"Pick Someone Who Can Kick Your Ass" - Moneywork in Financial Third Party Access

BELÉN BARROS PENA, Northumbria University, United Kingdom
BAILEY KURSAR, Touco, United Kingdom
RACHEL E. CLARKE, Open Lab, Newcastle University, United Kingdom
KATIE ALPIN, Money and Mental Health Policy Institute, United Kingdom
MERLYN HOLKAR, Money and Mental Health Policy Institute, United Kingdom
JOHN VINES, Northumbria University, United Kingdom

This paper explores some of the new possibilities for financial third party access that are enabled by "open banking". The term open banking is used to designate the availability of banks' customer data through application programming interfaces (APIs). Financial third party access refers to the mechanisms that facilitate the engagement of others in the management of our personal finances. Engaging trusted others in personal finances may be especially valuable for individuals experiencing financial hardship or life circumstances that place their financial stability at risk. We deployed a new third party access tool enabled by the UK Open Banking APIs for 90 days with 14 people who self-identified as living with a mental health condition. The tool, which was developed by a financial technology startup founded by the second author, allowed participants to select a trusted "ally" who was notified when certain transactions took place in participants' bank accounts. During the deployment, the 14 participants and 8 of their "allies" took part in a diary study and pre- and post-deployment interviews. The experiences of our participants reveal the inadequacy and shortcomings of existing formal third party access mechanisms, and the moneywork involved in financial third party access. We argue that focusing on this moneywork can help us design flexible, proportionate and practice-sensitive services for financial third party access that move beyond discourses of protection and control in order to enable meaningful financial collaboration.

CCS Concepts: • **Human-centered computing → Empirical studies in collaborative and social computing**.

Additional Key Words and Phrases: Digital Financial Services; Financial Third Party Access; Financial Collaboration; Open Banking; Diary Study; Interaction Design; User Experience Design

ACM Reference Format:
Belén Barros Pena, Bailey Kursar, Rachel E. Clarke, Katie Alpin, Merlyn Holkar, and John Vines. 2020. "Pick Someone Who Can Kick Your Ass" - Moneywork in Financial Third Party Access. 1, 1 (September 2020), 28 pages. https://doi.org/10.1145/xxx.xxx

Authors' addresses: Belén Barros Pena, belen.pena@northumbria.ac.uk, Northumbria University, Newcastle Upon Tyne, United Kingdom; Bailey Kursar, bailey@usetouco.com, Touco, London, United Kingdom; Rachel E. Clarke, rachel.clarke@newcastle.ac.uk, Open Lab, Newcastle University, Newcastle upon Tyne, United Kingdom; Katie Alpin, katie.alpin@moneyandmentalhealth.org, Money and Mental Health Policy Institute, United Kingdom; Merlyn Holkar, merlyn.holkar@moneyandmentalhealth.org, Money and Mental Health Policy Institute, United Kingdom; John Vines, john.vines@northumbria.ac.uk, Northumbria University, Newcastle Upon Tyne, United Kingdom.

XXXX-XXXX/2020/9-ART $15.00
https://doi.org/10.1145/xxx.xxx

1 INTRODUCTION

Many people rely on others for support with managing money. Those living with age-related conditions, illness, and temporary or permanent disability may require help with day-to-day tasks like paying bills, withdrawing cash or shopping, and may benefit from assistance with financial decision-making. Minding money has been recognised as a common care-giving task [51]. Support with minding money often involves carers handling financial information and assets belonging to those they help. To accommodate this activity, banks and governments offer formal ways of lawfully granting a third party access to someone else's financial assets. These include, amongst others, power of attorney of the kind usually called lasting, durable or enduring; and bank arrangements for third party access, which are known as "third party mandates" in the UK.

However, research has shown that people often disregard those formal mechanisms and develop instead informal collaboration practices (e.g. [51, 54]), such as individuals sharing bank cards and PINs with carers, or disclosing Internet banking security credentials to them. These practices are risky: they expose asset owners to financial abuse, and carers to false accusations of financial mismanagement and undue influence [16, 53]. There are several reasons behind these insecure behaviours, one of them being the *"lack of fit"* [45] between the design of formal third party access mechanisms and day-to-day financial practices. Formal third party access mechanisms like lasting / enduring power of attorney and third party mandates are essentially binary: they grant third parties *"full access (...) or no access at all"* [54] to financial assets. They lack flexibility and are too blunt an instrument for dealing with everyday financial tasks [16]. The need for flexible, proportionate, practice-sensitive and secure mechanisms for financial third party access has been recognised for well over a decade, but little has been done to address it.

This paper explores new approaches to financial third party access enabled by the technical capabilities of open banking. Open banking allows authorised services to access customers' data held by banks [11], and in doing so it provides new ways of sharing our financial information with others. We specifically examine the potential of open banking for people living with mental health conditions. We focus on mental health because this demographic can draw significant benefits from receiving assistance with money management [6, 32, 34]. The connection between mental health, debt, poverty and financial hardship is well documented (e.g. [18, 22, 30, 41]), although causality in any direction has not been established [30]. The complex relationship between financial and mental wellbeing makes it particularly urgent to develop systems that can support those living with mental health conditions. This group's needs regarding financial third party access are also different from those derived from disability and age-related conditions. The latter are often permanent or degenerative, coming with expectations of increased support over time. By contrast, impairment connected to poor mental health tends to be intermittent and fluctuating [32], with people requiring varying degrees of support at different times. Help may be also required at short notice, reducing the scope for planning [34]. This makes mental health a challenging context in which to explore financial third party access.

We deployed Toucan, a new tool for financial third party access enabled by the UK Open Banking APIs, with 14 people who self-identified as living with a mental health condition. Toucan, which was developed by a financial technology startup founded by the second author, allowed participants to designate a trusted collaborator who was notified when certain transactions took place in the participant's bank account. Participants installed and used Toucan on their smartphones for 90 days, while engaging in a diary study that started and ended with a semi-structured interview.

In reporting on our deployment and evaluation of Toucan, this paper makes the following contributions to the growing body of work on finance in HCI and CSCW (e.g. [16, 39, 40, 44, 47, 48, 56, 57]): i) it demonstrates how support with minding money can be facilitated through the

kind of information sharing enabled by open banking; ii) it suggests a framework for the analysis of financial third party access options based on the interaction between power to transact and information disclosure; and iii) it offers recommendations for the design of new forms of financial third party access, focusing on trusted sharing of financial information and transitioning from designing for financial protection to designing for financial collaboration.

2 RELATED WORK

The notion of "moneywork" [39] has been adopted in HCI to refer to research into *"the work of managing everyday financial tasks"* [27]. The term "moneywork" was initially coined by the sociologist Sandra Colavecchia, who defined it as the *"labour of managing family finances"* [9]. The concept has been expanded by the HCI literature to include *"the physical and social interactions that users make individually and collectively in order to enable transactions"* [27]. The HCI literature on moneywork is still relatively sparse, but growing. Studies have looked into, for instance, the moneywork involved in payment transactions (e.g. [39, 40]); money management practices (e.g. [23, 27]); banking habits (e.g. [3, 16, 44]); household finances (e.g. [47, 57]); and the particularities of managing money when on a low income (e.g. [48, 56]). This paper aims to contribute to this body of research by examining the moneywork involved in financial third party access, an area where the socially situated nature of money [23, 39, 48] manifests itself in a particularly meaningful and obvious way.

2.1 Formal and Informal Financial Third Party Access

Financial third party access refers to the act of granting others access to our financial information and/or assets in order to receive support with money management [6]. This support may involve receiving assistance when making a financial decision or undertaking a financial task (supported decision making); or making decisions on someone else's behalf if they are unable to do so themselves (substitute decision making) [58]. Several formal mechanisms exist to facilitate financial third party access. These include lasting / enduring power of attorney and banks' third party mandates. They are called "formal" because they do not violate government law or terms and conditions from a financial service provider.

Literature studying the financial lives of older adults has uncovered that such formal mechanisms are underused in care contexts. A survey of Australian non-professional carers found that only 15.4% of respondents had a lasting / enduring power of attorney in place, and 18.7% had a third party mandate [51]. The majority of responses indicated the use of what the authors called *"informal processes"* [51]. These included, between others, handing bank cards and PINs to carers, and sharing telephone and Internet banking credentials [51]. Vines et al.'s research with *"eighty somethings"* [54] in the UK identified similar practices, which the authors connected to earlier life experiences participants had of sharing money within households and local communities [54]. Policy-oriented research in the UK with older adults and people living with mental health conditions has reached similar conclusions [2, 5, 6, 17, 34]: those requiring assistance with money matters often disregard formal third party access instruments and instead deploy *"informal workarounds"* [17] and *"coping mechanisms"* [5].

Several such workarounds have been identified in both informal care contexts and residential care settings, but a few of them are especially noteworthy for the risks they entail: the aforementioned sharing of bank cards and PINs, which is used to delegate payment authority and to get access to cash through others [2, 17, 51, 54]; disclosing telephone and Internet banking credentials [17, 51], which allows helpers to set up direct debits and pay bills on someone's behalf; and the use of joint accounts for financial assistance, through which carers can take over financial responsibilities when needed and control spending [34]. These practices help people retain independence [2], but

they also introduce significant risks for both givers and recipients of help [16]. Sharing banking security credentials not only exposes asset owners to fraud and financial abuse: it constitutes a breach of the banks' terms and conditions, and voids all fraud protections as a result [17, 46, 54]. Carers engaging in these practices are at risk of false accusations of theft, fraud [16] and *"undue financial influence"* [53]. When they open joint accounts to enable oversight, carers jeopardise their own financial stability by becoming *"jointly liable for any spending on the account"* [34].

Explanations as to why people adopt these risky workarounds have often focused on accessibility barriers in mainstream banking channels [2, 17, 54]. Research commissioned by UK public institutions has also emphasised the lack of knowledge about formal third party access mechanisms, and the lack of awareness about the consequences of using informal workarounds [4, 5, 17]. Academic literature, however, has reported that people are often aware of the risks they take [44, 46, 54], and has drawn attention instead to the inadequacies of formal third party access mechanisms [16, 54]. These are essentially binary: they grant third parties *"full access (...) or no access at all"* [54]. They disregard the fact that social money practices are not *"all or nothing"* [54] and require greater flexibility. Existing formal mechanisms for third party access are too blunt an instrument for dealing with everyday financial tasks [16].

Furthermore, security and HCI literature has uncovered that these "informal workarounds" happen amongst other groups and in non-care contexts. Sharing passwords in general, including those for personal banking, appears to be common. Dhamija and Perrig's study about image-based authentication found that *"people viewed the ability to share passwords with others as a feature. Almost all participants shared their bank PIN with family or friends"* [13]. Kaye mentions that spouses *"frequently shared bank account details and PIN codes"* [24]. This is backed by research on banking habits. In a study carried out in Australia, Singh et al. report that *"married and de facto couples share Internet and phone banking passwords because they trust their partner and see all their money as joint, irrespective of the form of the account"* [44]. In their research on banking security practices in Saudi Arabian households, Alghamdi et al. uncovered that credential sharing takes place within family circles [3]. Of their 29 participants, 25 shared their cards and PINs with family members. One of their participants described the practice as *"a way of supporting each other"* and *"a kind of solidarity"*. Finally, Singh et al. observe that card and PIN sharing also takes place in remote aboriginal communities in Australia, not just due to difficulties accessing banking services in underserved areas, but also because of cultural norms that establish that *"money is shared with kin"* [44].

This evidence suggests that what have been called "informal" or "coping" workarounds are actually common and widespread, indicating the *"lack of fit"* [45] between the design of financial services and socio-cultural money practices. Formal third party access mechanisms are too rigid and ill-suited to the socially situated nature of our financial lives, and they do not take into account the cultural and symbolic meanings of money. Aggravating the problem, banking infrastructure lacks the tools, technologies and policies to support more nuanced forms of trusted sharing and access [6]. There is a clear need for flexible, proportionate, practice-sensitive and secure mechanisms for financial third party access that facilitate and legitimise collaborative financial behaviours, rather than penalising them. However, banks (especially in the UK) have largely ignored the recommendations from academia and advocacy organisations in this matter [2, 5, 6, 16, 37]. For example, AgeUK, a charitable organisation, has been recommending the deployment of carer cards - additional cards in the name of a third party attached to personal current accounts but with separate PINs and withdrawal limits [2] - since at least 2011. However, the first such cards appeared in the UK only in April 2020, as banks sought to improve support for vulnerable populations during the COVID-19 lockdown [38, 49].

2.2 A Different Approach to Financial Third Party Access

The arrival of open banking initiatives, which allow new services access to information held by banks, could provide opportunities for new approaches to financial third party access [5]. Initiated in the European Union by the Second Payment Services Directive (PSD2) [31], the idea of requiring banks to make their data available through application programming interfaces (APIs) has been adopted throughout the world [35]. In the UK, development of the Open Banking APIs started under the auspices of the Competition & Markets Authority (CMA), which wanted to promote competition and innovation in the provision of financial services, enable customers to better compare and assess products, and empower them to securely share their financial data with third parties [11]. The Open Banking APIs allow UK banks to disclose highly sensitive personal financial data in a way that is compliant with data protection regulations and addresses security and fraud risks. 145 companies are currently registered to use the Open Banking APIs in the UK [28]. These companies have enabled numerous new services and novel integrations [19]. One of them is Toucan, a new financial third party access tool that was designed for those living with mental health conditions.

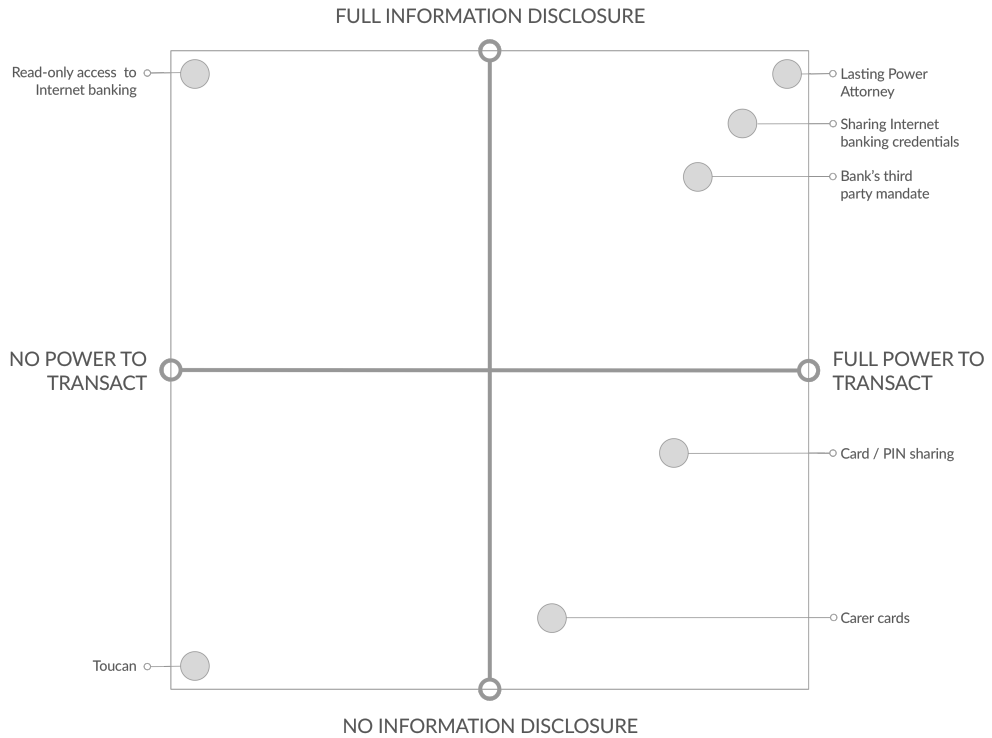

Fig. 1. Financial third party access represented by the axes of information disclosure and delegation of power to transact.

Toucan takes a different approach to financial third party access from the one deployed by the formal and informal mechanisms mentioned so far in this paper. In a report published in 2019, the Money and Mental Health Policy Institute represented financial third party access options as a spectrum that went from delegating total control to providing visibility of information [6]. That single spectrum aggregates 2 different factors that come into play in financial third party access: the delegation of power to transact, and the disclosure of financial information. A representation of

these 2 factors as a set of perpendicular axes, as in Figure 1 above, creates 4 quadrants that can be used to map both formal and informal, hypothetical and existing, mechanisms for financial third party access.

As shown in Figure 1, formal and informal instruments for financial third party access operate across both axes: they disclose most or all financial information to third parties and grant them ample powers to transact. Toucan, however, does not delegate any power to transact, and discloses almost no financial information, enabling in practice a lightweight form of financial oversight. In the next section, we introduce and describe Toucan in detail.

3 INTRODUCING TOUCAN

Toucan is a native mobile application for Android and iOS that allows people to collaborate on money management with someone they know and trust. As opposed to other third party access mechanisms, Toucan enables collaboration exclusively through information sharing: trusted third parties can not access Toucan users' money, or carry out financial transactions on their behalf. This approach derived from the recognition that many people living with mental health conditions fluctuate between highly functional periods and episodes of impaired capacity. Toucan's design aims to facilitate support during the latter, while preserving autonomy during the former.

Toucan was developed by a financial technology startup founded by the second author, and used the Open Banking APIs available in the UK to connect to a user's bank account. Once the bank account connection has been established, users can configure a set of SMS alerts that will be triggered by certain bank account activity. Users can choose to send those alerts only to themselves, or to deliver them also to a trusted third party of their choice. In order to generate the SMS alerts, Toucan checks users' bank accounts for new activity. Subject to the limitations of the UK Open Banking standard, it can only do so 4 times a day, and not in real time. This, together with the 2-to-3 day clearing time for most payment transactions in UK legacy banking systems, means that there can be significant delays between bank account activity and the corresponding alert delivery.

Toucan offers three different SMS alerts: a balance alert, a daily spending alert and a cash withdrawal alert. The balance alert is triggered whenever the connected bank account balance falls below a certain amount. The daily spending alert is triggered whenever the sum of all outgoing account transactions within a day exceeds a certain amount. The cash withdrawal alert is triggered whenever a cash withdrawal over a certain amount takes place. The choice of alerts was based on the results of an earlier survey, where respondents identified running low on money, unusually high spending, and specific transaction categories such as gambling as the financial events that should be notified to a trusted third party. Toucan provides default amounts for all three alerts, but users can edit them to suit their own financial habits. Toucan users can also choose which of the three alerts they wish to activate.

Once the SMS alerts are configured, Toucan users can designate a trusted third party who will also receive Toucan alerts. In the application, the trusted third party is called an "ally". Users can choose which alert types they want to share with their ally. Only one ally can be configured, who can be removed or changed at any time. Users can also skip the ally configuration altogether and use Toucan without a designated ally.

Once added to Toucan, an ally receives an invitation via email that they can accept or reject. If an ally accepts the invitation, they will start receiving an alert whenever one is sent to the Toucan user. Toucan delivers different alerts to users and allies. Alerts sent to users include the alert type, indicating the kind of bank account activity that triggered the alert: low balance, spending or cash withdrawal. Alerts to allies, however, contain no financial details whatsoever: they simply suggest to the ally they should get in touch with the person they support via Toucan. This conservative approach sets Toucan apart from existing financial third party access mechanisms, both formal and

informal, since Toucan neither transfers the power to transact to the third party, nor discloses any financial information to them.

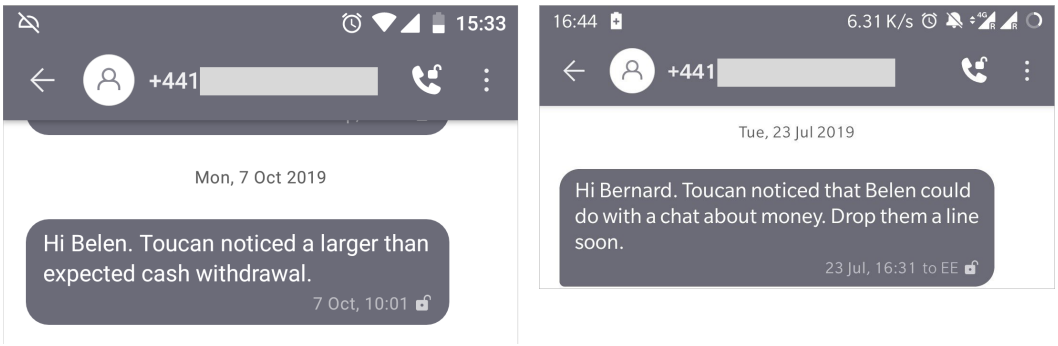

Fig. 2. A sample SMS alert for Toucan users (left) and allies (right). The alerts for allies do not disclose any personal financial information.

We evaluated Toucan through a controlled deployment between July and October 2019. In the next section, we explain how this deployment was carried out.

4 STUDY DESIGN

4.1 Participant Recruitment

We deployed the Toucan mobile application for 90 days from July to October 2019 with 14 people who self-identified as living with a mental health condition. The study also engaged with 8 of their chosen allies, for a total of 22 participants.

Participant recruitment was carried out in collaboration with the Money and Mental Health Policy Institute, a charity based in the UK. 14 people were recruited from a sample of 5,000 research volunteers administered by the charity. As part of a survey in April 2019, the Money and Mental Health Policy Institute identified 226 people from their sample who expressed interest in testing the Toucan mobile application. These 226 volunteers were contacted again in May 2019 to share more details about the study and to reconfirm their willingness to trial the application between July and October 2019. 25 people consented to be contacted by the Toucan researchers, 14 of which enrolled in the study.

Participants were not required to disclose any details about their age, mental health condition or employment status as part of the research protocol, but some chose to do so during their interactions with the researchers. 8 participants shared their age, which ranged from 27 to 60 years old; and 12 mentioned a mental health condition, diagnosis or symptom. 4 participants reported being diagnosed with borderline personality disorder, 3 with bipolar disorder, 2 with post-traumatic stress disorder, 1 with schizophrenia and 1 with agoraphobia. In addition, participants disclosed suffering from depression (6), anxiety (4), panic attacks (2), paranoia (2) and psychosis (1). Conditions often co-existed: 7 participants reported more than one of them, and the same number acknowledged some kind of physical ailment. These included osteoarthritis, tinnitus, diabetes, fibromyalgia, chronic fatigue syndrome, irritable bowel syndrome and spinal injury. 2 participants also had a history of addiction to gambling (1) and alcohol (1).

Table 1. Participants' profile

ID	Gender	Age	Mental health	Physical health	Income	Debt	Debt Support	Ally
P1	F	27	Borderline Personality Disorder Post-Traumatic Stress Disorder	Endometriosis	Benefits	Yes	-	Partner
P2	F	-	Post-Traumatic Stress Disorder Depression	Osteoarthritis Tinnitus	Benefits	Yes	Yes	Daughter
P3	F	48	Depression, Anxiety	-	Work F/T	Yes	-	Husband
P4	F	42	Depression Gambling addiction	Chronic pain	Benefits	Yes	-	Mother
P5	M	46	Schizophrenia	-	Work F/T	Yes	-	Partner
P6	F	44	Depression, Anxiety	Diabetes Recovering from surgery	Benefits	Yes	Yes	Partner
P7	M	60	Bipolar Disorder	-	Work F/T	Yes	Yes	Sister
P8	F	41	Borderline Personality Disorder Depression, Anxiety Panic Attacks, Paranoia, Psychosis	Fibromyalgia Chronic Fatigue Syndrome Irritable Bowel Syndrome	Benefits	Yes	Yes	Daughter
P9	F	-	-	Unspecified disabling physical condition	Work P/T + Benefits	-	-	Husband
P10	F	46	Borderline Personality Disorder Depression, Agoraphobia	Spinal injury	Benefits	Yes	Yes	Sister
P11	F	-	Bipolar Disorder	-	Work F/T	-	-	Partner
P12	F	-	-	-	Benefits	Yes	-	Support care worker
P13	M	-	Borderline Personality Disorder Anxiety, Panic attacks Paranoia, Alcohol Addiction	-	Benefits	-	-	Friend
P14	F	-	Bipolar Disorder	-	Work F/T	Yes	-	Husband

All 14 participants shared their employment status: 5 participants were employed full time; 8 were off work and received social welfare or income protection benefits; and 1 worked part time and received welfare benefits to complement their income. 11 participants had personal experience of debt, either in the past or during the time of the study; and 5 had liaised with debt relief and support services. Debt seemed to derive mostly from credit card and bank account overdraft use.

All participants identified a suitable ally: 7 of them chose their partner or spouse, and 5 picked a family member, with only 2 participants selecting someone outside their immediate family circle. Table 1 provides a breakdown of the relationships between participants and their chosen allies.

4.2 Study Design and Data Collection

During the 90 days of the deployment, participants installed and used the Toucan application on their personal smartphones, while engaging in a diary study through mobile messaging and paper diaries. The duration of the deployment was chosen to match the 90-day customer consent validity established by the UK Open Banking Standard [29, page 60], therefore avoiding the need for participants to re-consent to the Open Banking connection between Toucan and their bank accounts during the study period. As compensation for taking part, participants were offered a £50 Amazon voucher upon completion of the 90-day diary study, and a £50 Amazon voucher upon completion of a closing interview. A further £50 Amazon voucher was offered to Toucan allies willing to volunteer for a closing interview.

The study started with a semi-structured interview with each of the 14 participants who would be using Toucan. During that first interview, participants installed and configured the mobile application. Researchers also enquired about information and communication technology use, financial and banking habits, the alert options offered by Toucan and the chosen ally. 12 of the 14 interviews took place remotely via telephone or video calls, with one opening interview conducted face to face and another one via email upon the participant's request.

The 90-day diary study commenced immediately after the opening interview. Participants started the diary study between 8th and 25th July 2019, and completed it between 6th and 23rd October 2019. During the 90 days, participants were sent 2 questions per week, on Thursdays and Sundays, through mobile messaging. The Thursday question asked participants whether they had discussed any money-related subjects with their ally during the past week. The Sunday question asked participants to rate from 1 to 5 how positive they felt about money, with 1 being "not at all positive" and 5 being "very positive". Although participants were encouraged to choose an end-to-end encrypted mobile messaging application (WhatsApp) to receive and reply to the diary study questions, three of them preferred to communicate via SMS. One participant requested to be excluded from the mobile messaging altogether and was provided instead with additional writing material in the form of blank postcards, 3 of which were written and returned to the researchers. 2 participants stopped responding to the mobile messages during the diary study period, with 11 of them replying regularly until the completion of the 90 days. A total of 283 mobile communications relevant to the study were received from 13 participants: 111 answers to the Thursday question about money conversations; 141 money positivity ratings; and 31 additional comments.

Participants also received a custom-printed paper diary designed by the researchers. The diary invited participants to reflect on their financial lives and the role the newly-installed Toucan application played in them. It included prompts about mood, personal finances, the role of the ally and the Toucan application. The diary also featured non-directed space where participants could write about any subject they wanted to bring up, and included pouches for storing physical financial artifacts such as receipts, statements and bills. 7 participants used the paper diaries to document their experiences during the trial and posted them back to the researchers. One participant also kept a personal diary during the study and handed it over to the researchers as additional material.

The deployment was concluded with a semi-structured interview. This final interview discussed the study period in terms of wellbeing, mental health and personal finances, the design of the Toucan application, the experience of receiving alerts, the experience of sharing alerts with third parties, and the impact of Toucan use on personal financial habits. All closing interviews were carried out remotely via telephone or video call, except for one which was done via email upon the participant's request. 13 of the 14 participants who installed the Toucan mobile application agreed to take part in the closing interview, as did 8 of their allies. 4 allies decided to join the closing interview of the participant they had supported, and 4 opted for being interviewed separately. This brings the overall number of interviews for this study to 31 - 14 opening interviews and 17 closing interviews - for a total of 22 participants. Interviews lasted between 27 and 105 minutes, with an average duration of 69 minutes for the opening interviews, and 50 minutes for the closing interviews. Interviews resulted in a total of over 28 hours of audio recorded material.

In addition, we collected usage data from the Toucan application database about alerts and allies. Specifically, the number, type, time stamp and recipient of triggered alerts; changes to the ally configuration; and a partial history of changes to the alerts configuration. The latter required a modification to the database schema that was implemented after the starting date of the study. This prevented us from collecting the full change history. No personal financial data from participants was accessed or used for the purposes of the study.

To identify the source of participants' quotes within this paper, unique identifiers will be followed by "_opening" for the opening interviews, "_closing" for the closing interviews, "_mobile" for the messages exchanged via WhatsApp / SMS, and "_diary" for the paper diaries. Toucan users are identified by a "P" followed by a number (e.g. P5). Allies are identified by "AP" followed by the number of the participant they supported and their relationship to them (e.g. AP5:partner indicates P5's ally).

4.3 Data Analysis

The data collected was processed as follows: interview audio recordings were transcribed verbatim; mobile messages were exported into text files; diaries were scanned and transcribed; and relevant database information was exported into CSV files and then compiled into a master spreadsheet. To support analysis, the Toucan database information was used to produce a visual history for each participant (see Figure 3 for an example). The money positivity ratings were then extracted from the mobile messages and incorporated into each visual history.

We performed thematic analysis [7] on the interview transcripts, mobile messages, diaries and postcards, applying an inductive approach to the coding phase. Coding was carried out by the first and second authors using the Nvivo software application. The process rendered 188 codes that were imported into a web based kanban board to enable remote collaboration between all authors during theme development.

Overall, Toucan was found valuable, having a considerable effect on the nature and quality of money conversations between participants and their allies. These became more frequent, less stigmatised and more oriented towards financial planning and problem solving. Participants also reported feeling more reflective about their spending and their money habits. Beyond Toucan's impact on our participants' financial practices, our analysis highlighted the work and diligence involved in making financial collaboration possible, an aspect of third party access that is often neglected but can be particularly valuable for design purposes. In what follows, we identify and describe the main activities, interactions and decisions involved in making Toucan work.

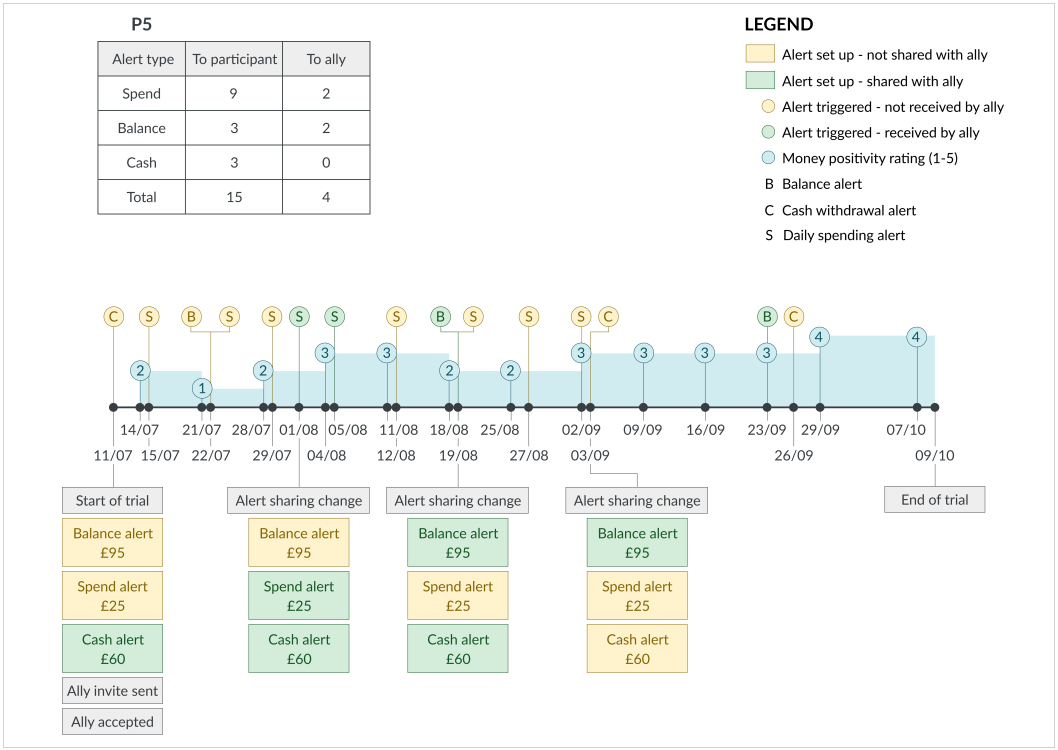

Fig. 3. P5's visual history of events during the Toucan trial, including alerts triggered, alerts shared, changes to alert configuration and money positivity ratings.

5 MONEYWORK IN FINANCIAL THIRD PARTY ACCESS

Engaging with the formal third party access service provided by Toucan required participants to undertake some additional, and somehow unusual, forms of moneywork. First, participants had to identify a suitable third party for financial collaboration. Then, participants had to communicate to their chosen third parties what Toucan was and what was required from a financial ally. In order to secure their agreement to engage with the app, participants also had to address any questions and concerns raised by the third parties. Once allies had consented to engage with Toucan, participants had to make decisions regarding what to share with them. Finally, participants and allies also had to establish a collaboration protocol within the framework provided to them by the Toucan functionality. We describe each of these activities in more detail in the sections below.

5.1 Choosing a Suitable Third Party

All participants were able to choose a third party to engage through the Toucan app, apparently without much difficulty. Although all 14 participants picked someone, only 13 configured the ally details in the app. P12 decided she would like someone from her professional care team to play that role. Unfortunately, because they supported her in a professional capacity, they were barred by their employer from communicating with the participant via mobile. That circumstance prevented P12 from setting up her chosen ally in the app. P12 and P13 were the only participants choosing a person outside their immediate family circle as their allies. All other participants picked their partner / spouse (7) or a family member (2 daughters, 2 sisters, 1 mother). All but one participant

(P4) kept the chosen ally for the whole trial. P4 switched between her husband and mother until finally settling on the latter.

The apparent ease with which people selected the third party conceals the true extent of the challenges involved. The task of picking a Toucan ally required participants to accept their own need for help, confronted them with the prospect of disclosing intimate information about their mental health and financial circumstances, and involved careful assessment of several relational factors. Participants considered the following when choosing their allies: degree of trust and closeness; "comfort" to discuss difficult subjects; ability to be firm when required; familiarity with the participant's mental health condition and consequences; degree and nature of prior financial support provided; money-management abilities; and pressures and life responsibilities of potential allies.

5.1.1 Trust and Closeness. Both allies and Toucan users spoke about their relationship in terms of trust and closeness. Trust was considered a baseline or precondition to engage in financial collaboration: *"I suppose that I have to be somebody that [P7] trusts and presumably I am or he wouldn't do this"* (AP7:sister_closing).

Several participants also described their relationship in terms of closeness. For some, closeness seemed to have an emotional meaning. AP8 was *"really close"* (AP8:daughter_closing) to her mother, as were AP10 and her sister; P13 and his ally were *"quite close as friends"* (P13_closing). For others, such as AP3:husband and P4, closeness referred to kinship ties. In this case, closeness was seen as a way of protecting the privacy of the Toucan user, given the personal and sensitive nature of the subjects at hand:

> I think to be an ally, especially as something as sensitive as their finances, I think you need to be fairly close. (...) It would have to be someone really particularly close, a sibling or a spouse. (...) I am very close to all of my friends, but I wouldn't necessarily want them to know what is going on with my finances (...) With [P3] and I doing it between us, I suppose it kept it private and kept it amongst ourselves. (AP3:husband_closing)

This helps explain why participants gravitated towards family members when choosing their allies: they seemed to consider money and mental health as belonging to the private sphere, and wanted to ensure it remained that way.

Closeness was also referred to in a physical sense. Geographic proximity played a role in the ally decision for at least 2 participants. P10 had 2 sisters, and she chose the sister living closer to her to be her ally. Between her 2 daughters, P2 selected the one living with her. Proximity makes allies more accessible, and equips them with valuable contextual knowledge that supports their role as financial collaborators:

> My daughter knows what day I go grocery shopping. She knows if I'm going to be making any big purchases (...) if she knows I'm ill in bed and she is getting an alert to say that I've spent over £100, she'd be like: Amazon app, cancel, cancel, cancel. (P8_opening)

However, closeness by itself was not sufficient: it was necessary to identify the right degree of closeness. AP7:sister, for instance, believed she had been chosen by her brother as his ally because she was one step removed from his immediate family. P7's wife had been directly impacted by the consequences of his bipolar condition over the years, and because of that *"It may be too difficult for her (...) she might get really upset and she might worry more, whereas I can be a bit more objective"* (AP7:sister_closing). P11 chose her partner, rather than her parents, for similar reasons:

> [my ally] is part of my inner support network when I am really poorly and I didn't want it to be my mum or dad. [Laughs] (...) Because I think he will be more relaxed

> about these things. They would maybe be like, oh God what have you done? Panic or whatever. (P11_opening)

It was this search for the appropriate degree of closeness that led P12 away from choosing a family member and into selecting her care providers instead. She *"felt more at ease"* and *"more able to talk"* (P12_closing) about money with her professional support than with her family: *"I would say don't pick a family member (...) not a total stranger, but I think someone outside the family maybe more able to kind of help you more and be less judgemental"* (P12_closing). The right level of closeness protected allies from emotionally-charged situations, provided them with a certain degree of objectivity, and shielded Toucan users against judgemental reactions, something to which participants gave great importance.

5.1.2 Relationship Depth and Resilience. Participants seemed to have a deep and resilient relationship that manifested in the allies' ability to discuss sensitive subjects, being firm when required, their knowledge about health conditions and symptoms, and their prior financial support. The quality of the relationship also showed in the Toucan users' careful consideration of their allies' personal circumstances and life responsibilities.

Participants brought up the need to discuss difficult subjects with their allies, and many spoke about it in terms of being comfortable with such conversations. For instance, P1 described her relationship with her ally as one *"where I'm comfortable talking about money and also my mental health"* (P1_closing). For a few participants, a good ally would also be firm when required. P8 was particularly emphatic about this point:

> pick someone who can kick your ass when needed (...) You don't want someone who is going to mollycoddle you and say: oh, it's going to be okay. You need somebody who is going to say: what the hell are you doing? (P8_closing)

According to our participants, a good ally should also be familiar with their mental health conditions, symptoms and consequences. P7 observed allies *"need to really know the person and know, not just what illness they have, but know how the illness affects people"* (P7_closing). P10 chose the same person who accompanied her to psychiatric appointments: *"[my ally] comes to my psychiatrist meetings and things, so she really understands what's going on"* (P10_opening).

Participants also considered financial aspects of the relationship with their allies. Some picked the person they usually turned to when requiring direct financial assistance. 7 participants (P1, P2, P4, P6, P10, P11 and P13) mentioned their allies had lent them money or had paid for things on their behalf. For others, financial support took a different shape. AP7:sister had never lent money to her brother, and supported him through listening and advice instead:

> when he talks about his money problems I just listen really, I never offer to help him in any way financially (...) I would rather just give him moral support or practical suggestions and that is all that I have ever done throughout the years. (AP7:sister_closing)

P12 received help for grant and emergency loan applications from the professional care staff she chose for the ally role; and P5 got encouragement to be sensible with money and to pay back his debts. For some participants it was also important to choose someone who was *"good with money"* (P8_closing). P13 considered his ally *"brilliant at budgeting"* and recommended others to pick somebody *"who is good with their money and manages their finances well"* (P13_closing).

Finally, our participants took into account the life responsibilities and personal circumstances of their potential allies, and picked those who they believed could take on the role without being overwhelmed. P10 wanted to spare her mother any worries: *"I can speak to my mum, but I rather speak to my sister just so that my mum is not worried. She's got enough on her plate"* (P10_opening). P13 decided not to ask his sister, who already had caring responsibilities towards their father

and also struggled with her mental health. P2 didn't pick her other daughter because *"she's busy working, as well as having a health problem (...) she has plenty on her plate"* (P2_opening). From our participants' point of view, a financial ally must have the time, energy and capacity to support others without it becoming a burden on their own lives.

5.2 Securing Agreement from the Third Party

Once participants had decided who their ally would be, they started the process of onboarding them into the role. The first step was introducing the Toucan application, what it did, and the concept of financial allies.

5.2.1 Introducing and Explaining Toucan. Most participants reached out to their allies before installing the Toucan app. Those who did not speak to their allies before installation (P2 and P12) postponed the ally configuration step at install time to ensure they spoke to their allies first. P6 also skipped the ally configuration step during the installation process. This participant had made her ally aware of the fact she was trialling Toucan before installing the app, but decided she would discuss it in detail only when ready to add him to the application: *"I had initially held off setting my ally up during the first weeks of the trial so that I could get a feel for it myself first, which also helped me to explain it better to [my ally] when the time came"* (P6_diary).

By the time P6 confronted the task of explaining Toucan to her ally, she already had first-hand experience of the service. Those who did not do this found it difficult to convey what Toucan did. P13 acknowledged that when he first engaged his ally, he *"wasn't quite sure what her involvement would be and what she would be doing"* (P13_opening). Other participants (P3, P4, P7, P8 and P10) used the information for allies the researchers provided at the beginning of the study. P10 and her ally took the time to review that information together. To make sure her ally understood the service, P3 went through the app with her ally after installing it:

> I sat with [my ally] once you kind of added the information to Toucan. I showed [my ally] what it led to and we were looking at that together (...) I just wanted him to be aware as to what this was all about. (P3_closing)

5.2.2 Addressing Allies' Concerns. The introduction to Toucan raised questions and concerns for many of the allies. The most common one related to the legitimacy of the application. Since the trial involved connecting the Toucan app to the participants' main bank account, many allies wanted to make sure Toucan was *"kosher"* (P5_opening). 6 allies (AP3:husband, AP4:mother, AP5:partner, AP8:daughter, AP12:support_worker and AP13_friend) expressed concerns about Toucan's legitimacy: *"When I first heard about it, when [P3] mentioned it, I suppose my first thoughts were: who are these people and why do they want access to your finances and bank account?"* (AP3:husband_closing). This mirrored participants' own worries. 8 of them (P1, P2, P5, P6, P7, P9, P11 and P13) brought up security and access to financial data during the interviews. The fact that they were engaging with a research study, and the connection to the Money and Mental Health Policy Institute, helped ease those concerns:

> normally I would have reservations about giving people access to my account but because I understand the ethics behind this research then I am happy for that to go ahead (P6_opening).

Participants overcame their allies' objections by referring to the connection with the Money and Mental Health Policy Institute, and by demonstrating they had done what AP3:husband called *"due diligence"* (AP3:husband_closing):

> I also said to [P5] please go away and do some more research on this company because I have not heard of them. (...) I was actually quite concerned about it initially ... but

> then obviously he did what he needed to do and he looked at it and he said, actually, you know, it's fine. Then I relaxed about it. (AP5:partner_closing)

There were some additional questions raised by allies upon being introduced to the Toucan concept. AP5:partner and AP7:sister enquired about data confidentiality and privacy. AP8:daughter worried about the degree of information disclosure on P8's financial affairs, and the impact that would have on her privacy:

> just like what it could see and so on and what it would tell me, because as much as I want to help her and stuff, I don't need to know every single penny my mum spends and even though she's unwell, she is entitled to that sense of privacy (...) I didn't want to be told, you know, where every single penny of her money was going. (AP8:daughter_closing)

As a young adult put in the position of having to raise difficult subjects with a parent, AP8:daughter was also concerned about the alerts and subsequent money conversations leading to conflict or tense situations: *"I was worried it would (...) create a bit of tension with me being like, why are you spending money? And her being like: back off ..."* (AP8:daughter_closing). Finally, AP10:sister wondered about the time demands of the role and how they would impact her busy life as a working mother with young children.

5.2.3 Securing Agreement from Third Parties. At that early stage, neither Toucan users nor allies seemed to have a clear view of what the service would mean in practice, how it would impact their money affairs or their existing relationships. AP10:sister told us she *"really didn't understand it at first"* (AP10:sister_closing), and AP7:sister that she *"wasn't really sure how it would work"* (AP7:sister_closing). In spite of this uncertainty, all allies agreed to take on the role. Allies accepted because they wanted to help - *"I was fine with it ... because I was just like, okay, if it helps mum, it helps mum"* (AP8:daughter_closing) -, and because they believed that the Toucan service was a good idea with the potential to bring *"real benefit for people that do struggle with finances"* (AP5:partner_closing). Only P12's care support workers refused due to professional restrictions, even though they would have been *"happy to do it"* (P12_closing).

5.3 Configuring Access

Once participants had secured the agreement of their chosen third party to become their Toucan ally, they were confronted with the need to make decisions about what was appropriate to share with their allies. They faced this issue for the first time during the Toucan installation, which required them to select which of the 3 alerts (spend, balance and cash withdrawal) they would like to share. Table 2 provides a breakdown of what each participant chose to share at the time of installation.

Of the 13 participants who configured an ally during the study, 7 shared all 3 alerts (P2, P3, P6, P7, P8, P10 and P14). Of the remaining 6 participants, 4 decided to keep the balance alert private (P1, P5, P11 and P13); 3 decided to keep the spend alert private (P4, P5 and P9); and 2 decided to keep the cash withdrawal alert private (P4 and P11).

When deciding which alerts to share, P1 took into consideration her financial behaviour when she was unwell. She explained she was prone to *"spend online at 3 am when I can't sleep"* (P1_closing), and how she had in the past *"bought things without knowing"* (P1_opening). Based on those behaviours, she concluded that the spend and cash withdrawal alerts were the ones that could better signal to her ally that she needed support, and shared them with him. In contrast, P1 considered the balance alert a poor indicator of her mental and financial wellbeing, so she decided to keep it private:

Table 2. Alerts shared with allies at installation time. "Shared" alerts were activated and shared with allies; "not shared" alerts were activated but not shared with allies; "off" alerts were not activated. P12 did not set up an ally.

ID	Spend	Balance	Withdrawal
P1	Shared	Not shared	Shared
P2	Shared	Shared	Shared
P3	Shared	Shared	Shared
P4	Not shared	Shared	Not shared
P5	Not shared	Not shared	Shared
P6	Shared	Shared	Shared
P7	Shared	Shared	Shared
P8	Shared	Shared	Shared
P9	Not shared	Shared	Off
P10	Shared	Shared	Shared
P11	Shared	Not shared	Not shared
P12	-	-	-
P13	Shared	Not shared	Shared
P14	Shared	Shared	Shared

> I decided to keep [private] the alerts that let me know that my balance was low as I felt that was something I could deal with on my own. At the time, I really didn't have a lot of income so I guessed I'd receive those alerts often and that it wasn't a sign that my mental health had declined. (P1_closing)

P11 seemed to apply a similar rationale. In her case, the cash withdrawal alert was a poor indicator of financial distress: *"I don't really withdraw cash and I think your bank only lets you take a maximum of £250 or £300 in a day anyway, so if I was poorly, it would be difficult to spend a large sum"* (P11_opening). The most reliable signal for P11 was her spending behaviour, so she decided to share the spending alert with her ally.

P9 decided to share only the balance alert. Her motivation was to compensate for her ally's lack of access to information about their joint bank account. P9's ally did not like using telephone or online banking, and he no longer received the paper statements he relied on in the past to keep track of the household finances. As a result, P9 felt her ally was being left *"in the dark"* (P9_opening). She hoped the balance alerts would get her ally more involved in overseeing their common finances.

P4 seemed to be more concerned about not divulging certain financial affairs of which her ally was not aware: *"I have got credit cards, which my [ally] will kill me (...) She's going to find out just now isn't she, with the ally?"* (P4_opening). Given her personal history of debt, and the financial assistance she had received from her ally in the past to recover from it, having credit cards was something P4 was not happy to disclose. She decided to share with her ally only the balance alert, which she set to a negative amount. Since the ally was well aware of P4's money situation, and often supported her financially when her overdraft was too close to its limit, sharing the balance alert did not reveal any new information to the ally.

A similar privacy-seeking motivation may have been behind P5's decision to share only the alert that he found irrelevant - the cash withdrawal one:

> my mental health is managed pretty well to be honest. So, if (...) I'd taken £60 out of the cash point… there isn't a time I wouldn't know I'd done that. (...) For me it's not really relevant, to be honest, the cash withdrawal [alert]. (P5_opening)

Still going through a divorce, P5 chose his new partner, who he had recently met, as his ally. He initially decided to share with her an alert he thought was unlikely to provide a reliable indication of financial difficulty. However, as the study progressed, P5 changed his mind about what was appropriate to share with his ally. He shared the spend alert some time in July and, in early August, he stopped sharing the cash withdrawal and spend alerts and started sharing the balance alert instead. As he developed trust in his new partner and Toucan ally, P5 proceeded to share more meaningful alerts.

5.4 Establishing a Collaboration Protocol

Given the lack of clear expectations about what using Toucan would entail in practice, it is perhaps not surprising that participants engaged in little preparation and planning before the alerts started. The researchers recommended participants to agree with their allies in advance a course of action for when an alert was received. This, however, did not happen, or happened only at a very high level. AP8:daughter told us they *"agreed that I would (...) bring it up or something, like I would just mention it"* (AP8:daughter_closing). P1 explained they didn't arrange anything specific: *"As we are so close whatever he'd do would be right. He's pretty level headed and knows how best to support me"* (P1_opening). At most, pairs agreed on a certain communication channel (e.g. a phone call), or on a question that would be asked. For instance, P1 and her ally decided that *"one of the things he'll do is ask me if I remember making a purchase. I dissociate frequently and have in the past bought things without knowing. Hopefully if I don't remember I might have a chance to cancel it!"* (P1_opening). With so little prior preparation, the protocol for responding to alerts developed organically and through practice.

5.4.1 Communication Channels and Contact Frequency. Allies understood Toucan alerts as a prompt to get in touch with their counterparts, and each pair did so in their own way. For instance, AP8:daughter always brought it up in conversation, mostly face to face. When away at university, she would call her mother rather than sending a message. When bringing up the subject, she did so in a lighthearted way. She would not broach the subject if her mother *"was in a bad mood"* (AP8:daugther_closing). AP8 also used contextual cues to start the conversation, for instance if she saw something new at home, or a delivery arrived: *"if Amazon turned up, she would be like, there you go, I've gotten a text message"* (P8_closing). After a while, P8 came to expect her ally to raise the subject within a day or two of receiving a Toucan alert.

AP10:sister also preferred to visit in person, but that was not always possible. If she was at work, she would send a text or contact P10 via Facebook Messenger: *"when my [ally] was at work and she would get an alert, she would text me saying: Is everything okay? I've had an alert. Check your bank and I will ring you later"* (P10_closing). Some allies, like AP10:sister here and AP4:mother, contacted their counterparts after every alert. Others, like AP3:husband, took a more relaxed approach, and didn't feel the need to mention every one of them:

> I discussed the account with [P3] (...) on the first few occasions. (...) I didn't go into any great depth. We are pretty close in that respect so I didn't feel the need to interrogate her every time I got a text message. (AP3:husband_closing)

It was the same with AP6:partner, who would mention the alerts when receiving several of them within a short period of time: *"I didn't talk to her about every single one. (...) It all depends just how many came through"* (AP6:partner_closing).

In general, allies who met their counterparts daily or frequently showed a preference for discussing the alerts in person. Those who didn't meet often resorted mostly to phone calls, with messages used as a way to acknowledge the reception of the alert and quickly confirm there were no major issues. AP6:partner represented this pattern: being on the road most of the week for professional reasons, he would see P6 only on the weekends. That cadence determined how he would react: he would text P6 if he received alerts at the beginning of the week, but would wait until the weekend to discuss them in person if he received the alerts towards the end of the week.

5.4.2 Reacting to Allies' Responses. Toucan users adjusted the app configuration and adapted their behaviour in response to their allies' reactions and their interactions with them after alerts were triggered. For example, P6 increased her spending alert threshold to avoid unnecessarily worrying her ally: *"I ended up increasing the daily spend allowance alert to minimise the frequency of the alerts. It was beginning to sort of worry him a bit"* (P6_closing). She also started to anticipate the triggering of alerts, and proactively let her ally know when one was likely to arrive:

> he gets the alerts and when he is not with me at the time, it sort of starts making him worry until he can speak to me later that day (...) it got to the point, sort of part way through, where I was saying: I've just paid this, I'm expecting a Toucan alert. [Laughs] And we did get it. [Laughs] (P6_closing)

P7 and P8 adopted a similar behaviour. P8 started to notify her ally about her big purchases before an alert was triggered: *"Whenever my mum bought (...) big things, like she recently redid her bedroom and she bought a wardrobe. She told me about that kind of thing in advance"* (AP8:daughter_closing). P7 told us how *"a few times I'd phone [my ally] and tell her that she was going to get some [alerts], in case she was getting browned off with them (...) or think there was problems developing"* (P7_closing). In that process, P7 would share information about his financial affairs with the person he trusted. These participants moved from reacting to Toucan alerts to proactively sharing details of their money lives with those close to them.

5.5 Negotiating Information Disclosure with Allies

Participants discussed at length the consequences of Toucan's non-disclosure of financial information. Toucan sent different messages to users and allies. While user alerts specified the type of financial event that triggered the message (low balance, spending or cash withdrawal), ally alerts always showed the same generic text, which simply suggested getting in touch with their counterpart without revealing any financial details. Toucan users and their allies were torn between the privacy and control this non-disclosure afforded to application users, and the vulnerabilities it caused for allies.

5.5.1 The Impact of Non-Disclosure. In general, Toucan users seemed determined to remain in control of their money, and rejected any form of support or assistance that was perceived as too overbearing. Toucan's lack of financial information disclosure aligned with this desire to retain control, and was well received. P9 thought this approach protected her privacy and contributed to her security. For P1 and P11, it preserved their *"autonomy"* (P11_opening), and meant they could keep control over their finances: *"I like that even though my ally is made aware of my spending, they don't know the amount etc, so I still have control over my finances and stuff is still kept private"* (P1_closing).

Many of the allies we spoke to were also satisfied with Toucan's non-disclosure approach. They felt it protected the privacy and dignity of their loved ones, and shielded them from intruding into their counterparts' affairs. For AP8:daughter, Toucan non-committal alerts meant she *"was invading less"*, and that her mother *"didn't feel like she had to be held accountable"* (AP8:daughter_closing).

AP4:mother and AP5:partner thought that what Toucan said was *"sufficient"* (AP4:mother_closing) and didn't *"need any more detail"* (AP5:partner_closing).

Although Toucan's non-disclosure approach had significant advantages, some allies believed it negatively impacted their ability to support their counterparts. Since they knew nothing about the circumstances that had triggered the alerts, it was difficult for them to assess what would be an appropriate reaction:

> I'm not completely sure what triggers them, what happens at Toucan's end for that message to go out. (...) I'm not sure if I'm supposed to run around the house with arms waving or not [laughs]. (AP3:husband_closing)

The lack of detail also generated some anxiety, since after receiving an alert allies did not know whether there was cause for concern or it simply had been triggered by routine spending:

> I was getting texts, I could be getting 5 texts and they could all be bills, but because I don't know that, I'm thinking: oh no, what money is going out on what? You don't know if it is something to worry about or not. (AP6:partner_closing)

Toucan's non-disclosure approach also meant allies could be easily deceived. AP7:sister, P7 and P8 observed that alert configurations could be changed in order to avoid triggering alerts:

> it would be easy to kind of up everything to an excess without everyone else knowing. (...) I personally didn't do it, but it's easy to manipulate the app when you're the only person in control of it and that's the one thing that I do feel strongly about. (...) and if you're then changing round the numbers without [allies] knowing then they don't know ... they're not fully aware of what is going on. (P8_closing)

Allies may not be told the whole truth, as AP7:sister observed:

> it didn't give me any indication if it was really something to worry about or not. I had to rely on [P7] telling me that, which is fair enough but he might have not told me the truth, because he maybe might not want me to know if he was having problems. (AP7:sister_closing)

AP8:daughter actually believed her counterpart had lied to her at some point: *"I am aware that people lie and I know sometimes [P8] lied"* (AP8:daughter_closing). She brought it up in conversation: *"[AP8] has pointed out to me: you could lie to me at any point and there is nothing to tell me that"* (P8_closing). Perhaps as a result of discussing this subject with their allies, P7, P8 and P13 expressed a willingness to share more information with them, albeit always subject to their explicit consent: *"I would be more than happy to authorise [my ally] knowing more specifics with regards to where the money had been spent or how much I'd spent"* (P13_closing).

5.5.2 Striking a Balance Between Autonomy and Support. Participants believed there was a need to strike a balance between preserving privacy, keeping control and enabling the allies in their supporting role:

> should they give you more? I don't know. (...) you're not going to let me know what [P7] is spending his money on. That's somebody's own business and it's their privacy. So it is getting that balance between expecting someone's privacy but also giving me enough information to think, wait a minute now, this is ringing alarm bells. (AP7:sister_closing)

When making suggestions as to how that balance could be achieved, Toucan users listed information they would be willing to disclose, while allies preferred indicators of severity. Regarding information disclosure, P7 suggested showing allies the type of alert, and therefore the kind of event that had triggered the message. P8 proposed using thresholds, rather than exact amounts.

She would also be willing to provide transaction breakdowns in order to encourage more detailed conversations:

> if you spent over £60 in one day, they'd get a kind of break down. There were 5 transactions resulting in this and it would be like ... (...) What was on there that you thought you needed? Why did you feel the need? I think it would be more about the conversation and helping them to speak more. (P8_closing)

P13 considered the type of expense and merchant a particularly meaningful piece of information for allies:

> I think I would have been happy for [my ally] to know how much I had spent, what the actual sum was and possibly whereabouts (...) what kind of shop or organisation it has been with (...) she would know that I was spending (...) on essential items and that I hadn't, you know, I wasn't wasting £50 in some shop on rubbish. (P13_closing)

Regarding the indicators of severity preferred by the allies, AP3:husband suggested wording the messages differently for routine transactions and for events that could signify trouble. AP7:sister proposed classifying the alerts based on severity:

> maybe like a green, amber and red warning system. Like this is just a bit of expenditure, we're just letting you know. Or there has been quite a lot of expenditure. Or this is quite serious because it is actually a huge amount. That might be quite useful actually so that you get an indication of the severity or the seriousness of the expenditure. (AP7:sister_closing).

Finally, P7 and P8 proposed solutions based on expanding the remit of the relationship to include the app configuration process. At a minimum, Toucan users may agree to seek consent from their allies in order to make changes to their alerts:

> if you could lock them in. If you could unlock them maybe with the approval of your ally, (...) if it was an ally that knew the situation, they knew how your illness affects you, like my sister does me, you know it might be beneficial in certain circumstances. (P7_closing)

P8 went further and suggested that the app configuration should be a collaborative process. Allies and their counterparts would discuss and agree on which alerts to activate and the rules that would trigger them. The app configuration would then be locked for a certain period of time, and changes could only be made if authorised by both parties. Authorisation could be ratified by requiring both user and ally to enter a password:

> I think it would be a bit better if the ally had the thing where they had to sit down, make a plan and then it is passworded by both. From the start you're told that it can't be changed until both are in agreement. (...) I think it should be a two-people process setting up the limits, etc. (P8_closing)

P8 made a point of clarifying that the app should not affect the ability to transact, but would simply disclose information as per the agreement reached between the parties during the configuration process:

> You could have it that they can set it up for 2 weeks. Until you get kind of a flavour of what is going on. Then at that point you decide what is reasonable and what is not. You are not saying that no, they can't spend the money. You are just saying that if they are having, I don't know, 6 alerts within 2 hours on a Friday evening that's not a good thing. (P8_closing)

For P7 and P8, the key to strike the right balance between privacy and support was further empowering the parties to collaborate on their own terms.

6 DISCUSSION

Using Toucan involved a set of activities that can be seen as various instances of moneywork. These included selecting a suitable third party, securing their agreement to engage with the service, configuring access, establishing a protocol for financial collaboration, and negotiating the trade-offs between privacy and information disclosure. Our findings highlighted the great degree of consideration and effort from our participants in how they configured Toucan to suit their changing needs and the needs of their ally. The complexity of this moneywork is somewhat obscured by the relative simplicity of Toucan and, on an initial look, the apparent ease by which the participants initially identified their allies and engaged with the application. The understanding of such activities has been largely ignored in the design of third party access mechanisms, rendering them somehow *"invisible"* [26]. This invisibility may reflect the power relationships currently embedded in the design of third party access mechanisms - including Toucan - which position those who use them as vulnerable by virtue of their needing assistance. Recognising the true importance and complexity of fundamental tasks like selecting a suitable third party, together with supporting them accordingly, may be the first step towards mechanisms for third party access that establish a more equal relationship between all involved.

Like Perry and Ferreira, while acknowledging the *"limits to which generalisations can be made"* [39] from specific cases like the one presented in this paper, we postulate that the moneywork activities involved in the use of Toucan do *"capture valuable aspects"* [39] of financial collaboration. As such, the practices described may extend to some degree to other forms of financial third party access. In the following discussion sections, we make a case for designing such services with a focus on moneywork, providing design recommendations in the process.

6.1 Designing for Trusted Sharing of Financial Data

Toucan users had to approach their chosen third parties to secure their agreement to engage with the service. In order to do so, they had to be capable of explaining what Toucan did, and what was expected from financial allies. They were also required to provide satisfactory answers to the questions posed by the third parties, the most prevalent ones being about the security and trustworthiness of the service. This confronts us directly with one of the main challenges faced by open banking initiatives: overcoming users' privacy concerns in order to drive adoption.

Open banking initiatives will have to contend with the social norms and expectations about information flows in the context of financial services. Open banking fundamentally disrupts one of the main *"entrenched norms"* [36] in this domain: that we and our banks shall carefully guard and not disclose personal financial data. In their study of personal information sharing across finance and health, Singh and Cassar Bartolo observed that minimising risk in the financial domain involved *"withholding information"* [43], and that sharing was limited to spouses and partners. The risk derived from privacy breaches was perceived as high, since it could lead to money loss [43]. As Nissenbaum warns, violating the social norms of information flow for a certain context, as open banking initiatives seem to do, often results in *"protest and complaint"* [36].

The UK Open Banking initiative's approach to privacy protection and information flow seems inappropriate to tackle this challenge. It currently relies on informed consent, and appears to take inspiration from what Crabtree and Mortier call the *"dataware model"* [12]. Both concepts are problematic. According to Nissembaum, informed consent offers privacy on a *"take it or leave it"* [36] binary basis. In addition, it assumes individuals are free to choose between those 2 options.

However, deciding not to engage with digital services comes with social, commercial and financial costs that question how freely such choices are actually made [36].

The dataware model *"seeks to federate disparate sources"* [12] of personal data and to build digital infrastructure that enables people to exercise control over such data. It involves 3 types of interacting entities: *"the user, by or about whom data is created; the data sources, which generate and collate data; and the data processors, which wish to make use of the user's data"* [12]. This structure is clearly at play in the UK Open Banking initiative, where bank customers (the user) authorise third party services (data processors) to access information held about them by banks (data sources). Crabtree and Mortier observe that the dataware model lacks accountability, legibility and intelligibility [12]. It tells users nothing about how the data will be processed, which inferences will be drawn from it or how it will be combined with other data. Without this information, users cannot understand the implications of the data-sharing decisions they make and the permissions they grant [12].

The disruption of the social norms around information flows, in combination with a flawed privacy model, poses a sizable challenge to the uptake and success of any services relying on open banking. This in turn threatens innovation in financial third party access. Services enabled by open banking initiatives should treat the regulatory privacy framework as a baseline, and consider deploying their own privacy initiatives. In this unfamiliar context, Nissenbaum recommends to start with *"ends, purposes and values"* [36], using those as a guideline to develop personal information management and flow rules. Coles-Kemp and Kani-Zabihi [10] suggest the development of tools that enable services and their users to establish a dialogue about privacy.

6.2 Designing for Appropriable Financial Third Party Access

We have presented the moneywork involved in using Toucan as a sequence of activities but, in practice, interaction outcomes and application use built upon each other and continuously adapted based on the context, behaviours and responses of our participants. Allies switched between communication channels depending on their circumstances when an alert arrived; Toucan users changed the alerts they shared as their confidence in their allies grew; they modified alert thresholds to achieve what they perceived as the right volume of messages based on their allies' prior reactions; and started notifying allies in advance that an alert would be coming to save them unnecessary worry and anxiety. Toucan activities were situated: they depended in essential ways upon the specific circumstances in which they took place [50]. In order to fully enact this *"situatedness"* [14], participants had to appropriate the Toucan app. Participants' moneywork was shaped by the technology, but participants also shaped the technology through use by configuring it for their specific needs and developing workarounds to overcome its limitations [8]. For example, participants started to warn their allies in advance of expected alerts in order to overcome the inability to stop routine payments from triggering messages. This reshaping of technology through use has been referred to as *"appropriation"* [8], and it is in this sense that we employ the term in this paper.

Much has been written in CSCW and HCI on how to design for appropriation (e.g. [14, 15, 21]), and some of the qualities of *"appropriable systems"* [15] can be observed in Toucan. For example, alerts acquired different meanings depending on each users' own financial behaviours, so the system allowed interpretation [14]. Toucan also provided infrastructure for sharing financial information with a third party without imposing a specific workflow, supporting rather than controlling users [14]. The choice of SMS for alert delivery may have contributed to Toucan's appropriability as well. According to Höök, potentiality for appropriation resides in the technologies available to us [21], and SMS has been noted elsewhere as an example of a technology that is highly appropriable [42]. Although scarcely used for financial service delivery in the Global North, SMS is an almost

pervasive, and cost effective, technology, which made it a good medium for the delivery of Toucan alerts.

When compared to Toucan, existing formal third party access mechanisms leave little room for appropriation. For example, the access permissions in third-party mandates are tightly defined by the banks: they are non-negotiable, and users have no choice but to accept them as they come. New forms of financial third party access should embrace the principle of user appropriation. They should acknowledge the situated nature of financial third party access activities, and create systems that leave space for interpretation, support users rather than enforcing specific workflows, and deploy appropriable technologies. At the same time, designers must remain aware of the potential for introducing risk. Alternative third party access practices demonstrate how PINs and Internet banking credentials can be highly appropriable, albeit in a way that can lead to great financial harm. Possibilities for appropriation must establish certain boundaries in order to strike a balance between security and flexibility.

6.3 From Designing for Protection to Designing for Collaboration

Seeking balance between security and flexibility, Toucan established strict constraints in terms of what information could be shared with allies, while opening up other areas of the interaction. While Toucan users cannot change the content of the alerts delivered to third parties, they can decide which alerts to share with their allies, and modify those at any time and with little effort. They can also choose not to share any alerts at all, and are free to pick a different ally at any point. This flexibility gives Toucan users a high degree of autonomy, and offers a stark contrast to the rigidity of other formal mechanisms. New forms of third party access should explore more flexible approaches to access configuration, while preserving appropriate levels of security. Flexibility enables all parties involved to experiment with the relationship and develop trust progressively [55]. It may also reduce the risks involved in financial collaboration by allowing access to be swiftly revoked if trust is betrayed. Possible design strategies for secure flexibility in financial third party access include limiting its scope and duration, as proposed by Dunphy et al. [16]; and disclosing only information - without any power to transact - as exemplified by Toucan.

However, flexibility should not happen to the detriment of, or cause disadvantage to, any of those involved in financial third party access. When discussing assistance in the management of older adults' financial assets, Tilse et al. observed that third party access policies have so far focused on protecting asset owners from financial abuse [52]. This emphasis on protection precludes consideration of how to preserve the autonomy of asset owners, and encourage their participation in financial decision-making [52]. In response to this challenge, HCI literature has proposed designing for control. Singh et al. suggested users of financial services should be given ample control over their personal information [46], including the ability to share it with others [43]. Dunphy et al. conceived their Helper Card to ensure that asset owners *"are empowered to be in control of their resources"* [16]. Toucan was, in many ways, guided by the same idea of designing for control, and deployed flexibility for this purpose. However, during the study we observed how concentrating flexibility and control of information on the Toucan user generated power imbalances between the two parties to the relationship, leaving allies vulnerable to manipulation, lies and anxiety.

The experiences of our participants foregrounded the importance of designing for financial collaboration instead. Designing for protection and designing for control establish an unequal relationship between the parties involved in financial third party access. The former tends to prioritise substitute decision making and therefore empowers the third party; while the latter tends to prioritise autonomy and therefore empowers the asset owner. Designing for collaboration aims to establish an equal relationship between the parties involved in financial third party access, one where control is shared and negotiated. When the purpose is to enable support in the management

of personal finances, flexibility and control of personal information should be accompanied by mechanisms that encourage the negotiation and formalisation of collaboration protocols that have been agreed by all parties to an egalitarian relationship. New forms of financial third party access should consider moving beyond designing for protection and designing for control, and prioritise instead designing for meaningful financial collaboration. Flexibility should be put at the service of this collaborative purpose.

6.4 The Potential of Information Disclosure

Figure 1 mapped formal and informal mechanisms for financial third party access based on the 2 axes of information disclosure and power to transact. In that map, the top right quadrant contains the most invasive options that delegate ample powers to transact and disclose most or all financial details to the third party. These include lasting power of attorney and banks' third party mandates between the formal mechanisms, and the sharing of Internet banking credentials between the informal ones. The bottom right quadrant contains options that delegate limited power to transact and disclose some to little financial information, such as the sharing of bank cards and PINs, and carer cards. The top left quadrant contains mechanisms with a high degree of information disclosure, but that do not delegate any power to transact. For instance, read-only access to someone else's Internet banking. Finally, the bottom left quadrant includes mechanisms like the Toucan app, which disclose little or no financial information, and do not delegate any power to transact.

Disaggregating the 2 factors of financial third party access in this manner may contribute to a more exhaustive examination of the domain, helping us identify new design opportunities. For instance, the map in figure 1 reveals that little attention has so far been paid to information disclosure only options, i.e. mechanisms that do not delegate any power to transact but support asset owners by enabling oversight and advice through information sharing. Research by the Money and Mental Health Policy Institute reported many participants being *"enthusiastic"* about this approach, which would allow someone *"to watch over their account, without decision-making power"* [6]. In spite of this evidence, there has been little experimentation with information disclosure-only strategies.

Advocacy organisations in the US and the UK have recommended banks should offer read-only access to Internet banking for a third party [20, 33]. Work on accommodating shared identities in digital accounts suggests some of the ways such read-only access could be provided. Online services today assume each account will only be used by one person. This creates barriers for information sharing. To move beyond this paradigm and overcome its limitations, Adams and Williams [1] proposed 4 new types of digital accounts: several, shared, subordinate and nominees. In shared accounts all members have access to information, but other actions require permission from, or are only available to, certain members. Such a digital account would accommodate read-only access for designated third parties, while restricting power to transact to the account owner. Control over which information can be seen by read-only members would also be desirable [6, 44], and Toucan users made suggestions as to what they would like to share. For example, amount spent over a certain period of time such as a day or a week, transaction lists, and merchants or merchant categories where expenses took place. Access to more abstracted information, as proposed by the Toucan allies, could also be considered. For instance, by setting thresholds for high, medium or low spending; or by providing spending trends over time without displaying any amounts or transaction details.

Until recently, the only organisations in a position to put into practice these recommendations were banks. The arrival of open banking initiatives, first in Europe through the Payment Services Directive 2 (PSD2), then across the world [35], has substantially transformed this landscape. People's financial data is becoming accessible to authorised services through APIs, creating new possibilities for third party access. In the UK, financial technology startups using open banking capabilities have

mostly perpetuated the mainstream focus on the *"individual level"* [48], providing functionality for data aggregation, personal budgeting, financial planning, savings and automated investment advice. All these applications put emphasis not just on the individual, but also on sharing our financial data exclusively with service providers. This individualistic and entrepreneurial perspective misses the fact that open banking also introduces the possibility of sharing our financial data with each other, and with those in our *"circle of care"* [43]. In doing so, open banking may create new opportunities for secure, flexible, proportionate and practice-sensitive forms of third party access that, moving beyond protection and control, enable meaningful financial collaboration.

7 CONCLUSION

In this paper, we have explored the moneywork involved in granting others access to our finances in order to enable support with money management. We have demonstrated, through the Toucan example, how the opening up of banking data to external services can contribute to the development of new financial third party access mechanisms. We have shown the value of designing those mechanisms with a focus on moneywork, and emphasised the importance of moving beyond protection and control in order to enable meaningful financial collaboration. Financial third party access services face the difficult task of striking a balance between autonomy and protection [25]. Designers can contribute to this challenge by deploying practice-sensitive approaches that start from people's situated actions.

ACKNOWLEDGMENTS

This research was funded by a UKRI Arts and Humanities Research Council doctoral studentship (Ref: 1947353). We would like to thank our participants for sharing their experience and making this research possible.

REFERENCES

[1] Andrew A. Adams and Shirley Ann Williams. 2013. What's Yours is Mine and What's Mine's My Own: Joint Accounts and Digital Identity. *ACM SIGCAS Computers and Society* 44, 1 (2013). https://doi.org/10.1145/2602147.2602150

[2] AgeUK. 2011. *The Way We Pay: Payment Systems and Financial Inclusion.* Retrieved April 27, 2020 from https://www.ageuk.org.uk/Documents/EN-GB/For-professionals/Consumer-issues/the_way_we_pay_research_report.pdf?dtrk=true

[3] Deena Alghamdi and Ivan Flechais Marina Jirotka. 2015. Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. In *Symposium on Usable Privacy and Security (SOUPS '15)*. The USENIX Association. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-alghamdi.pdf

[4] Anna Beckett, Katrina Leary, and Lauren Cumming. 2014. *The Future of Lasting Power of Attorney.* Retrieved March 12, 2020 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/358560/OPG_LPA_Ipsos-MORI_Nov_13.pdf

[5] Victoria Bew, Wania Cautela, Vivienne Man, Raza Yasmin, Anna Seligman, Anne Stewart, and Isobel Yiannopoulos. 2017. *Ageing Population and Financial Services - Occasional Paper 31.* Retrieved April 27, 2020 from https://www.fca.org.uk/publication/occasional-papers/occasional-paper-31.pdf

[6] Nikki Bond, Katie Evans, and Merlyn Holkar. 2019. *A little help from my friends. Tools to support financial decision-making for people with mental health problems.* Retrieved March 22, 2020 from https://www.moneyandmentalhealth.org/thirdpartyaccess/

[7] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[8] Jennie Carroll. 2004. Completing Design in Use: Closing the Appropriation Cycle. In *Proceedings of the European Conference on Information Systems (ECIS '04)*. Association for Information Systems. https://aisel.aisnet.org/ecis2004/44/

[9] Sandra Colavecchia. 2009. Moneywork: Caregiving and the Management of Family Finances. In *Family Patterns, Gender Relations Third Edition*, Bonnie Fox (Ed.). Oxford University Press, 417–427.

[10] Lizzie Coles-Kemp and Elahe Kani-Zabihi. 2010. On-line Privacy and Consent: A Dialogue, Not a Monologue. In *Proceedings of the 2010 workshop on New security paradigms (NSPW '10)*. ACM, New York, NY, 95–106. https://doi.org/10.1145/1900546.1900560

[11] UK Competition and Markets Authority. 2016. *Retail banking market investigation.* Retrieved May 18, 2020 from https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf

[12] Andy Crabtree and Richard Mortier. 2015. Human Data Interaction: Historical Lessons from Social Studies and CSCW. In *Proceedings of the 14th European Conference on Computer Supported Cooperative Work (ECSCW '15)*. Springer, 3–21. https://doi.org/10.1007/978-3-319-20499-4_1

[13] Rachna Dhamija and Adrian Perrig. 2000. Deja‘ Vu: A User Study Using Images for Authentication. In *Proceedings of the 9th USENIX Security Symposium (SSYM '00)*. The USENIX Association. https://www.usenix.org/legacy/publications/library/proceedings/sec2000/full_papers/dhamija/dhamija.pdf

[14] Alan Dix. 2007. Designing for appropriation. In *Proceedings of the 21st British HCI Group Annual Conference on People and Computers (BCS-HCI '07)*. British Computer Society, 27–30. https://dl.acm.org/doi/10.5555/1531407.1531415

[15] Paul Dourish. 2003. The Appropriation of Interactive Technologies: Some Lessons from Placeless Documents. *Computer Supported Cooperative Work (CSCW)* 12 (2003), 465–490. https://doi.org/10.1023/A:1026149119426

[16] Paul Dunphy, Andrew Monk, John Vines, Mark Blythe, and Patrick Olivier. 2014. Designing for Spontaneous and Secure Delegation in Digital Payments. *Interacting with Computers* 26, 5 (2014), 417–432. https://doi.org/10.1093/iwc/iwt038

[17] Lisa Edgar, Frances Green, Victoria Ward, and Mark Gumbley. 2017. *The Ageing Population: Coping Mechanisms and Third Party Access.* Retrieved April 27, 2020 from https://www.fca.org.uk/publication/research/coping-mechanisms-third-party-access.pdf

[18] Eric B. Elbogen, Joshua Tiegreen, Colleen Vaughan, and Daniel W. Bradford. 2011. Money Management, Mental Health, and Psychiatric Disability: A Recovery-Oriented Model for Improving Financial Skills. *Psychiatric Rehabilitation Journal* 34, 3 (2011), 223–231. https://doi.org/10.2975/34.3.2011.223.231

[19] Chris Elsden, Tom Feltwell, Shaun Lawson, and John Vines. 2019. Recipes for Programmable Money. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, 1–13. https://doi.org/10.1145/3290605.3300481

[20] Annie Harper, Michaella Baker, Dawn Edwards, Yolanda Herring, and Martha Staeheli. 2018. Disabled, Poor, and Poorly Served: Access to and Use of Financial Services by People with Serious Mental Illness. *Social Service Review* 92, 2 (2018). https://doi.org/10.1086/697904

[21] Kristina Höök. 2006. Designing Familiar Open Surfaces. In *Proceedings of the 4th Nordic conference on Human-computer interaction (NordiCHI '06)*. ACM, New York, NY, 242–251. https://doi.org/10.1145/1182475.1182501

[22] R. Jenkins, D. Bhugra, P. Bebbington, T. Brugha, M. Farrell, J. Coid, T. Fryers, S. Weich, N. Singleton, and H. Meltzer. 2008. Debt, income and mental disorder in the general population. *Psychological Medicine* 38, 10 (2008), 1485–1493. https://doi.org/10.1017/S0033291707002516

[23] Jofish Kaye, Mary McCuistion, Rebecca Gulotta, and David A. Shamma. 2014. Money Talks: Tracking Personal Finances. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, 521–530. https://doi.org/10.1145/2556288.2556975

[24] Joseph 'Jofish' Kaye. 2011. Self-reported Password Sharing Strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, 2619–2622. https://doi.org/10.1145/1978942.1979324

[25] Joan Langan and Robin Means. 1996. Financial Management and Elderly People with Dementia in the U.K.: As Much a Question of Confusion as Abuse? *Ageing & Society* 16, 3 (1996). https://doi.org/10.1017/S0144686X00003433

[26] Susan Leigh and Anselm Strauss. 1999. Layers of Silence, Arenas of Voice: The Ecology of Visible and Invisible Work. *Computer Supported Cooperative Work (CSCW)* 8 (1999), 9–30. https://doi.org/10.1023/A:1008651105359

[27] Makayla Lewis and Mark Perry. 2019. Follow the Money: Managing Personal Finance Digitally. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY. https://doi.org/10.1145/3290605.3300620

[28] Open Banking Limited. [n.d.]. *Meet the regulated providers.* Retrieved April 27, 2020 from https://www.openbanking.org.uk/customers/regulated-providers/

[29] Open Banking Limited. [n.d.]. Open Banking Customer Experience Guidelines Version 1.3.0. Retrieved January 28, 2020 from https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines-V1.3.0.pdf

[30] Ingemar Ljungqvist, Alain Topor, Henrik Forssell, Idor Svensson, and Larry Davidson. 2016. Money and Mental Illness: A Study of the Relationship Between Poverty and Serious Psychological Problems. *Community Mental Health Journal* 52 (2016), 842–850. https://doi.org/10.1007/s10597-015-9950-9

[31] Rowland Manthorpe. [n.d.]. To change how you use money, Open Banking must break banks. Retrieved March 18, 2020 from https://www.wired.co.uk/article/psd2-future-of-banking

[32] Daniel C. Marson, Robert Savage, and Jacqueline Phillips. 2006. Financial Capacity in Persons with Schizophrenia and Serious Mental Illness: Clinical and Research Ethics Aspects. *Schizophrenia Bulletin* 32, 1 (2006), 81–91. https://doi.org/10.1093/schbul/sbj027

[33] Money and Mental Health Policy Institute. 2018. *Written evidence to the House of Commons Treasury Committee.* Retrieved August 31, 2020 from http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/consumers-access-to-financial-services/written/94086.html

[34] Nic Murray. 2016. *Strength in numbers: consumers, carers and financial services.* Retrieved April 27, 2020 from https://www.moneyandmentalhealth.org/wp-content/uploads/2016/11/Strength-in-Numbers-report.pdf

[35] ndgit. 2019. *Open Banking APIs Worldwide.* Retrieved April 27, 2020 from https://ndgit.com/en/open-banking-whitepaper

[36] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Dædalus Journal of the American Academy of Arts and Sciences* Fall 2011 (2011), 32–48. https://www.amacad.org/publication/contextual-approach-privacy-online

[37] House of Commons Treasury Committee. 2019. *Consumers' access to financial services.* Retrieved March 18, 2020 from https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/inquiries1/parliament-2017/consumers-access-to-financial-services-17-19/

[38] Royal Bank of Scotland. 2020. *NatWest, Royal Bank of Scotland and Ulster Bank launch card for carers to support vulnerable customers and those in isolation.* Retrieved May 1, 2020 from https://www.rbs.com/rbs/news/2020/04/natwest--royal-bank-of-scotland-and-ulster-bank-launch-card-for-.html

[39] Mark Perry and Jennifer Ferreira. 2018. Moneywork: Practices of Use and Social Interaction around Digital and Analog Money. *ACM Transactions on Computer-Human Interaction (TOCHI)* 24, 6, Article 41 (Jan. 2018). https://doi.org/10.1145/3162082

[40] Gary Pritchard, John Vines, and Patrick Olivier. 2015. Your Money's No Good Here: The Elimination of Cash Payment on London Buses. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15).* ACM, New York, NY, 907–916. https://doi.org/10.1145/2702123.2702137

[41] Thomas Richardson, Megan Jansen, Wendy Turton, and Lorraine Bell. 2017. The Relationship Between Bipolar Disorder and Financial Difficulties: A Qualitative Examination of Patient's Views. *Clinical Psychology Forum* 295 (2017).

[42] Antti Salovaara, Kristina Höök, Keith Cheverst, Michael Twidale, Matthew Chalmers, and Corina Sas. 2011. Appropriation and Creative Use: Linking User Studies and Design. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems (CHI EA '11).* ACM, New York, NY, 37–40. https://doi.org/10.1145/1979742.1979585

[43] Supriya Singh and Kylie Cassar Bartolo. 2004. The Privacy of Money and Health: A User Study. In *Proceedings of the OzCHI (OzCHI '04).*

[44] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07).* ACM, New York, NY, 895–904. https://doi.org/10.1145/1240624.1240759

[45] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Security Design Based on Social and Cultural Practice: Sharing of Passwords. In *Usability and Internationalization. Global and Local User Interfaces. UI-HCII 2007*, Nuray Aykin (Ed.). Springer-Verlag.

[46] Supriya Singh, Anuja Cabraal, and Gabriele Hermansson. 2006. What is your husband's name?: sociological dimensions of internet banking authentication. In *Proceedings of the 18th Australia conference on Computer-Human Interaction (OzCHI '06).* ACM, New York, NY, 237–244. https://doi.org/10.1145/1228175.1228217

[47] Stephen Snow and Dhaval Vyas. 2015. Fixing the Alignment: An Exploration of Budgeting Practices in the Home. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15).* ACM, New York, NY, 2271–2276. https://doi.org/10.1145/2702613.2732808

[48] Stephen Snow, Dhaval Vyas, and Margot Brereton. 2017. Sharing, Saving, and Living Well on Less: Supporting Social Connectedness to Mitigate Financial Hardship. *International Journal of Human-Computer Interaction* 33, 3 (2017), 345–356. https://doi.org/10.1080/10447318.2016.1243846

[49] Team Starling. 2020. *Introducing: Connected cards for Starling personal accounts.* Retrieved May 1, 2020 from https://www.starlingbank.com/blog/introducing-connected-cards-for-personal-accounts/

[50] Lucy A. Suchman. 2007. *Human-Machine Reconfigurations. Plans and Situated Actions* (2nd ed.). Cambridge University Press.

[51] Cheryl Tilse, Deborah Setterlund, Jill Wilson, and Linda Rosenman. 2005. Minding the money: a growing responsibility for informal carers. *Ageing & Society* 25, 2 (2005), 215–227. https://doi.org/10.1017/S0144686X04002983

[52] Cheryl Tilse, Deborah Setterlund, Jill Wilson, and Linda Rosenman. 2007. Research Note: Managing the Financial Assets of Older People: Balancing Independence and Protection. *British Journal of Social Work* 37, 3 (2007), 565–572. https://doi.org/10.1093/bjsw/bcm014

[53] Cheryl Tilse, Jill Wilson, Linda Rosenman, David Morrison, and Anne-Louise McCawley. 2011. Managing older people's money: assisted and substitute decision making in residential aged-care. *Ageing & Society* 31, 1 (2011), 93–109. https://doi.org/10.1017/S0144686X10000747

[54] John Vines, Mark Blythe, Paul Dunphy, and Andrew Monk. 2011. Eighty Something: Banking for the older old. In *Proceedings of the 25th BCS Conference on Human-Computer Interaction (BCS-HCI '11).* BCS Learning & Development

Ltd., Swindon, UK, 64–73.

[55] John Vines, Paul Dunphy, Mark Blythe, Stephen Lindsay, Andrew Monk, and Patrick Olivier. 2012. The Joy of Cheques: Trust, Paper and Eighty Somethings. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work (CSCW '12)*. ACM, New York, NY, 147–156. https://doi.org/10.1145/2145204.2145229

[56] John Vines, Paul Dunphy, and Andrew Monk. 2014. Pay or Delay: The Role of Technology When Managing a Low Income. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, 501–510. https://doi.org/10.1145/2556288.2556961

[57] Dhaval Vyas, Stephen Snow, Paul Roe, and Margot Brereton. 2016. Social Organization of Household Finance: Understanding Artful Financial Systems in the Home. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. ACM, New York, NY, 1777–1789. https://doi.org/10.1145/2818048.2819937

[58] Jill Wilson and Cheryl Tilse. 2015. Opening up Options: Decision Making Around Older People's Assets. *Australian Social Work* 68, 2 (2015), 153–155. https://doi.org/10.1080/0312407X.2015.1010555