in the previous section, there are significant differences in the legal setting of banking between countries, as well as between banks within the same country. 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 UK and the USA. Consumer protection for fraudulent transactions in Germany and the UK is governed by the same law, the EU Payment Services Directive (PSD)[1] (soon to be replaced by PSD2[2]), whereas USA disputes are governed by the more consumer-friendly federal regulations E[3] and Z.[4] 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 three-fold:

1. identify the perceptions and prejudice of participants towards banking T&Cs;
2. measure the ability of our participants to understand the banks' T&Cs and act on them;
3. on a country-specific basis and as a cross-cultural study.

Related literature

While there are to our knowledge no cross-cultural examinations of the understanding of T&Cs, many methodologies of cross-cultural studies have been explored. Similarly, text comprehension is an established research branch.

Cross-cultural study design

The field of psychology has devoted much research into conducting valid cross-cultural studies. Jones and Kay lay out a number of challenges that cross-cultural research faces [15]. In this study we are interested in the comparative use of the scores deduced from the responses from each of the countries, as we intend to perform analysis on the differences between the groups. This requires us to aim for a construct-referenced meaning across the different languages: the study's 'aim' needs to be translated to the cultures [16]. This is not a purely translational issue: social norms and concepts may well be different. Hence in our study we have opted for a symmetric translation: we have adjusted cultural symbols (as far as these are present in contractual terms) to the best of the translator's knowledge of the target cultures.

The difficulty of conducting studies is not just limited to the textual content. The steps on Likert scales may have different meanings in different languages [17]. We have taken great care that our study is accurately represented in the three cultures studied, but a full sociological validity analysis is outside the scope of this research.

Reading comprehension

There is an existing body of research on the comprehension of legal texts. The initial research seems to have been carried out by Masson and Waldron, who simplified T&Cs in three steps [18]. Each simplification increases comprehension, but absolute comprehension values were still very low. Further studies on the topic point out individuals do not read contracts before signing them [19], or do not read Software Licensing Agreements before clicking OK [20]. Shorter End User License Agreements (EULAs) may actually

1 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance), available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007L0064 (2 August 2017, date last accessed).

2 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance).

3 https://www.federalreserve.gov/bankinforeg/regecg.htm (2 August 2017, date last accessed).

4 https://www.federalreserve.gov/bankinforeg/regzcg.htm (2 August 2017, date last accessed).

decrease number of software installations [21], as can politely asking for user permission [22]. Paraphrasing may well aid readability [23], but just as in [18], absolute values of readability remain low.

These empirical findings are supported by one analytical study: Prichard & Hayden analyse the EULAs of freeware using a number of readability metrics [24]. They (perhaps unsurprisingly) support the findings from the literature: the vast majority of EULAs were very difficult to read and very long.

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 customer. We elicit the responses to the scenarios twice: before being aware of the T&Cs and again afterwards. The scenarios are sourced from the UK Financial Ombudsman newsletter [25–27]. The scenario texts presented below have not been changed in meaning from the Financial Ombudsman newsletter. The Financial Ombudsman Service (FOS) is an arbitration service that was set up by the UK banks as an alternative to using the court system to resolve disputes with customers, and that now adjudicates according to their interpretation of the requirements set out in the PSD. Arbitrations are binding on the bank, and while a customer may instead take a case to the courts, the prohibitive costs involved make this rare, so the FOS interpretation of the PSD is dominant in the UK. Its quarterly newsletter publishes examples of its common dispute resolutions.

After asking a number of questions regarding the scenarios, we introduce a set of T&Cs on payment safety and fraud (as discussed in the previous 'Discussion' section on Page 116. We next ask the participant a number of questions to gauge their understanding of these T&Cs on a following page, without allowing them to page back to access the terms.

We then reintroduce the two scenarios, this time giving them access to the text of T&Cs, and again enquire about their expectation of the outcome. The full survey text can be found at http://dx.doi.org/10.14324/000.ds.1554770.

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 contract terms, we wanted to remove any form of prompt in order to get unbiased responses. These free-text responses are then manually grouped using Thematic Analysis [28]. The raw counts are normalized, 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.[5] The survey took on average 18 minutes to fill out, and we paid each participant £2.50. We trialled 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 USA (the USA 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 T&Cs on the two scenarios. Secondly, 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.

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.

Scenario 1: Card loss

The first scenario is based on a typical story of theft [25]. 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.

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.

Scenario 2: Phone scam

The second scenario is based on a combination of Ombudsman News stories [26, 27]. 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 authorized the transaction. The Financial Ombudsman chose the wording of the first line of the scenario to intentionally highlight that the customer was unable to verify the identity of the bank. There is a large number of similar cases in the UK (although this type of fraud is less common in Germany), 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.

5 https://www.prolific.ac/ (2 August 2017, date last accessed)

The T&Cs

It is infeasible to have our participants work through an entire document of T&Cs 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 T&Cs (HUK2), 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 (CUS1). 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 our previous analysis.

Following the same argument, we chose the T&Cs for Debit Cards of Deutsche Bank (DBG1) for Germany. Here, we focused on section 6. *Geheimhaltung der persönlichen Geheimzahl (PIN)* (Keeping your PIN secret), Section 12. *Erstattungs- und Schadensersatzansprüche des Kontoinhabers* (Reimbursements and claims for damages of the account owner), and Section 13. *Haftung des Kontoinhabers für nicht autorisierte Kartenverfügungen* (Liability of the account owner for unauthorized card charges).

Demographics

We recruited 151 participants in total: 41, 56 and 54 participants from the DE, UK and USA, respectively. An overview of the age and gender of all recruited participants can be found in Fig. 1 and Table 4. 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 USA. 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 geolocation is far from accurate, however, all but 3 participants' IP addresses matched their declared country. We decided to include the answers from these outliers, 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 USA, respectively, with standard deviations of 6.6, 12.7 and 9.8 years, respectively. In general, Prolific Academic seems to have the most representative demographics for the UK.

There are distinct differences in employment across the USA, DE and UK, as can been seen in Table 5. Almost all our participants claim to be native speakers in our study; 100%, 92% and 92% for the DE, UK and the USA, 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 or equivalent (see Table 6). The translation of education levels is not straightforward, which may explain the 0% value for GCSE level education in the USA. Two participants revealed that they had learning disabilities.

It is obvious that our participants' demographics could be better aligned for a crosscultural 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 5) and gender, participants age and educational demographics (Figure 1 and Table 6) are fortunately similar.

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 three histograms for the number of payment cards our participants have in the DE, UK and the USA, 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 USA, our participants there also have the smallest number of bank accounts.

Table 4. Gender of our participants

Gender	DE (%)	UK (%)	USA (%)
Female	24	52	27
Male	73	48	71
Other	2	0	2

Table 5. Employment demographics of our participants

Employment Status	DE (%)	UK (%)	USA (%)
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

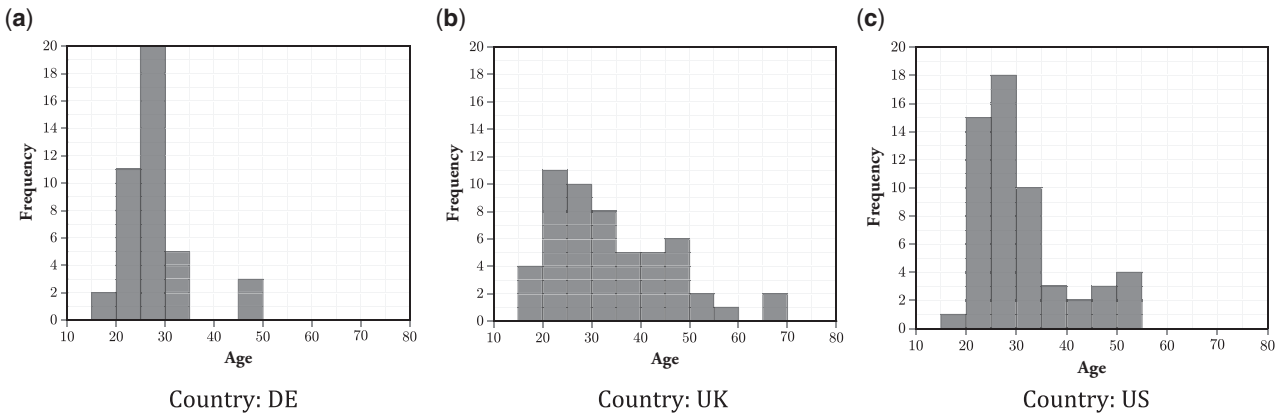

Figure 1. Histogram of our participants' age.

We also 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 7), yet payment card penetration rates are still high. Virtually, no participant manages a week on average without using a card.

Fraud experience

We hypothesize 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 fraud victims, and to explain the experience to us if they have. In Table 8, we list our participants' frequency of fraud experience. In order to get as complete description as we could, we solicited free-text responses.

We analysed these responses using Thematic Analysis, and the results can be seen in Table 9. 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 is noticed by the customers. This is reversed for the UK and the USA, 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'.

Table 6. Educational demographics of our participants

Highest qualification	DE (%)	UK (%)	USA (%)
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

Scenario overview

In the following sections, the participants consider the two scenarios in two different combinations: once before seeing the relevant T&Cs, and once afterwards. Each time they are asked if they think the protagonist should be reimbursed by the bank and why. The results of the binary question can be found in Table 10. We find that in all but one case, the participants are more likely to have the protagonist reimbursed after reading the T&Cs. 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.

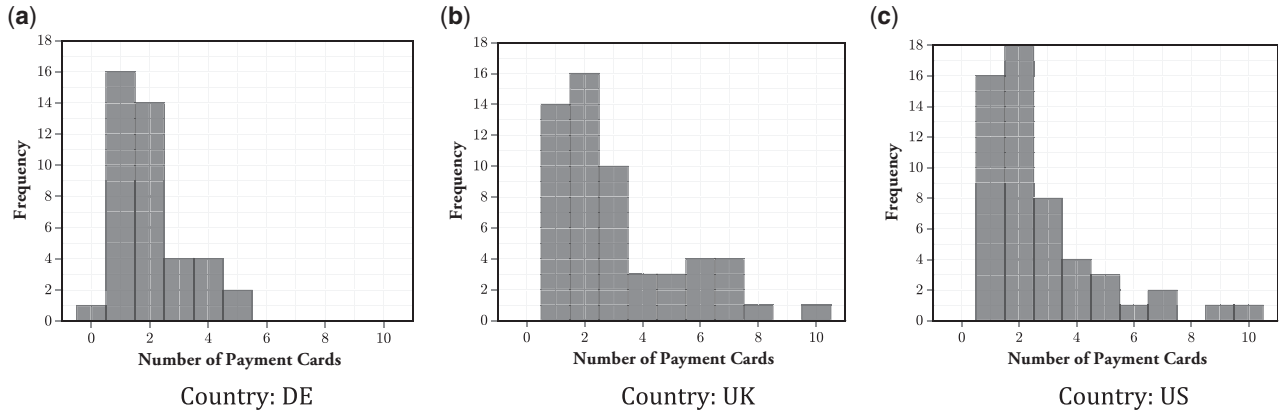

Figure 2. Participants' number of payment cards.

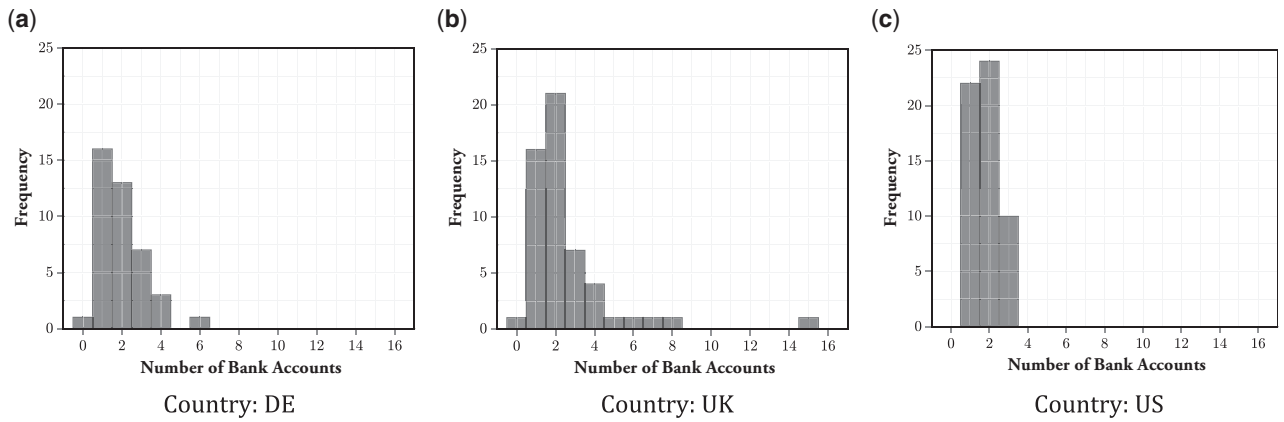

Figure 3. Participants' number of bank accounts.

Table 7. Frequency of use of any of our participants' payment cards

Frequency	DE (%)	UK (%)	USA (%)
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 8. Have you ever experienced fraudulent transactions or incidents on any of your payment cards or bank accounts?

	DE (%)	UK (%)	USA (%)
No	88	72	66
Yes	12	28	34

Table 9. Thematic analysis of the description of frauds 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

Code	DE (%)	UK (%)	USA (%)
Customer identifies fraud 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 10. 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: Phone Scam

Question	DE (%)	UK (%)	USA (%)
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: Phone Scam	31.7	37.0	35.7
Scenario 2: Phone Scam after T&Cs	43.9	46.3	42.9

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.

Prior to revealing T&Cs

Tables 11 and 12 show the results of the 'Card Loss' scenario before revealing the T&Cs. The respondents who supported reimbursement gave a wide range of reasons (Table 11). The most recurring reasons across the German, the UK and the USA surveys are: (i) the theft was reported immediately, cited by 52.9%, 50.0% and 41.9% of respondents respectively, and (ii) 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 authorize the transaction and, hence, she should be reimbursed; only 6.8% and 2.3% mentioned the same reason in the UK and the USA 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 USA survey. Interestingly, only USA participants, with about 9%, mentioned that reimbursement depends on Miss K's bank T&Cs.

Table 12 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 the 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% (USA). 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 USA (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 USA 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.

After revealing relevant T&Cs

After revealing the T&Cs to our participants, we were interested in their comprehension. Table 13 presents the reasons provided by the respondents who believed that Miss K should be reimbursed (after reading the T&Cs). 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 unauthorized; 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 T&Cs; 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.

Table 11. Thematic analysis of the answers in support of reimbursement in Scenario 1: Card Loss

Code	DE (%)	UK (%)	USA (%)
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 12. Thematic analysis of the answers not in support of reimbursement in Scenario 1: Card Loss

Code	DE (%)	UK (%)	USA (%)
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 13. Thematic analysis of the answers in support of reimbursement in Scenario 1: Card Loss, after the participants have seen the T&Cs

Code	DE (%)	UK (%)	USA (%)
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

In contrast, Table 14 displays the reasons mentioned by the participants who said that Miss K should not be reimbursed, after seeing the T&Cs. 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.

Table 14. Thematic analysis of the answers not in support of reimbursement in Scenario 1: Card Loss, after the participants have seen the T&Cs

Code	DE (%)	UK (%)	USA (%)
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

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 T&Cs: two-thirds of those who oppose reimbursement give the same reason as the Ombudsman.

We do not know how this case would have been decided in Germany and the USA, but we can still analyse the change in perceptions. In the case of Germany and the UK, the percentages in favour of reimbursement did not change with the revelation of the T&Cs. In the USA, 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 T&Cs carefully.

In contrast to the American T&Cs ('sixty days after the statement was mailed to you'), the German terms do not give a definite time frame as to when a transaction has to be reported as fraudulent. This may have motivated the high response rate in Table 14.

Scenario 2: Phone scam

Prior to revealing T&Cs

Table 15 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, the UK and the USA respondents. Secondly, banks should be insured, should be ethical, and should be able to reverse any unauthorized transaction; support was 30.8%, 35.0% and 25.0%. Thirdly, 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.

Table 16 shows the reasons given by the respondents who initially opposed reimbursing Mr L. Threequarters 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.

Table 15. Thematic analysis of the answers in support of reimbursement in Scenario 2: Phone Scam

Code	DE (%)	UK (%)	USA (%)
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 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 16. Thematic analysis of the answers not in support of reimbursement in Scenario 2: Phone Scam

Code	DE (%)	UK (%)	USA (%)
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

After revealing relevant T&Cs

After revealing the relevant T&Cs, the respondents who supported reimbursement provided the reasons shown in Table 17. 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 USA 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 USA surveys. Most of the USA respondents believed Mr L should be reimbursed because he was not the one who authorized the transaction, a view shared by only 16.7% of Germans, but 28.0% of Brits.

Finally, Table 18 documents the reasons for why Mr L should not be reimbursed. About 60% and 50% in the DE and the UK surveys believed that Mr L was grossly negligent; 28% of the USA 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% (USA). Other reasons included that Mr L was the one who gave his details 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 T&Cs.

Analysis

In the UK, the Ombudsman decided that the protagonist was not to be reimbursed as he was deemed to have authorized 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 10), the majority of participants were unable to give the same reason after reading the T&Cs, 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 vaguer but more consistent with the T&Cs view of 'gross negligence' (Tables 16 and 18). Interestingly, even though 'gross negligence' is not mentioned in the T&Cs shown to the American customers, still 28.1% gave this reason (or one to that effect). But, only in the USA 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 USA.

Table 17. 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 (%)	USA (%)
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 authorized transaction	16.7	28.0	75.0
Phishing is 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 18. Thematic analysis of the answers not in support of reimbursement in Scenario 2: Phone Scam, after the participants have seen the T&Cs

Code	DE (%)	UK (%)	USA (%)
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

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 15)—does not appear as a reason in favour at all in Table 17. 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 USA initially gave the same reasons as those from the UK and Germany, after reading the T&Cs the vast majority (75.0%) agree that the protagonist did not authorize the transactions. This must have been a clear feature of the T&Cs presented to the participants from the USA.

Understanding of T&Cs

The T&C documents are not easily 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 to return to the terms page once they had left. On average, the participants spend 204 seconds on reading the T&Cs.

A set of comprehension questions followed on the next page. It seems that many of the participants had never read their bank's T&Cs before. One commented: '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 19, 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.

Table 20 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 USA 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.

Next, we asked how one was supposed to remember PINs (Table 21). Writing down PINs is more accepted in the USA than in Germany or the UK with over a quarter of participants stating that the T&Cs allowed them to do so. Unfortunately, it was difficult here to find sample T&Cs whose intentions were actually made clear in the extract. Still further insights can be gained: there is a tendency in the USA 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 [2]. 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.

In contrast to these tables, we asked the participants to self-judge their own understanding of the T&Cs. Table 22 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 USA 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.

Diving into more detail, Table 23 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.

Table 19. Thematic analysis of the answers to the comprehension question: 'When are you liable for an unauthorised transaction?'

Code	DE (%)	UK (%)	USA (%)
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 20. Thematic analysis of the answers to the question: 'What is gross negligence?'

Code	DE (%)	UK (%)	USA (%)
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 21. Thematic analysis of the answers to the question: 'What can you do to remember your PIN?'

Code	DE (%)	UK (%)	USA (%)
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 22. How confident are you that you have understood the T&Cs?

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

Table 23. Thematic analysis of understanding issues of the T&Cs of the participants

Code	DE (%)	UK (%)	USA (%)
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

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 vague 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.

Customers disputing transactions frequently contact the authors to discuss their case. We find that a common approach of the bank is to request that the customer answers a checklist of whether they complied with security recommendations taken from the bank T&Cs. This advice includes recommendations that never appear in bank publicity, and even contradict advice from banking trade bodies, and so the checklist will likely be the first time the customer has ever seen the recommendations. This creates 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. This also explains a possible reason for banks to list some security recommendations only in T&Cs that they know the vast majority of their customers will not read. But, rather than a blanket assertion to this effect, the actual argument for refusing a refund 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 USA, where consumer laws are held to discourage such an argument, the bank can argue instead 'As your password was used, you authorized this transaction' [29]. The exceedingly onerous UK bank T&Cs are particularly worrisome in this context.

The initial draft of the PSD would have restricted the UK and other EU banks from using their T&Cs in this way, as the bank would be required to find additional evidence of negligence, in addition to their own records showing that the transaction was performed with a payment instrument they issued (such as a card). During the development of the PSD, we know from banking industry submissions [30] and our discussions with the individuals involved in the drafting process, that industry lobbied to continue to be permitted to treat their own records as authoritative statements showing that customers are liable for disputed transaction. The banking industry proved successful in doing so by amending Article 59(2) to insert the word 'necessarily' and so, in the view of regulators enforcing the PSD who the authors met with, nullifying the original version's effect. The final version of the PSD Article 59(2), substantially replicated in PSD2 Article 72, reads 'Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under Article 56' (emphasis ours). The PSD2 does add the requirement that 'The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user.' Banks may however may continue to decide that their records showing that a transaction was authorized are such sufficient supporting evidence.

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 T&Cs, 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 T&Cs and their translations that we studied can be found at http://dx.doi.org/10.14324/000.ds.1554770. The survey data used in this article can be downloaded from: http://dx.doi.org/10.14324/000.ds.1489747.

Funding

This work was supported by The Royal Society [grant number UF110392] to SJM; the Engineering and Physical Sciences Research Council [grant number EP/G037264/1] to IB; the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific [contract number N66001-13-C-0131] to AH. The opinions, findings, conclusions or recommendations expressed are those of the authors and do not reflect those of the aforementioned agencies.

Acknowledgements

We are grateful to Tristan Caulfield, Pyrros Chaidos, Boris Hemkemeier and Kat Krol for helpful discussions.

References

1. Bohm N, Brown I, Gladman B. Electronic commerce: Who carries the risk of fraud. *J Infor L & Technol* 2000;**3**. http://elj.warwick.ac.uk/jilt/00-3/bohm.html.
2. Murdoch SJ, Becker I, Abu-Salma R *et al*. Are payment card contracts unfair? In: *Financial Cryptography and Data Security*. Berlin, Heidelberg: Springer, 2016.
3. Beautement A, Sasse MA, Wonham M. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 workshop on New Security Paradigms*, 2008, pp. 47–58.
4. Adams A, Sasse MA. 'Users are not the enemy'. *Commun ACM* 1999;**42**: 40–46.
5. Steves M, Chisnell D, Sasse MA *et al*. Report: Authentication Diary Study, National Institute of Standards and Technology, NIST IR 7983, February 2014.
6. Financial Fraud Action UK, Year-end 2016 fraud update: Payment cards, remote banking and cheque. London, UK, Bulletin, 2017.
7. Cheney J, Hunt R, Mikhed V *et al*. Consumer use of fraud alerts and credit freezes: an empirical analysis. Federal Reserve Bank of Philadelphia, Philadelphia, PA, Discussion Paper, September 2014.

8. Sullivan RJ. Controlling Security Risk and Fraud in Payment Systems. Federal Reserve Bank of Kansas City, Economic Review Third Quarter 2014, 2014.
9. Stanley A. Voting With Your Feet: Consumers' Problems With Credit Cards and Exit Behaviors. Federal Reserve Bank of Philadelphia, Philadelphia, PA, Discussion Paper, May 2003.
10. Hache ACB, Ryder N. Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas: A critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud. *Infor & Comm Technol L* 2011;**20**:35–56.
11. Anderson R, Moore T. The economics of information security. *Science* 2006;**314**:610–613.
12. Anderson R, Bond M, Murdoch SJ. Chip and spin. *Comp Security J* 2006; **22**:1–6.
13. Jansen J, Leukfeldt R. Phishing and malware attacks on online banking customers in the Netherlands: a qualitative analysis of factors leading to victimization. *Intl J Cyber Crimino; Thirunelveli* 2016;**10**:79–91.
14. Anderson R. Closing the phishing hole–fraud, risk and nonbanks. In: *Proceedings of the Conference on Nonbanks in the Payments System, Federal Reserve Bank of Kansas City, 2007*, 2007.
15. Jones EG, Kay M. Instrumentation in cross-cultural research. *Nursing Research* 1992;**41**:186–188.
16. Hui CH, Triandis HC. Measurement in cross-cultural psychology: A review and comparison of strategies. *Of Strategies. J Cross-Cultural Psychol* 1985;**16**:131–152.
17. Heine SJ, Lehman DR, Peng K *et al*. What's wrong with cross-cultural comparisons of subjective Likert scales?: The reference-group effect. *J Person & Social Psychol* 2002;**82**:903.
18. Masson ME, Waldron MA. Comprehension of legal contracts by nonexperts: Effectiveness of plain language redrafting. *Applied Cog Psychol* 1994;**8**:67–85.
19. Wogalter MS, Howe JE, Sifuentes AH *et al*. On the adequacy of legal documents: factors that influence informed consent. *Ergonomics* 1999;**42**: 593–613.
20. Wogalter MS, Hayes MR. Online and software licensing agreements: User beliefs and expectations of risks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 2014;**58**:1391–1394.
21. Good NS, Grossklags J, Mulligan DK *et al*. Noticing notice: A large-scale experiment on the timing of software license agreements. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2007, pp. 607–616.
22. Böhme R, Köpsell S. Trained to accept?: A field experiment on consent dialogs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2010, pp. 2403–2406.
23. Waddell TF, Auriemma JR, Sundar SS. Make it simple, or force users to read?: Paraphrased design improves comprehension of end user license agreements. In *Proceedings of the 2016 SIGCHI CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2016, pp. 5252–5256.
24. Prichard JJ, Hayden MB. Assessing the readability of freeware end-user licensing agreements. *Issues in Information Systems* 2008;**9**: 452–459.
25. Financial Ombudsman Service, case 116/02, Ombudsman News March/ April 2014, 2014.
26. Financial Ombudsman Service, case 116/08, Ombudsman News March/ April 2014, 2014.
27. Financial Ombudsman Service, case 116/09, Ombudsman News March/ April 2014, 2014.
28. Fereday J, Muir-Cochrane E. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *Intl J Qual Methods* 2006;**5**:80–92.
29. Patrick K. Reg E: To Pay Or Not To Pay. *Bankers' Hotline* 1996;**6**:7/96 https://www.bankersonline.com/articles/103455 (6 May 2017, date last accessed).
30. Barclays PLC. *Response to consultation on a possible legal framework for the single payment area in the internal market*, July 2002 http://ec.europa.eu/internal_market/payments/docs/framework/framework-workingdoc-contrib/barclays_en.pdf (6 May 2017, date last accessed).