An Exploratory Study of User Perceptions of Payment Methods in the UK and the US

Kat Krol[1,*], Muhammad Sajidur Rahman[2,*], Simon Parkin[1,*], Emiliano De Cristofaro[1], and Eugene Y. Vasserman[2]
[1] University College London, {kat.krol.10, s.parkin, e.decristofaro}@ucl.ac.uk
[2] Kansas State University, {sajidrahman, eyv}@ksu.edu

***Abstract*—This paper presents the design and the results of a cross-cultural study of user perceptions and attitudes toward electronic payment methods. We conduct a series of semi-structured interviews involving forty participants (20 in London, UK, and 20 in Manhattan, KS, USA) to explore how individuals use the mechanisms available to them within their routine payment and banking activities. We also study their comprehension of payment processes, the perceived effort and impact of using different methods, as well as direct or indirect recollections of (suspected or actual) fraud and related interactions with banks and retailers. By comparing UK and US participants, we also elicit commonalities and differences that may help better understand, if not predict, attitudes of US customers once technologies like Chip-and-PIN are rolled out – for instance, several US participants were confused by how to use it, while UK participants found it convenient. Our results show that purchasing habits as well as the availability of rewards schemes are primary criteria influencing choices relating to payment technologies, and that inconsistencies, glitches, and other difficulties with newer technologies generate frustration sometimes leading to complete avoidance of new payment methods.**

I. Introduction

Over the past few years, electronic payments have become the primary transaction method in many countries, overtaking cash payments for the first time in 2006 in the US [29] and in 2014 in the UK [2]. Just in January 2015, there were more than one billion purchases – totaling £48M – in the UK [26]. In the US, there are roughly 50% more credit card accounts (500M) than people living in the country (318M) [25].

Unsurprisingly, payment cards have been targeted by malevolent actors, and financial loss from fraud has increased steadily as the number of payment cards has grown [23]. Aiming to curb fraud, chip-enabled EMV (Europay, MasterCard, Visa) cards have started to be distributed – gradually between 2003 and 2006 in the UK, and in other countries shortly afterwards. EMV cards, also known as Chip-and-PIN, require customers to authenticate transactions by inserting the side of the card with the chip into the Point-of-Sale (POS) terminal and keying in a PIN. US providers have also started to roll out chip-enabled cards, although, at the time of writing, customers are asked to sign rather than enter the PIN, even if the card is inserted rather than swiped. At the same time, RFID/NFC *contactless* cards as well as Apple Pay/Android Pay have also entered the global market, effectively aiming to reduce the effort/duration of performing a payment task as well as to make the process more 'fun' for the customer.

Naturally, the user experience of the payment task may differ remarkably, not only across individuals and across different countries/cultures, but also based on the actions and the steps involving the customer. For instance, with Chip-and-PIN, the customer usually goes through six different steps: wait for the POS to prompt them to insert the card, insert the card, wait for PIN request, enter PIN, wait for the POS to request card removal with the "remove card" message, and finally remove the card. If the card is removed too early, the transaction is declined. In contrast, traditional swipe-and-sign transactions only require the customer to hand the card to the cashier or swipe the card at the POS terminal, wait for a signature request, and sign.

Such a diverse landscape motivates the need to analyze the perspectives and attitudes of payment cards' users, looking at the usability of different payment methods as well as the related security/trust perceptions. To this end, we design an exploratory qualitative study based on a series of semi-structured interviews, involving forty participants who are regular users of payment cards. We introduce an additional dimension by recruiting participants in two different countries: the UK (London) and the US (Manhattan, KS). Our aim is to not only compare across different 'financial cultures', but also to interview individuals with different payment habits, as UK participants are exposed to Chip-and-PIN, while most in the US are not. Specifically, we set out to analyze purchasing habits, covering both online and in-person transactions, and the way the individuals use the payment mechanisms available to them as part of their routine payment and banking activities. We elicit individual comprehension of payment processes and the perceived effort and the impact of using various payment mechanisms, as well as any direct or indirect recollections of both suspected and actual fraud, including related interactions with banks and retailers.

In general, we find that purchasing habits and the availability of rewards schemes are the primary criteria influencing payment choices. Interviewees reported on a range of measures to feel secure, at times – for example, avoiding new technologies like contactless, or trusting popular brands. Our participants also reported on a number of inconsistencies and

[*] Authors contributed equally.

Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page. Reproduction for commercial purposes is strictly prohibited without the prior written consent of the Internet Society, the first-named author (for reproduction of an entire paper only), and the author's employer if the paper was prepared within the scope of employment.
USEC '16, 21 February 2016, San Diego, CA, USA
Copyright 2016 Internet Society, ISBN 1-891562-42-8
http://dx.doi.org/10.14722/usec.2016.23018

glitches, as well as difficulty in managing and remembering many PINs and different/new technologies, causing frustration and nudging them to undertake several interesting coping strategies. When asked about their experience with chip cards, several US participants were confused by what they are and how to use them, while UK participants found them convenient and/or straightforward, with the extra hurdles giving them an additional sense of security as compared to contactless.

To the best of our knowledge, our exploratory study is the first to focus on perceptions and attitudes of users of several different payment cards. By comparing UK and US participants, we also elicit commonalities and differences that may help better understand, if not predict, attitudes of US customers once Chip-and-PIN is rolled out across the country.

II. Related work

A number of prior studies have examined how users perceive and behave with respect to different payment systems. Howcroft et al. [16] examined perceptions and attitudes of UK customers toward phone and Internet-based banking, focusing on past (actual) and future (projected) behaviors. They highlighted a match between behavior and preference for branch-based operations. Then, Forsythe and Shi [12] found risk perception to be a consistent predictor of Internet shopping behavior; shoppers who felt at higher risk were less likely to make a purchase online. Of the six types of perceived risk identified in the previous literature (physical, financial, social, psychological, product performance concerns, and time/convenience loss), authors examined the most common ones among Internet shoppers and concluded that increased uncertainty regarding the result of a potential behavior leads to a decrease in that behavior. Of 18 potential risks that might prevent Internet users from shopping online, respondents mostly mentioned risks related to product performance (39%), financial loss (23%), psychological/privacy concerns (32%), and time/convenience (20%) [12]. However, perceptions and behaviors may have changed significantly since the time of these studies – 2002 and 2003, respectively.

Underscoring that behavior is driven by *subjective* consumer beliefs (and not necessarily correlated with good security), Kim et al. [18] conducted a customer-centric study of electronic payment security and trust. They found that technology as well as statements by payment providers both positively correlated with consumers' perceptions of security and trust and their use of e-payments. Somewhat surprisingly, perceived security exhibited a stronger positive correlation with the use of technologies than perceived trust, although there is a strong relationship between perceived security and perceived trust – a fact also observed by De Cristofaro et al. [10] in the context of two-factor authentication (2FA).

Just and Aspinall [17] also analyzed dual credential authentication for online banking from both security and usability perspectives. They considered granularity and time of feedback given to users during the authentication steps as main usability properties, and found that some banks delayed feedback by not providing it when screen content changed, or otherwise provided granular feedback too late in the authentication process. They concluded that these issues are likely to confuse users, but did not conduct an actual user study.

Crane et al. [9] studied trust in information and communication technologies in the UK and also looked at Chip-and-PIN cards. Opinions among study participants were divided: while some emphasized that Chip-and-PIN authentication addressed the security flaws of signature-based methods, others stressed that the entry of a PIN only shows that the person presenting the card knows the PIN, and not necessarily that they are its legitimate user. Some participants appreciated that transactions happened faster than with signature, but felt that Chip-and-PIN shifted the responsibility for fraud from the retailer to the customer. Murdoch et al. [23] investigated whether it is feasible for bank customers to comply with their banks' terms and conditions in the first place, or whether the stated requirements are unreasonable. Their results show that in most cases the terms are too vague to be testable and advice can even be contradictory. Their survey respondents had an average of 2.53 payment cards and 2.28 PINs.

Paul et al. [24] used ethnographic methods to study user behavior and perceptions in the context of smartcard-based authentication (as opposed to payment) systems. They found that personal opinions were largely subjective and benefits-driven rather than derived from actual security gains from smartcards. In this study, new smartcards and a new authentication procedure were provided to users, meaning the experience was potentially a very new one. Negative experiences were largely the result of a lack of applications that support the new smartcard authentication procedures. In contrast, Krol et al. [21] studied the *post-adoption* user experience of two-factor authentication for UK online banking using a similar methodology. They found that users were frustrated with hardware tokens, likely due to the pre-adoption vs. post-adoption effects, but further work is needed to confirm this conjecture.

Bonneau et al. [6] conducted a survey of over 1,100 US-based banking customers. They found that 7% of banking customers base their PIN on their birthdays and 21% on some kind of a date. Around 19% rarely or never use their PIN but instead use cash, cheques or withdraw funds in person with a teller. Several participants reported distrust in ATM security, while many preferred signature verification to typing in their PIN, even though almost half of the participants indicated that PINs were their primary authentication method for in-store payments and nearly all (93%) used their PINs on at least a weekly basis. Borzekowski et al. [7] examined US consumers' behavior with respect to debit cards. They found that 'security' led participants to use debit cards rather than cash, and that customers whose banks charge PIN fees (debit-and-PIN costing more than debit-and-signature) were discouraged from using debit at all if debit-and-signature was not accepted at the point of sale. In a more recent study, Kosse [20] found that payment choices by Dutch consumers were strongly influenced by the perceived likelihood of "payment incidents" and individuals' past histories: the majority of participants used credit cards less than once a month (45%) or never (32%) and viewed them as unsafe to carry compared to cash.

Prior work has also focused on various vulnerabilities of EMV. Anderson et al. [4] were among the first to investigate the security properties claimed by EMV technology and highlighted several flaws, including (i) skimming by exploiting Static Data Authentication (SDA) from offline POS, (ii) downgrading the Cardholder Verification Method (CVM) of

a card using a relay attack, (iii) man-in-the-middle attacks to capture PINs, and (iv) power analysis to recover PINs. Adida et al. [3] developed a POS skimmer prototype implementing PIN eavesdropping on SDA-supported cards and described possible phishing scenarios for chip-enabled cards. Just and Aspinall [17] also presented an attack on the EMV back-end API, while Drimer et al. [11] introduced another PIN skimming technique by exploiting poor tamper resistance of Chip-and-PIN terminals. Finally, Murdoch et al. [22] showed that Chip-and-PIN cards can be used without knowing the PIN.

III. Background

A. Overview of payment methods

EMV (Europay, MasterCard, Visa) cards, commonly known as Chip-and-PIN, have embedded microprocessors (chips) which communicate with POS terminals and ATMs through direct contact with the card-reader. EMV payment requires inserting the card into the reader, which then either requests the customer to (physically) sign a receipt or enter their PIN to complete the transaction. EMV standards also support *contactless* transactions, where a dual-interface card includes both a contact interface (chip) and a contactless interface (typically an embedded antenna).

With increased financial loss due to card fraud, EMV is increasingly adopted in cards and POS terminals. According to EMVCo, there were 1.62 billion EMV-compliant payment cards in use across the globe in Q4 2012. In 2014, 29.74% of global transactions were EMV. Eighty countries are in various stages of EMV chip migration, including countries in North America, Europe, Latin America and Asia.[1] The US is one of the last countries to migrate its payment systems to EMV, although banks have been issuing Chip-and-PIN cards for years without requiring the usage of Chip-and-PIN at POS. The deadline for no-penalty EMV adoption for US retailers and banks was October 1, 2015,[2] although whether or not any punitive action has taken place for non-compliant parties is unknown as of December 2015.

B. Fraud and liability in the UK and US

In the UK, Chip-and-PIN cards were first introduced in 2004 and made mandatory in 2006. They enforce a 4-digit PIN and are backwards compatible by design, meaning that they can be used (by signing a receipt) in countries that have not yet introduced Chip-and-PIN. RFID-based contactless cards were introduced in 2010–2011, so that customers can make payments by tapping the card on the POS. As of January 2016, the spending limit for contactless transactions is £30 (up from £20 in September 2015). Another contactless payment technology available in the UK (since July 2015) is Apple Pay, currently supported by 70% of UK cards [15].

In 2014 in the UK, fraud from stolen cards amounted to £59.7M, £47.8M from counterfeited cards, £10.1M from cards intercepted in the postal system, and £331.5M from Internet transactions [27]. The additional cost of processing card-not-present transactions falls on the merchant, while that of card-present transactions falls on the banks. Merchants often have no contract with the cardholder that would allow the cost of fraud to be passed on, whereas banks may claim that the customer has been negligent in protecting their PIN (e.g., writing down the PIN and keeping it with the card).

In the US, debit and PIN, debit and signature, and credit and signature payment methods have been around for many years. In-person debit-and-PIN purchases require the customer to enter their debit card PIN like they would for ATM transactions, although occasionally signatures may be used in place of the PIN. A brief history may be found in [7]. RFID-based contactless cards have been slowly making their way into consumers' wallets since before 2003, but have not gained significant prominence until recently, when they have had to compete with e-wallets such as Google Wallet and Apple Pay, possibly due to consumers being largely unaware that the technology had already been incorporated into their existing cards [13]. According to a report by Aite Group, credit card losses have been stable over the past few years while debit card fraud have been on the rise [1]. It is estimated that the US suffers a loss of $8.6bn per year due to card fraud, which is 0.4% of the $2.1 trillion card payment industry. Although US card users are accustomed to debit-and-PIN transactions, the PIN-debit fraud rates have increased more than threefold between 2004 and 2010, growing from 0.003% to 0.013% [19].

US card regulations favor consumers, although it is not necessarily clear whether consumers have a good understanding of the details, and this status quo may change with the introduction of Chip-and-PIN cards and compliant POS terminals [5]. Federal Reserve regulations E and Z cap consumer liability for fraudulent debit and credit transactions at $50 (except in the case of debit transactions wherein the customer did not promptly notify the bank of a lost or stolen card, in which case the limit is $500) [23]. It is not relevant whether the customer was negligent for the purposes of liability, and the only way to refuse a refund is to show that the customer actually authorized the transaction or authorized someone else to perform it. This imposes a high burden of proof on the bank and so fraud victims are generally refunded (banks usually contractually waive the $50 limit in order to advertise "$0 fraud liability").

IV. Methodology

A. Study goals

We aim to compare experiences with, and perceptions of, different payment methods across UK and US customers. More specifically, UK users are mostly accustomed to Chip-and-PIN and contactless payments for both debit and credit cards, while US consumers have only now started to be exposed to them [5]. Therefore, our study also analyzes the impact that Chip-and-PIN technology could have on US customers as adoption grows as we examine the experiences of UK participants. Finally, we examine the perceived shift (if any) in direct or indirect financial risks that can arise from different payment technologies.

B. Procedure

Our study was conducted by means of 30-minute semi-structured face-to-face interviews at UCL (London, UK) and KSU (Manhattan, KS). Upon arrival, participants were asked

[1] http://www.smartcardalliance.org/publications-emv-faq/

[2] https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/index.jsp

to read an information sheet and sign the consent form, and were encouraged to ask any questions they had about the study.

Interviews started with a brief questionnaire about participants' backgrounds (including whether and how long they have lived in the US and the UK), what kind of technology-related experience they had, and the computing devices they owned and used regularly. Then we asked about their shopping habits (e.g., offline, online, catalogue), leading to which payment methods they used for each type of purchase. The interviewers followed the natural flow of the conversion but made sure to: (i) cover both online and in-person shopping habits, and the way the individual uses the payment mechanisms available to them within their routine payment and banking activities (including paying bills); (ii) elicit individual comprehension of payment processes and the perceived effort and the impact of using various payment mechanisms; (iii) ask about any direct or indirect recollections of both suspected and actual fraud, and any related interactions with banks and retailers; (iv) for UK participants, ask if they had any experience of non-Chip-and-PIN payment methods either from trip abroad or from before its introduction in the UK; and (v) for US participants, ask covert questions (e.g., Does your credit card require a PIN? Does it have a chip?) to understand if participants (knowingly or not) had any hands-on experience of using Chip-and-PIN payment cards either in the US or from foreign trips.

At the end, UCL participants received £10 for participating in the study, while KSU participants were given $10. Note that, while £1 roughly equals $1.50, we decided to keep these amounts, as they are typical of similar university studies with interviews lasting under an hour. (Also, costs of living in London are significantly higher than in Manhattan, KS.)

Research ethics. The study underwent a standard ethical review process at both universities (UCL Research Ethics Committee's approval number 3615/006; KSU Institutional Review Board's approval number 7715).

C. Participants

Recruiting and sampling. The study was advertised in the UK through the UCL Psychology Subject Pool and in the US through a mailing list to all staff and students at KSU. Interested individuals were asked to fill in a pre-screening questionnaire collecting basic demographics and individuals' use of different payment methods. Over 180 individuals filled in the questionnaire in the UK and 94 individuals in the US. Participants were sampled to ensure a good representation of different groups of people based on gender, age, and the payment methods they used. We chose participants so that the samples were demographically comparable between the two countries by having quotas for gender and different age groups.

Demographics. A total of forty participants took part in the study, twenty in London, UK and twenty in Manhattan, KS. Mean age was 38.4 (range: 24–65, SD=12.8) for UK participants and 36.5 (range: 20–65, SD=13.56) for US participants.

UK participants had, on average, 1.5 debit and 1.3 credit cards. Note that we only counted actively used cards and only UK cards (as participants reported having cards in other countries). Four participants had no UK credit cards. Two participants said they had at least one card, which we count as 'one', therefore the average may be skewed by participants saying they had 6+ debit and 5+ credit cards.

For US participants, the average number of cards per participant was 1 debit card and 1.25 credit cards. Unlike UK participants, no US participants reported having foreign cards and no participants reported having multiple debit cards. Two participants reported having more than one credit card which we count as 'two'. Three participants did not have any credit cards at the time of interview, while two participants had 3 and 4 credit cards, respectively. In several ambiguous cases, we concluded as a result of participants' detailed comments that they had one debit card and at least one credit card.

V. Results

This section presents the results of our study. Interview recordings were transcribed and coded using thematic analysis [8]. There was one coder for US transcripts and two coders for UK transcripts, and a common codebook was maintained and revised throughout.

A. Purchasing habits

As discussed in Section IV-B, we asked study participants about their purchasing habits. We found that nine UK participants bought items online in order to get the lowest price, and two used shopping websites just to research prices (without necessarily buying items). Ten US participants used online shopping for at least half of their purchases. P:US02 explained:

"Purchasing things online has saved me a lot of money and it's been very convenient as well, so it's worth the risk."

P:US02 and P:UK12 also appreciated the increased availability of items online and two UK participants enjoyed the ease of getting items delivered to their house. Seven UK participants tried out items (such as clothes) in a physical shop, which then nudged them to purchase items while in the store, while four others would examine items in-store then purchase them online. In-store purchase was quite popular among US participants too and seven participants used in-store purchase more than 50% of the time. Nine UK and five US participants reported buying regularly-purchased or perishable items (such as groceries) in-store.

Three UK participants who regularly shopped online reported it was easier to buy things online since transactions did not feel as "real". For instance, P:UK03 explained:

"it's not a real transaction. I know it is, I know the money is going to come out but psychologically if you just pop your details in, it doesn't feel like you are spending money."

Three US participants regularly used their smartphones to buy items online:

"Especially the Best Buy app… I'm buying a lot of things, especially when school time starts… and when I know I need certain things, my computer, whatever… " (P:US10)

Three UK participants explicitly avoided using certain kinds of card technology, as P:UK12 explained:

"I've avoided [contactless], none of the cards I've been issued with is contactless, I just prefer to have some control."

The role of rewards schemes. A number of participants noted being incentivized to use particular payment cards or smartphone shopping apps. Ten UK and two US participants changed their shopping habits – and in the case of two UK participants, which card they used – based on the rewards or loyalty schemes offered by card providers and retailers [14]. P:UK01 was considering leaving their bank to avoid a cumbersome authentication process for online banking and to open a different account with more rewards, but they were rejected due to their employment status:

"it's just such a laborious process logging in. I don't really like it. I have thought of leaving that bank and trying another one but I couldn't because I'm unemployed, my status is quite low. I think I was rejected, it was about two months ago. But the incentive there was you got a hundred pounds for changing the account plus you got five pounds a month for being with them. So it would have been more money as well."

P:US04 preferred to use a credit card for most of their purchases but used their debit card at least ten times in a month to receive the higher interest rate incentive offered by their bank. P:US01 chose to pay with a credit card for the majority of their transactions in order to use a cash back offer from their credit card company. They elaborated:

"[. . .] I heard that in this country you have to build credit to buy bigger stuff later. . . yeah that's one thing and then they have like cash back things that was interesting for me. . . "

Online security measures. Participants took a range of measures to feel secure when shopping online. Three UK and four US participants actively avoided storing their payment details with shopping websites while another US participant did not appreciate when online retailers were able to draw funds without explicit permission. Four UK and seven US participant used – or stored their details with – sites they felt were trustworthy or had reasonable privacy terms and conditions. P:UK16 stated:

"I trust Amazon so I'm okay with them saving my bank details, whenever you choose a [new delivery destination] they ask you to put your details in again. . . whereas other shops if I just buy a one-off thing I wouldn't save my details."

P:US04 also had a similar attitude, as they chose to store information in places where they made *"pretty consistent purchases, like Amazon."* Six US and one UK participants deliberately avoided using their debit cards online, while four UK and one US participants thought linking of payment details with a shopping website account was convenient:

"On Amazon it saves my details, I don't have to have my debit card on me to purchase which is handy. You just put in your security code and you're done." (P:UK03)

One UK and three US participants reported using smartphone shopping apps. P:US12 explained:

"I do have the Amazon app and I do use Victoria's Secret app to purchase stuff. . . so I think those were the two I have. . . I use the credit card for the apps. . . I think I already stored card information in the apps and there's the 'one click' thing. . . "

P:US12 also reported their own strategy for online security, saying:

"I made it pretty safe. . . I mean. . . I don't give away my credit card information and I don't use the private. . . like other people's Wi-Fi whenever I do pay something, I use my own data plan."

In-store shopping and cash. Seven UK and ten US participants felt less concerned about making in-store purchases than on-line purchases, with four UK participants noting that payment in person made it easier to resolve trust concerns:

"I'm doing it in-person and I am holding the card and if something happens to go wrong, and I would definitely know where to go. . . and not to mention you would actually remember the person who did it for you. . . " (P:US10)

However, P:UK07 was concerned that a shopkeeper could tamper with a card-reader, which may go unnoticed:

"I guess [the merchant] could install something to get your data, but I guess its difficult, but not impossible."

Whereas, P:UK11 noted that advances in self-service tills and card-readers can leave shoppers stranded:

"I see it all the time people standing there stranded because [a machine] is not working, a technical hitch or electronic communication goes down, the world just stops, it's very far from convenient."

A US participant expressed concern that their transactions might be intercepted, whatever precautions they might take:

"[. . .] see, maybe you can be responsible for your information and take care of it as much as you can but seems it's going from the point-of-sale to some place to some place, somewhere over there it could be intercepted and it's out of your control and it creates a problem for you. . . " (P:US11)

Finally, a number of participants felt that using their cards abroad was problematic, although three UK participants reported being able to withdraw cash from ATMs in other countries without problems. Three UK and two US participants attempted to limit potential problems with using cards abroad by notifying their banks in advance – this also helps with preventing cards from being blocked (see Section V-I).

B. Payment methods – Credit cards

Six UK and seven US participants reported using credit cards for online purchases. Five UK participants did not use their credit card online as some websites add extra fees, and opted for using their debit cards instead. Four UK and four US participant said they used a credit card for in-person purchases – six of them actually preferred credit cards whether it was online or in-person. Two US credit card consumers felt using them was risky, if the card were to be lost or stolen. Conversely, four US participants thought that using credit cards was more secure; P:US08 explained:

"I feel more secure with the credit card because I've had my credit card number stolen in the past and I know that when that's happened I can call them and they will, you know, revoke the transaction and I don't have to worry about paying for something that I didn't buy."

Choosing to use credit rather than debit cards is, somewhat unsurprisingly, also influenced by price; two UK and one US

participants reported using credit cards only for high-value items. P:US15 used their credit card only for emergencies:

"I use the credit card for strictly emergencies, usually it's like gas for vehicles or something... sometimes I pay bill with it if I'm... short of money... it's just strictly for emergencies..."

A small number of UK and US participants only used their credit cards occasionally, relying mostly on debit cards instead.

Four UK and two US participants instead avoided using credit cards owing to the fear of finding themselves in debt. Three US participants used credit cards as a "buffer":

"I feel more secure with a credit card... I feel like their's more of a buffer in there... And I feel like at least for my experience working with credit card companies, they're going to help you rectify the situation if something did take place fraudulent." (P:US04)

C. Payment methods – Debit cards

Nine UK and five US participants used debit cards as their main method of payment, with one and two of these participants, respectively, used their debit card in order to get cash back in-store. Two other UK participants noted only using a debit card for in-store or small purchases, and two more said additional fees charged in-store nudged them to only pay with cash. This is line with our results in the context of credit cards.

Six US and one UK participants felt it was risky to use debit cards, as they are directly linked to their personal bank accounts, but they used them anyway. P:US17 explained:

"... with a debit card, it's more taking out of your account, more instantaneously..."

D. Payment methods – PayPal

Ten UK and eight US participants also mentioned PayPal as a payment method they used online. Two UK and two US participants pointed to PayPal's customer protection scheme and said it made them pay with PayPal for riskier purchases, for example with sellers of unknown reputation:

"I usually try to pay with PayPal instead of getting whatever XYZ company it is my credit card, when I don't know how reputable XYZ company is..." (P:US04)

In terms of usability, two UK participants stressed that PayPal required them to enter a password, which made the transaction less smooth than when paying by card; P:UK02 explained:

"Say I bought something from John Lewis,[3] [...] with PayPal you need to put in a password. It would take you to PayPal and they will ask you for your PayPal password and you will just check your card details and everything and then you confirm. I prefer when I just buy something from John Lewis and I just put in my card details and they take the payment."

[3] A chain of department stores in the UK.

E. Card technology – Chip-and-PIN

Perceptions of Chip-and-PIN. Throughout our interviews, we found that most US participants had not been exposed to the Chip-and-PIN technology, although they were all familiar with using PINs for debit card payments or ATM cash withdrawals. Seven US participants reported to have chip-enabled cards which were shipped with no PIN, and did not know whether or not the cards should actually have a PIN:

"I don't know... I honestly don't know what that chip is for. I don't know!" (P:US08)

Another US participant zeroed in on the differences of using a magnetic stripe versus a chip-enabled card:

"It didn't require a PIN but you put the credit card into the machine a different way and you leave it there until the entire transaction is over." (P:US07)

In contrast, six UK participants said that Chip-and-PIN was convenient and otherwise straightforward. Two UK participants felt that the technology was not secure until they had changed the provided PIN while two others actually felt that Chip-and-PIN is more convenient than signing for card payments. Two others felt that Chip-and-PIN is more convenient than signing for card payments.

We also investigated the perception of Chip-and-PIN's security. Ten UK and three US participants felt that it was "secure" or "secure enough", but for some it came at a cost:

"Chip-and-PIN does seem secure but incredibly impersonal, the swipe-and-sign is again you're actually signing and enacting something as a human being rather than being a machine." (P:UK12)

Nine US participants expressed positive attitudes toward PIN-authenticated debit cards transactions, owing to their effectiveness against fraudulent activities. For those US participants who were less familiar with Chip-and-PIN technology, one thought it would add more security, while another was concerned that PINs are vulnerable to shoulder-surfing. Similarly, one US and one UK participants felt that PINs are vulnerable to guessing.

Perception of Chip-and-PIN – Infrastructure. Two UK participants noted that they actively covered the Chip-and-PIN terminal when entering their PIN and three actively ensured that they had the card-reader in sight throughout the payment process. Three UK participants also felt that card-readers at different retailers or locations behaved differently, providing an inconsistent experience. P:UK18 told us:

"maybe its just my local [supermarket] that's really quick, [...] maybe the Internet connection in the area is quick."

One UK participant also shared their experience with a retailer not knowing what to do when the payment process did not go smoothly:

"I bought something in the supermarket the other day with the credit card and I had to sign, [the staff called someone over, they didn't know what to do]." (P:UK7)

Coping strategies – PINs. All UK and US participants had experience of managing PINs for payment cards (specifically,

debit cards for US participants). Five UK and one US participants understood Chip-and-PIN as 'something you have' (the card) and 'something you know' (the PIN), with three UK participants who had used PINs highlighting that using the PIN reinforced memory recollection:

"the [PIN] I don't use much is more difficult but I do know it, my credit card number I [know] a bit less because I don't use it that much." (P:UK06)

The experiences of managing card PINs in practice varied across both UK and US participants. Two UK participants reported that remembering their PINs was difficult. Five UK and four US participant kept the original PINs that came with their cards, with two UK participants saying that they had developed a strategy for remembering all of their PINs, for example, by making all their PINs the same, or related to a memorable number or date – which is consistent to findings in [6]. Seven UK participants proactively took action to make the process more manageable by changing the PIN to something they felt was more memorable, as P:UK14 explained:

"It's taking control of your own finance. In case there was any discrepancy in the security in the initial moment where they are issuing the PINs, I think it's a good idea to change that and to use your own PIN and there is the convenience of having some personal number which you can memorize. And I know birthdays are the most insecure things to use but it works for me."

One UK participant changed all of their PINs to the same combination of digits. Participant P:UK09 was conscious of the potential impact of taking action to make recall of PINs easier, noting that they ensured that all of their PINs were different, never wrote them down but this had consequences:

"I find the PIN on the credit card really really terrible [. . .] and I forget it constantly because I don't want it to be the same as my debit card's."

Twelve US participants noted changing their debit card PINs.

F. Card technology – "Swipe-and-Sign"

Seven UK participants felt that authorizing a payment with a signature was less secure than Chip-and-PIN, in particular, three in the UK and three in the US stated that signatures are easy to forge:

"Chip-and-PIN is just a lot more sensible. I think it's because it's a lot more encrypted and not so open to abuse. People can always forge signatures." (P:UK09)

Additionally, one UK and nine US participants mentioned that signature is rarely checked when they pay anyway:

"well I think the signature thing is completely ridiculous right now. . . nobody checks it. . . now with electronic pad. . . you don't even make the signature really how you supposed to be. . . I think that one is completely outdated and should be replaced somehow." (P:US11)

Physical wear of the cards was mentioned too, with two UK participants stressing that the signature or the magnetic stripe can become unreadable with time.

No US participants actually expressed positive views on the security of Card and Signature, which may naturally be due to the lack of alternatives to compare. UK participants, being exposed to both technologies, were in a better position to make such a comparison: although negative views on the security of Card and Signature outweighed the positive ones, one UK participant emphasized that having human contact while authorizing a transaction made them feel more secure. Also, P:UK04 found it was more fun to use it, explaining:

"it's exotic in a way to go to another place and having to do something every-day and mundane differently."

G. Card Technology – Contactless

No US participants were familiar with contactless cards; comments in this subsection are from UK participants only.

Perceptions. Eight participants appreciated the convenience of using contactless cards. P:UK09 stressed it is better than Chip-and-PIN since they do not have to wear glasses to pay:

"I really like contactless, I'm so into contactless, that is just great. Especially now since I have to wear glasses all the time. Because you just go "brmmm" and that's it. Because I'd have to go and put my glasses on and make sure I put the correct PIN in and everything. So for older people it's a real godsend."

However, four participants felt it was not as secure, with six emphasizing that the easy authorization step might allow accidental or fraudulent purchases. In fact, some were surprised that banks allow such a low-security payment method and found this inconsistent with their general stance on security:

"If they were really serious about security, then. . . I mean it's nice to have it and I use it but obviously it's a loophole, I mean they aren't being consistent with their approach." (P:UK01)

Adoption. Six participants stressed that not every POS supports contactless. P:UK14 explained this was the reason why they had not used their contactless card yet:

"I haven't just got round to it yet. It's not widespread enough for me to use yet."

Two participants expected that routine use of contactless payment would become the norm, with P:UK18 explaining that they ended up using it without initially intending to:

"[I use contactless] if I'm in a hurry, but some of the cards are old some of them are new."

Two participants also mentioned that one can lose money learning how to use a contactless card. Contactless cards can be used in London to pay for public transport and there have been campaigns alerting passengers to avoid "card clash." For example, passengers should not tap their whole wallet on the reader since the wrong card could be charged (e.g., not their travelcard but their contactless bank card). P:UK15 reported the experience of intending to pay with the London Oyster travelcard but ending up being charged on their bank card. Luckily, the issue was resolved and the charge disappeared before he could complain:

"On my card statement, it showed that a £4 fare got off at the exact time I travelled and I thought I'd sort it at the weekend but by then the money got back on again because for some bizarre reason they realized they'd made a mistake."

H. Managing banking mechanisms

Online banking. Many UK and US participants used online banking for a range of activities such as checking their account balance, setting up regular payments, and transferring funds. P:UK12 noted that they used online banking because there was a lack of local branches:

"you're kind of forced to these days, time-wise and service-wise, anything you want to deal with, a pension or a driving license or a bill, all the regional offices are closed or gone."

Eight US participants reported using online banking on a daily/weekly basis, primarily for checking balance and statements, while three of them also used online banking for fund transfer across accounts and/or utility bill payments. P:US12 said that they used online banking service for electronic cheque deposit, thus trying to avoid visiting bank:

"I check my bank account stuffs usually through online banking and never go to the bank... I use mostly for transfer, checking if my cheque coming like the deposit coming and stuffs."

Eight UK participants said that they had good experiences when accessing and using online banking services, three emphasizing that it saves time. However, three other UK participants felt that it was difficult to complete all of the authentication steps, in line with the findings in [21]. Two UK participants complained that the token required to access an online bank account created problems of its own, and three felt that the extra security steps didn't make them feel any more secure. Two UK participants did not feel that banking on their mobile would be secure, while at least one US participant instead relied on their phone to ensure secure banking.

Combining payment mechanisms. Several participants reported different ways of delegating purchases to others (which, at least in the UK, is a violation of terms for most banks [23]). Six UK participants said that with PINs it was possible to give their card (and their PIN) to someone they trust, to make purchases on their behalf (or, in some cases, for themselves):

"I wouldn't have any qualms giving my PIN to friends if I've known them a few years and know their calibre." (P:UK11)

In contrast, three UK participants said that they had no reason or want to share their PIN with anyone. P:UK12 had a partner who signed an informal note authorizing the participant to use their card wherever a signature was required (while living in the US). Signing for a purchase was seen as useful if a PIN had been forgotten (P:UK05) or if the card chip itself had malfunctioned (P:UK03). One US participant used gift cards to make purchases at their favored online shopping portal:

"When I shop on Amazon there's multiple sellers on there and you don't know the other person you're buying it from, so that's why I like to use gift-cards so... Because I trust Amazon with that information but I don't trust some of the sellers that work on Amazon..." (P:US05)

Several US participants observed that, when in stores or at restaurants, staff would only check the signature if it happened to be in a big city, or for a high-value purchase. Those using foreign bank cards – certainly in the UK – found that if the card was not chip-enabled, staff in a shop would often be caught unaware, choosing then to ask for a signature.

I. Fraud

Experiences of actual fraud. Five UK and six US participants reported having experienced actual fraud on their accounts. P:UK03 was puzzled how fraudsters were able to make purchases when they lost their Chip-and-PIN card even if they did not know the PIN:

"they'd spend about £600 at certain stores that I didn't know what they were because it's Spanish. And the bank said that the PIN number had been entered. So I had quite an argument with them about claiming that money back because from them point of view, it could only have been me but I got it back in the end."

In general, participants were not worried about fraud as long as they received a refund, P:UK01 explained:

"I noticed that somebody had bought two washing machines, it was about £350 worth. I just rung them up and I they produced various forms that I had to fill in, it took about two months to get the money back. [...] It didn't really bother me as long as I got the money back. It was just a case of being nervous and worried for a few weeks."

Every participant was able to get their money back, although for one UK and one US participant it required significant effort.

Banks' response to fraud. One UK and five US participants reported that their banks successfully prevented fraud on their account, while eight UK and two US participants had their card blocked because of their own activity. P:UK03 travelled through South America and, despite having told their bank beforehand, had their card blocked as they attempted to use it:

"I travelled a little bit through South America, entering different countries [...] if I crossed a border and went to Bolivia, again it wouldn't work and I had to ring them again saying "I'm sorry I'm still overseas, I'm going here. Can you please unblock the card?" So that was a bit of a pain but again quite reassuring that they keep an eye on what I was doing."

Overall, five UK and two US participants felt that although having their card blocked was frustrating, they were happy to see their bank was monitoring their account and flagging up any suspicious activity. P:US12 explained:

"[...] a lot of time when I make purchases in a foreign country, they would give me a call before the purchase go through... they called me, after I made two trials, there was like 'are you making this purchase' and I 'yeah,' and 'okay, we'll let it through then'... I think that's a really good way to make sure that there's no fraud going on."

Presumptions about fraud. Many participants had not experienced fraud personally – in fact, two US participants felt secure for not having experienced any fraud:

"I have been accessing it for several years and I haven't had a problem. And so far I haven't been in any of the things that have been hacked." (P:US15)

Generally participants were unsure if the customer or the bank were liable in the case of fraud. Nine US participants openly stated they did not know who was liable, while eight UK participants used credit cards with an assumption that there was

some form of purchase insurance that covered losses attributed to fraud. Three UK participants expected they might not be reimbursed in case of genuine fraud. Three UK and six US participants thought that the person who was defrauded had no personal liability for the money taken.

When asked about the consequences of fraud, most participants expressed concern about their account being emptied, with three US participants worried about the damage to their credit score and a further three about identity theft:

"[. . .] they could use my identity to make other purchases like car loan or mortgage or something. . . so yeah, it could be very expensive. . . paper work would be horrendous." (P:US16)

J. US-UK commonalities and differences

In the UK part of the study, there were three participants who spent time living in the US and therefore had first hand experiences of using both systems. P:UK10 (who was born in the US and maintains accounts in both countries) stated:

"Banking in the US is a completely different thing because they are just starting to have Chip-and-PIN, just now which is absolutely ridiculous."

When asked about paying for goods in the US, they explained:

"It's very rudimentary. You have to sign pieces of paper, sometimes they have to run it through like this –gesture–. *I don't know if you've seen that thing. You put the card in and you run it and all. [. . .] Sometimes you have to swipe it and it doesn't swipe properly. I've had that so many times. I think Americans just tend to use cash a lot more, I don't know why, they are just really funny about that, they are just very suspicious about not having their dollar bills in their hand."*

P:US10 was a prior resident in the UK and compared their payment experience in the US with that of the UK, saying

"The only thing I will say is that in the US there's not been a time when I've come in a shop and they swipe my card and then just automatically. . . doesn't ask me for my PIN. In the UK, it's always PIN, PIN, PIN. But here, it's like you swipe and then it's done. . . You just swipe and then it would say 'Do you want cash back?' or anything like that. . . "

VI. Discussion

Adjusting behavior to habits and experiences. Across the two participant groups, there was a range of efforts made to adapt use of payment mechanisms to the individual's own habits and experiences. In some cases, they did so to achieve some sense of security and/or trustworthiness. A few UK participants even refused to adopt contactless cards, with some opting to maintain accounts and cards they had already set up (or would require time time and effort to switch from). Many participants in the UK and the US actively changed the PINs for a range of cards as an effort to reduce the number of PINs to memorize, or otherwise relied on regular use of a card to reinforce the PIN in memory. As Chip-and-PIN becomes more widespread in the US, more customers may choose to employ such strategies. Krol et al. [21] found that banking customers actively switch their account to another banking provider if the security procedures that permit access to their funds become too arduous.

Rewards and loyalty schemes. Another interesting finding is that for many participants in the UK and the US, rewards associated with banking providers, credit cards, and shopping outlets are often the primary criteria in choosing the payment method, more important than their security or ease of use. Rewards and loyalty schemes also influenced payment habits and – as in the case of P:US01 – willingness to use mobile devices for shopping and payment. Reward programs have an especially strong influence on US consumers when choosing credit and debit cards [14]. For example, P:US04 tried not to use debit cards as often as credit cards, but was incentivized to do so anyway in order to get better interest rates.

Participants associated measures of trust with established or familiar brands (e.g., Amazon), with participants feeling comfortable storing their account details with these popular services where establishing trust online was otherwise seen by many as a challenge. This is somewhat in contrast to some findings from prior work: for instance, Bonneau et al. [6] reported that individuals distrust ATMs to the point that they would not even know their PIN. Their survey results show that around 19% rarely or never used their PIN, relying instead on cash, cheques or withdrawing money face-to-face in a branch.

Feeling protected. Occasional contact with banks seemed to assure participants that their finances – and their financial well-being in turn – were being looked after, regardless of what that contact was. Many who had legitimate transactions denied were naturally frustrated but felt it was for their own good, in some cases seeing it as the primary indicator that their bank was actively combating fraud. For the majority of US participants, there was a presumption of zero liability on the part of the customer in the event of fraud being committed on their accounts, suggesting that it was in the interest of the banks themselves to remain alert.

New payment systems. As chip-enabled cards are starting to be deployed in the US, and contactless cards now widespread in the UK, it is interesting to shed light on the effects of these new technologies. At least in the UK, the apparent ease of use of contactless was the same characteristic which made it equally easy for participants to make mistakes while learning how to use the technology. When making in-store payments, the same card-reader could accommodate payment by either Chip-and-PIN or contactless, which had the potential to be both familiar and confusing. A similar journey of familiarization may be seen in the US if for instance cards are rendered unusable after successive failed PIN entries and people are not told that this can happen to them (as did happen for one UK participant, P:UK6). Combined with staggered or 'patchy' technology deployment, individuals can have differing experiences from those around them, compounding the challenge of understanding how technologies operate. They may then develop "Folk Models" [28] of how the technology works, and equally what is expected of them as customers (as with the terms and conditions of managing their accounts [23]).

Limitations. Ours is an exploratory study of user perceptions of payment methods in the UK and the US. As such, it presents a few limitations, such as the fact that we interviewed participants in two areas that may be appreciably different in terms of urbanization, as Greater London has a population of over 8.5 million people while around 135,000 people

live in the greater Manhattan (Kansas) area. In both cases, participants were relatively well-educated and most had their own computer, even though these samples may not be fully representative of the general UK and US populations.

VII. Conclusion

This paper presented an exploratory interview-based study of attitudes and perceptions of payment methods. We recruited forty participants divided equally across the UK and the US, aiming to compare across financial cultures. We found that purchasing habits as well as the availability of rewards schemes are primary criteria influencing payment choices. Interviewees reported on a range of measures to feel secure, at times, avoiding new technologies like contactless payment, or trusting popular brands as mediators for payment. They also reported on a number of causes for frustration and shared their coping strategies. When asked about their experience with chip cards, several US participants were puzzled and confused by how to use them, while UK participants found then convenient and/or straightforward, with the extra hurdles giving participants an additional sense of security (e.g., as compared to contactless). Participants were mixed in being satisfied with provisioned banking facilities and motivated to adapt them to their own practices. The factors in these personal decisions varied in how informed they were, suggesting that as new payment mechanisms are deployed – and as new threats emerge – there is opportunity to further tailor the information and assurances given to customers to a range of payment touchpoints.

As part of future work, we plan to conduct a larger, follow-up quantitative study based on the responses from participants in this study. In doing so, we aim to address some of the limitations discussed above, but also to capture the potential of how customers adapt their banking behavior in response to the capabilities of available payment mechanisms. A large-scale survey can also begin to frame the role that communities of customers play in the payment ecosystem, especially in relation to economic devices such as reward schemes or liability insurance. A follow-up study could also be conducted to see if perceptions and payment behavior will have changed with adoption of Chip-and-PIN in the US.

Acknowledgments. The authors would like to thank Brian Glass for helping with a pilot interview, Jonathan M. Spring for feedback on an earlier draft of this paper, Steven Murdoch for technical discussions of different payment systems, and our anonymous reviewers for their thoughtful suggestions.

References

[1] EMV: Lessons Learned and the U.S. Outlook. http://aitegroup.com/report/emv-lessons-learned-and-us-outlook, 2014.

[2] Card and automated payments overtake cash transactions for the first time. http://gu.com/p/494d6/stw, 2015.

[3] B. Adida, M. Bond, J. Clulow, A. Lin, S. Murdoch, R. Anderson, and R. Rivest. Phish and chips: Traditional and new recipes for attacking EMV. In *Security Protocols*, 2009.

[4] R. Anderson, M. Bond, and S. J. Murdoch. Chip and spin. *Computer*, 22(2), 2006.

[5] R. Anderson and S. J. Murdoch. EMV: Why payment systems fail. *Communications of the ACM*, 57(6), 2014.

[6] J. Bonneau, S. Preibusch, and R. Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. In *Financial Cryptography*, 2012.

[7] R. Borzekowski, E. K. Kiser, and A. Shaista. Consumers' use of debit cards: Patterns, preferences, and price response. *Journal of Money, Credit and Banking*, 40(1), 2008.

[8] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 2006.

[9] S. Crane, H. Lacohée, and S. Zaba. Trustguide – Trust in ICT. *BT Technology Journal*, 24(4), 2006.

[10] E. De Cristofaro, H. Du, J. Freudiger, and G. Norcie. Two-Factor or not Two-Factor? A Comparative Usability Study of Two-Factor Authentication. In *NDSS Workshop on Usable Security (USEC)*, 2014.

[11] S. Drimer, S. Murdoch, and R. Anderson. Thinking inside the box: System-level failures of tamper proofing. In *IEEE Security & Privacy*, 2008.

[12] S. M. Forsythe and B. Shi. Consumer patronage and risk perceptions in Internet shopping. *Journal of Business Research*, 56(11), 2003.

[13] S. L. Garfinkel, A. Juels, and R. Pappu. RFID Privacy: An overview of problems and proposed solutions. *IEEE Security & Privacy Magazine*, 2005.

[14] F. Hayashi. Do U.S. consumers really benefit from payment card rewards? Technical report, 2009.

[15] A. Hern. The Guardian – Apple Pay to launch in UK in July. http://gu.com/p/49gmf/stw, 2015.

[16] B. Howcroft, R. Hamilton, and P. Hewer. Consumer attitude and the usage and adoption of home-based banking in the UK. *International Journal of Bank Marketing*, 20(3), 2002.

[17] M. Just and D. Aspinall. On the security and usability of dual credential authentication in UK online banking. In *International Conference for Internet Technology and Secured Transactions*, 2012.

[18] C. Kim, W. Tao, N. Shin, and K.-S. Kim. An Empirical Study of Customers' Perceptions of Security and Trust in e-Payment Systems. *Electronic Commerce Research and Applications*, 2010.

[19] D. King. Chip-and-PIN: Success and challenges in reducing fraud. 51(4), 2012.

[20] A. Kosse. The safety of cash and debit cards: A study on the perception and behavior of Dutch consumers. *International Journal of Central Banking*, 2013.

[21] K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse. *"They brought in the horrible key ring thing!"* Analysing the usability of two-factor authentication in UK online banking. In *NDSS Workshop on Usable Security (USEC)*, 2015.

[22] S. Murdoch, S. Drimer, R. Anderson, and M. Bond. Chip and PIN is broken. In *IEEE Security & Privacy*, 2010.

[23] S. J. Murdoch, I. Becker, R. Abu-Salma, R. Anderson, N. Bohm, A. Hutchings, M. A. Sasse, and G. Stringhini. Are Payment Card Contracts Unfair? In *Financial Cryptography*, 2016.

[24] C. L. Paul, E. Morse, A. Zhang, Y.-Y. Choong, and M. Theofanos. A field study of user behavior and perceptions in smartcard authentication. In *HCI*, 2011.

[25] Statista. Statistics and facts about credit cards in the United States. http://www.statista.com/topics/1118/credit-cards-in-the-united-states/, 2015.

[26] The UK Card Association. Card Expenditure Statistics. http://www.theukcardsassociation.org.uk/wm_documents/January%202015%20Full%20Report.pdf, 2015.

[27] The UK Card Association. Card Fraud Figures. http://www.theukcardsassociation.org.uk/wm_documents/January%202015%20Full%20Report.pdf, 2015.

[28] R. Wash. Folk models of home computer security. In *SOUPS*, 2010.

[29] B. Woolsey. Plastic transactions overtake cash, check payments. http://preview.tinyurl.com/jpldrmm, 2006.