From Intent to Action: Nudging Users Towards Secure Mobile Payments

Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh, *Carnegie Mellon University;* Florian Schaub, *University of Michigan*

https://www.usenix.org/conference/soups2020/presentation/story

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

From Intent to Action: Nudging Users Towards Secure Mobile Payments

Peter Story
Carnegie Mellon University
pstory@andrew.cmu.edu

Daniel Smullen
Carnegie Mellon University
dsmullen@cs.cmu.edu

Alessandro Acquisti
Carnegie Mellon University
acquisti@andrew.cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
lorrie@cmu.edu

Norman Sadeh
Carnegie Mellon University
sadeh@cs.cmu.edu

Florian Schaub
University of Michigan
fschaub@umich.edu

Abstract

Despite experts agreeing on many security best practices, there remains a gap between their advice and users' behavior. One example is the low adoption of secure mobile payments in the United States, despite widespread prevalence of credit and debit card fraud. Prior work has proposed nudging interventions to help users adopt security experts' recommendations. We designed and tested nudging interventions based on *protection motivation theory* (PMT) and *implementation intentions* (II) to encourage participants to use secure mobile payments. We designed the interventions using an interview study with 20 participants, and then tested them in a longitudinal, between-subjects field experiment with 411 participants. In one condition, drawing on PMT, we informed participants about the threat of card fraud and the protection offered by mobile payments. In a second condition, we combined the PMT intervention with an II-based intervention, and asked participants to formulate a plan to make a mobile payment in the week ahead. A third condition acted as a control. Both PMT-only and PMT+II interventions made participants more likely to make mobile payments relative to the control group. The results suggest that PMT and implementation intention-based nudges can help people translate their desire to behave securely into actual behavior.

1 Introduction

Survey research consistently shows that people are concerned about their security and privacy [36, 53]. However, research also shows that people often do not take steps to protect themselves [14, 45]. A prime example is the continued prevalence of payment card usage (and the elevated risk of fraud associated with them) in the United States, despite the availability of alternative payment technologies that could limit fraud. Card fraud remains enormously lucrative for criminals, and compromised point-of-sale terminals are a major source of card information [29, 30]. Mobile payments (e.g., Apple Pay) incorporate security measures that protect against this threat (i.e., payment tokenization) [10, 21, 58], and are widely available [51]. Despite this, adoption of mobile payments in the United States lags far behind other countries [50, 57]. The reasons for this lag may be multiple and various, from status quo bias, to faith in card issuers' willingness to cover losses, to lack of awareness about the threat of card fraud and the protection offered by using mobile payments.

In the context of security and privacy, behavioral economics provides convincing explanations for why people sometimes act in manners that subtly diverge from their expressed preferences, including failing to protect their security and privacy even when users claim security and privacy to be important to them [2, 3]. Researchers have proposed a variety of ways to help users protect themselves, and frameworks incorporating *nudges* are especially promising [4]. Nudges are carefully crafted interventions that help users to act in ways that align with their stated preferences. The privacy and security literature demonstrates the effectiveness of a number of different nudges in this domain [4–6, 8, 17]. However, it is notable that *implementation intentions* are largely unstudied in the field of security and privacy, despite decades of strong support for their effectiveness in the medical domain [19, 32, 56]. Implementation intentions are contextually activated mental plans that help people follow through on their goals. Implementation intentions appear to be well-suited to situations where a person needs to remember to take an action to protect themselves, such as remembering to pay using a secure mobile payment system instead of swiping their card [22]. Prior work suggests that implementation intentions are effective when paired with *protection motivation theory*-based (PMT) interventions [42]. Protection motivation theory claims that users'

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

protection-seeking actions are based on their perceptions of threats and possible responses [43, 54, 62]. In the context of mobile payments, our interventions aimed to educate participants about the threat of card fraud and the protection offered by using mobile payments instead of physical cards.

To investigate the impact of PMT and implementation intention nudges on the adoption of mobile payments, we first conducted a series of interviews with 20 participants to understand people's thoughts about card fraud, mobile payments, and our implementation intention plan (§ 3). Next, informed by the findings from our interviews, we conducted a longitudinal, randomized controlled experiment with 411 participants to measure the effect of two interventions on participants' use of a specific payment system (Apple Pay) (§ 4). We preregistered our study design prior to collecting any data. Our results showed that participants in our PMT-only and PMT with implementation intention treatment groups were 2.4x ($p = 0.020$) and 3.9x ($p < 0.001$) more likely to use Apple Pay than were participants in our control group, respectively. Our findings further suggest that adding an implementation intention to our PMT-only treatment increased its efficacy (1.7x more likely, $p = 0.085$). These results show that PMT and implementation intention-based nudges can be a powerful tool for helping people translate their intention to behave securely into actual behavior. Finally, we discuss the implications of our findings (§ 5) and our conclusions (§ 6).

2 Related Work

In this section we describe the rationale for nudging people to adopt mobile payments (§ 2.1), previous use of nudges in the context of security and privacy (§ 2.2), and how protection motivation theory and implementation intentions informed the design of our nudges (§ 2.3).

2.1 Card Fraud and Payment System Security

Credit and debit card fraud takes place when a criminal either obtains a physical card or obtains information about a card, and then initiates a transaction that the card owner did not consent to. Two major sources of card information are compromised point of sale terminals (POSs) [29, 30] and compromised retail websites [28]. The interventions we study focus on protecting against compromised POSs. Criminals can compromise POSs by remotely installing malware on them [30], but physical compromise is also possible (e.g., using skimmers) [26]. When a card's magnetic stripe is swiped on a compromised POS, the information on the magnetic stripe can be recorded and used to make counterfeit cards. When a card's chip is inserted into a compromised POS, in the best case the only useful information that can be stolen are the card number, cardholder name, and expiration date [27]. However, chips implement a variety of EMV protocols, some of which are susceptible to card cloning (e.g., static data card authentication) and have other known weaknesses [25, 69]. Contactless card transactions suffer from similar weaknesses [69]. Thus, compromised POSs can trivially steal valuable magnetic stripe data and still pose a threat to EMV cards.

Apple Pay, Google Pay, and Samsung Pay allow users to register credit or debit cards on their phone, so that payments can be made through the phone rather than with physical cards. These mobile payments systems can protect against compromised POSs. First, Pay[1] always uses transaction-specific codes [10, 21, 58], making re-use of transaction information theoretically impossible. Second, Pay uses a device-specific card number in transactions, so a compromised POS cannot steal the original card number. Thus, mobile payments are a strong protection against compromised POSs. In addition, unlike most EMV cards in the United States, a biometric or PIN is used to authenticate the user before a transaction can be made, making it much more difficult for a thief to use a stolen device with Pay.

Despite their security benefits, fewer than half of Americans use mobile payments regularly [50, 51, 57]. As noted in the Introduction, the reasons behind the lag in adoption may be various. For instance, research by Pew and Huh et al. suggest that it is partly due to people's belief that smartphone-based payment systems are less secure than paying with physical cards [22, 50]. Furthermore, Huh et al.'s participants reported that lack of availability, convenience, and forgetfulness were reasons why they did not use Apple Pay or Android Pay [22]. These findings led us to test using nudges to correct people's misconceptions and to encourage them to start using Pay.

2.2 Nudges for Security and Privacy

A large body of research examines ways to help people protect their security and privacy. For example, researchers have studied how to improve privacy notices [24], how to guide people towards choices that fit their preferences [34], and how a lack of usability can inhibit adoption of security tools [31, 72]. This varied research is unified by the acknowledgment that people have limited cognitive resources and suffer from behavioral biases.

Inspired by work in psychology and behavioral economics [67], researchers are increasingly studying how *nudges* can improve design for security and privacy [4]. Nudges are design elements that help people overcome their cognitive and behavioral biases in order to make decisions which align with their stated preferences. For example, Almuhimedi et al. used nudges to mitigate the information asymmetry between users and the behaviors of apps on their devices [7, 8]. Their nudges were successful at encouraging users to reassess and restrict permissions settings. Frik et at. tested using nudges to overcome present bias [17]. They

[1] In the rest of this manuscript, we use *Pay* to refer to Apple Pay, Google Pay, and Samsung Pay generically.

found that users given the option to be reminded later were less likely to completely dismiss prompts for security updates and 2FA configuration. Albayram et al. and Al Qahtani et al. used educational videos to motivate participants to enable lock screens on their smartphones [5, 6]. In both studies, the videos successfully motivated many participants to enable secure lock screens. However, nudges are not always effective [4], which shows the value of empirical research like ours.

2.3 Nudges to Protect Against Card Fraud

Our goal was to test whether nudges that focus on security can induce individuals to consider using mobile payments to protect themselves, and whether those nudges can help them translate that intention into actual behavior. *Implementation intentions* are designed to help people translate intention into behavior, especially in cases when people must remember to take some action (i.e., use Pay instead of swiping a card). An implementation intention is a concrete, contextually activated plan to achieve a goal [19]. The plan should be specific (e.g., specifying location or time), which facilitates the plan being triggered in the planner's mind by contextual factors (e.g., when they arrive at a certain location). In our study, we encouraged participants to fill in a plan template detailing up to three locations where they would make a mobile payment in the week ahead (Figure 12).

Research in the medical domain has shown that encouraging people to form implementation intentions can have a powerful effect on people achieving their goals. For example, Milne et al. successfully used implementation intentions to encourage young people to exercise in order reduce their future risk of heart disease; 91% of the participants who formed implementation intentions exercised in the week after treatment, as compared to only 35% of the group that was only exposed to motivational materials [42]. Implementation intentions have been shown to be effective in many other contexts [40, 41, 44, 46, 47]. However, with the exception of a study design described by Liao et al. [33], we are unaware of explicit application of implementation intentions in the domain of security and privacy. Thus, a contribution of our work is bringing awareness of implementation intentions to our research community.

In a review of studies of implementation intentions, Gollwitzer explains why and when implementation intentions are effective [19]. Implementation intentions are effective because they help people remember to perform their planned action. Also, planning the details of the action reduces the amount of conscious effort needed when it comes time to perform the action. Implementation intentions are most likely to be effective when the person has a strong commitment to both their plan and to the goal that motivates the plan. Thus, implementation intentions to protect security and privacy should have an effect when users are motivated to take action to protect themselves. In order to motivate participants in our study, we draw on Protection Motivation Theory (PMT) [37, 54, 55]. PMT has been applied in both the medical domain [43, 74] and in computer security [5, 6, 12, 60–62]. PMT proposes that people are more likely to take action to protect themselves from a threat when they perceive that the threat is severe (i.e., greater perception of *threat severity*), that they are susceptible to the threat (i.e., greater perception of *threat susceptibility*), that the action they could take is not too difficult to perform (i.e., greater perception of *self-efficacy*), and that the action they could take will be effective in protecting against the threat (i.e., greater perception of *response efficacy*) [43, 74]. PMT has been effectively combined with implementation intentions in domains outside of security and privacy. For example, in their study of implementation intentions for exercise, Milne et al. used PMT to motivate participants [42].

In summary, in our study we designed and tested nudges to help participants protect themselves from card fraud by adopting mobile payments. In particular, we designed our nudges based on PMT and implementation intentions, a combination which, to the best of our knowledge, we are the first to test in the domain of security and privacy.

3 Qualitative Interviews

The first part of our study focused on gathering qualitative information on people's thoughts about the threat of card fraud, the use of Pay[1] to protect against card fraud, and people's experiences forming implementation intention plans to use Pay. We conducted a series of surveys and interviews to gather longitudinal self-reported data about participants' experiences. Our findings informed the design of our controlled experiment (§ 4), allowing us to refine our interventions, correct common misconceptions, and to understand some of the limitations of our approach. All of our study protocols were approved by Carnegie Mellon University's IRB.

3.1 Protocol

This portion of our study included three surveys and two interviews (illustrated in Figure 7 in the appendix). We recruited participants from Craigslist and Carnegie Mellon University's participant pool. Survey #1 gathered information about users' devices, prior use of payment methods, perceptions of the likelihood and severity of card information theft and fraud, prior experience with card information theft and fraud, and demographic information. We reasoned that our nudges would have the largest impact on people who were not already using Pay,[1] but whose phones were compatible with Pay and were likely to have opportunities to use Pay. Thus, we screened out participants who reported having used Pay in a physical location in the past month, we required that participants had made at least one payment with a credit or debit card in a physical location in the past month, and we required that their smartphone be compatible with either Apple Pay, Google Pay, or Samsung Pay.

We invited a diverse subset of qualifying participants to participate in a semi-structured interview (Interview #1). In accordance with purposive sampling, our attempt to balance several factors of interest (e.g., phone type, age, occupation, fraud-related perceptions, etc.) influenced our choice of who to invite to the interview. 20 participants attended Interview #1. 75% of our participants were female, their median age was 26.5, 55% had iPhones, 25% had Samsung phones, and 20% had other Android phones. The interview started with a discussion of prior experiences with card fraud, card information theft, and prior experiences with Pay. Next, the interviewer described recent cases of card information theft from major retailers, and the potential consequences of such theft for the participant. This intervention was included in order to help participants develop an accurate perception of their *susceptibility* to card fraud and the potential *severity* of card fraud, two elements of *threat appraisal* that protection motivation theory (PMT) suggests are associated with protective behavior [43]. Then, the interviewer described how Pay may protect against card information theft, presented the participant with instructions for setting up and using Pay, and gave the participant the opportunity to set up Pay if they wanted to. This intervention was included in order to help participants understand how Pay may help protect them from card fraud and to give them confidence that they can use Pay, influencing perceptions of *response efficacy* and *self-efficacy*, two additional elements of PMT. Next, participants were given an opportunity to form an implementation intention by filling out a paper template. The template encouraged participants to plan where they might use Pay in the coming week and to mentally rehearse using Pay in these locations. These activities were designed to help mentally activate participants' plans to use Pay when they were in these locations [19]. Finally, participants were given the opportunity to express a strong commitment to their plan, which prior work suggests increases the efficacy of implementation intentions [19, 63]. The template was similar in content to the template in our controlled experiment (see Figure 12).

One week after completing Interview #1, participants were sent Survey #2, which asked whether participants had set up Pay after the interview, whether they had tried to use Pay, and whether they had successfully used Pay. Participants who completed Interview #1 and Survey #2 were compensated with a $15 Amazon e-gift card.

Participants who completed Survey #2 and who had set up Pay on their phones were invited to Interview #2, which was designed to understand people's experiences using Pay or their reasons for not using it. We also asked questions about whether participants followed their implementation intention plans and whether they found the plans to be helpful. Participants in Interview #2 were compensated with an additional $15 Amazon e-gift card.

Four weeks after completing Survey #2, participants who had set up Pay on their phones were invited to take Survey #3, which asked whether participants had used Pay in the past week. We also asked whether participants thought they were likely to use Pay in the future. Our surveys and interview scripts are included in the appendix (§ 8.1-8.5).

3.2 Analysis

We used thematic coding to analyze transcripts of our interviews and our survey's open-text responses. Two of the authors reviewed these materials together and collaboratively developed a codebook. To ensure that the codes we developed later were consistently applied to the materials we analyzed earlier, one author then re-reviewed all the materials. Since our goal for this portion of our study was to gather rich, qualitative data, we did not attempt to calculate measures of annotator reliability [39]. Table 4 in the appendix contains our final codebook and the frequencies of our codes.

3.3 Results

Below we summarize key takeaways from our survey and interview data. Although in some cases we report the frequency of codes, due to our use of purposive sampling in selecting participants, it would be inappropriate to assume that these frequencies correspond to the frequencies that might be observed in the general population.

Use of Pay

We received 288 complete responses to Survey #1. Among these respondents, only 34.7% reported using Pay sometime in the past, and a mere 23.6% reported using Pay in the past month. We recruited only respondents who had not used Pay in the last month for Interview #1. In Interview #1, nearly all participants (19/20) said they had heard of Pay before our study, but only one participant reported using it to pay in a physical location before. Multiple participants mentioned seeing Pay in advertisements, seeing it on their phone, seeing it as a payment option, using it for digital purchases, or knowing that friends or family use it. This widespread awareness of Pay makes sense, considering that many smartphones come with Pay preinstalled [20, 59] and that iPhones include persistent reminders to set up Apple Pay [23].

Prior to Interview #2, 11/20 participants had Pay set up on their phone, and so could have used it before Interview #2. One participant had set up Pay prior to Interview #1, four set it up in Interview #1, and six set it up after Interview #1. Participants gave a variety of different reasons for not setting up Pay including being too busy, not thinking they needed it, wanting to do more research, and wanting to consult their partner. Between Interview #1 and Interview #2, seven participants used Pay. Three of these participants used Pay successfully at at least one of the locations in their plan.

To understand whether participants were likely to continue using Pay after our study, four weeks after completing Survey #2 we sent Survey #3 to all participants who had set up Pay. In response to Survey #3, three participants indicated that they had successfully used Pay to make a payment in a physical location in the prior week.

Our results suggest that despite widespread awareness of Pay, most people are not using it regularly. However, after being exposed to our nudges in Interview #1, a substantial percentage of participants (35%) used Pay at least once during the remainder of our study. Furthermore, responses to Survey #3 indicate that our nudges may increase use of Pay long after the initial intervention. These results encouraged us to move forward with the controlled experiment described in § 4.

Perceptions of Threat Susceptibility and Severity

All but one participant recounted their own or others' experiences with card fraud. Fewer participants (10/20) recounted experiences with card information theft. When asked to describe experiences with card information theft, seven participants instead described cases of card fraud or theft. This makes sense, given that card information theft can be difficult for individuals to detect directly.

After we described recent hacks in which credit and debit card information was stolen and the possible consequences of having one's information stolen, we asked questions to gauge participants' levels of concern about and perceptions of susceptibility to card fraud and information theft.

Participants expressed varied opinions about their susceptibility to these threats. Eleven participants expressed that information theft happened frequently (P14: "It just seems like it does happen so frequently..."), but three participants said such occurrences were infrequent (P6: "Cause even like ... the hacking things you mentioned, I mean they're once in a blue moon."). Three participants said their behavior made theft or fraud more likely, but nine others thought their behavior lowered their likelihood of suffering from card information theft or fraud.

Participants described a number of negative outcomes associated with card theft and fraud, including the hassle and stress of dealing with it, feelings of anger and helplessness, loss of money due to theft or overdraft fees, and the fear that additional bad things might happen to them. Participants also mentioned that their level of concern would depend on the size of the fraudulent purchase and whether the purchase was on their credit or debit card. Ten participants expressed confidence that their card issuer would help them resolve fraudulent purchases, and two even thought they would be refunded under all circumstances. It is potentially a misconception to believe that fraudulent charges will be refunded in all cases, since U.S. law does not require this of card issuers [13].

Our takeaway is that while most participants have a high level of awareness of the possibility of card fraud, some people remain under-informed and might benefit from additional information.

Perceptions of Self-efficacy

Some participants thought Pay setup was easy, but others encountered difficulties. In particular, two participants were confused by Apple Pay's ability to automatically add card details using the phone's camera and three mentioned interacting with their bank to approve registering their card as a challenge. Additionally, two participants found that certain cards simply could not be added to Pay. Seven participants said that setup or use would be a challenge, and would require practice, learning, or attention to detail.

Eleven participants said they did not (or might not) have opportunities to use Pay because they did not go shopping, did not have enough money, or due to other reasons.

Participants described different challenges they might (or did) encounter in stores using Pay. First, stores might or might not accept Pay. Second, participants might not remember to use Pay, suggesting an opportunity for implementation intentions to help in this area. Third, participants might experience difficulty using Pay. Despite our written instructions, some participants still had questions about how to use Pay. Thus, we included a short video alongside written instructions in our controlled experiment (§ 4). Participants also described positive aspects of Pay. Some participants expressed that Pay was easy to use, that it would allow them to not carry or take out their cards or wallet, that it would be a good backup option if they didn't have a card, and that it would be fun to try something new.

Two usability challenges in particular may be of interest, due to their potential generalizability: the case of accidental activation and the case of failure to activate. Four of our participants who set up Apple Pay described accidentally activating it and not knowing why this was happening. Not understanding this accidental activation alarmed at least one of our participants (P19: "The credit thing keeps popping up whenever I angle my phone a certain direction. I wonder where it's sending my credit info each time."). It is possible to open Apple Pay by either double-clicking the home button when the phone is locked or by bringing the phone in proximity to an NFC reader (even if the NFC reader is not a payment terminal). To address some of this confusion, we added the double-clicking functionality to our instructions in subsequent interviews and in our experiment. One of these same participants (P11) also experienced the problem of Apple Pay not activating. At one location, this participant reported having to scan their phone twice before it worked. At another location, the participant was ultimately unsuccessful using Apple Pay, concluding that it must not have been supported and expressing frustration with this failure mode:

“What happens when it doesn’t work is nothing happens. It just sits there. And it doesn’t even apologize. You know it doesn’t say anything on it. ‘Oops, sorry. Try again.’ Nothing like that.” Unfortunately, due to the lack of an NFC signal in the case when a terminal does not support NFC payments, it is hard to imagine a technical solution to this kind of silent failure mode. Thus, while some of these usability challenges may be addressable through education, some may be inherent to the technology.

Perceptions of Response Efficacy

Most participants (14/20) expressed some confidence in the security properties of Pay that we described. However, nine participants also expressed concern about Apple, Google, or their phone being hacked. P16 cited their previous experience having their iTunes account hacked as a reason for not believing that Apple Pay would protect their card information: “[T]he only time I’ve been hacked was with an Apple product. That’s the only reason. ... [T]he only time I had a fraudulent charge was when I was with an Apple product.” Interestingly, this participant also recognized that the hack was likely due to their choice of a weak password, saying: “I guess my password wasn’t as secure as I thought it was.” P11 said that “I feel as if the phone is more vulnerable than the computer.” P8 expressed a more concrete concern about NFC signal skimming, expressing concern that “...in a physical store ... the person behind you can actually take your information if they know what they’re doing on the phone.”

Despite participants’ concerns about hacking, Apple Pay is designed to be resistant to hacking: card information is not stored with Apple after the initial enrollment process, mitigating the risk of data breach, device-specific Device Account Numbers are stored on each phone’s Secure Element, protecting against phones being compromised, and user interaction is required before making payments [10]. Google Pay and Samsung Pay employ similar protections [21,58]. Of course, attacks that can thwart these protections are possible (e.g., a persistent threat on Apple’s servers), but such attacks would require substantially more resources than simply adding card skimmers to point of sale terminals. Communicating useful mental models to non-technical users remains an open research area [71]. Our participants’ responses point to the challenge of communicating complex threat models to a general audience.

Awareness of Protection Actions

Participants demonstrated awareness of many different ways they could protect themselves from credit and debit card information theft and fraud. The most prevalent actions involved working with one’s card issuer, such as reporting fraudulent purchases or receiving a new card. Actions involving physical awareness (e.g., looking for card skimmers), monitoring card statements for unauthorized transactions, protecting access to one’s account (e.g., with a strong password), using cash, or using a credit card (e.g., due to liability protections) were also common. Interestingly, two participants brought up the possibility of using Apple Pay to protect themselves before we had described it as being a secure payment method (but after we had asked them whether they had used it). P18 even gave an accurate explanation of why Apple Pay might be more secure: “Maybe I could use Apple Pay or something. Then if I don’t give my card information directly to these companies or grocery stores, if I go via a secure party like Apple Pay, it should be a good option.”

Our overall takeaway is that most participants are aware of some ways they can protect themselves from card information theft and fraud. Unfortunately, prior work and the continued profitability of card fraud suggest that people’s ability to protect themselves is limited (e.g., password re-use is prevalent [48]). In addition, most participants seemed unaware that Pay could protect them before we explained that it could, suggesting our information about Pay may be helpful.

Effectiveness of Implementation Intentions

All participants were given the opportunity to form an implementation intention plan to help them remember to use Pay. 16/20 participants wrote or described at least one location where they might use Pay. About half of participants checked or otherwise indicated that they performed at least one mental rehearsal activity. As we conducted interviews, we refined the way we introduced the plan to communicate that filling out and following the plan were not mandatory, but that filling out the plan was encouraged if the participant wanted to remember to use Pay. Participants described several obstacles to forming an implementation intention, including not being able to think of places they would visit, not having decided whether they wanted to use Pay, and simply thinking the plan wouldn’t be helpful for them. In addition, four participants had at least some difficulty remembering their plan in Interview #2. The act of forming a plan seemed to help four participants understand where Pay could be used. For example, P11 realized that it would be difficult to use Pay at a restaurant where waiters collect cards for payment processing. Participants also described other things that could remind them to setup or use Pay, including receiving notifications from Google Pay about availability, adding Pay to their shopping list, and putting the Pay app on their home screen.

Of the seven participants who used Pay between Interview #1 and Interview #2, three used Pay successfully at at least one of the locations in their plan. As the majority of participants were able to form plans, and some of the participants who formed plans went on to use Pay at their planned locations, we thought that our implementation intention plan template was worth testing in our controlled experiment (§ 4). At the same time, our plan may be unhelpful to participants who have difficulty thinking of locations they are likely to make payments in the coming week, and is almost certain to be unhelpful for participants who simply decide not to use Pay. Since Pay is not available in all locations, it is unsurprising that many participants had questions about where they could use Pay. As part of our description of Pay, we described just four popular locations where Pay can be used in our city. With a more comprehensive list of locations, it might be possible to develop an interactive plan template which could contribute to greater awareness of where Pay is available.

Misconceptions and Other Concerns

Our interviews helped us identify a number of misconceptions related to Pay. For example, four participants thought Pay might interfere with their credit card rewards (P5, P9, P12, P16), four participants thought our study was affiliated with Apple (P11, P16, P19, P20), three participants wondered if Pay cost something (P5, P8, P15), and one participant thought Pay might prevent them from getting receipts (P12). In addition, P7 thought Samsung Pay was a credit card and two participants confused Apple Pay with iPad-based point of sale terminals (e.g., Square). We addressed several of these misconceptions in a "Frequently Asked Questions" section in our controlled experiment (Figure 11).

Pay on watches offers the same level of security as on phones, but with potentially greater convenience. Thus, we were surprised that all three of the participants we spoke with about their smartwatches expressed skepticism about using Pay with their watches. P1 thought they would start using Apple Pay on their iPhone, because they thought they would need to practice the motion of making payments with their Apple Watch. P12 thought Apple Pay would be less secure on their Apple Watch than on their iPhone because their Apple Watch did not have a fingerprint reader. Neither P1 nor P12 set up Apple Pay during our study. In Interview #1, P15 was worried that setting up Samsung Pay might allow transactions to be made through their Samsung Watch without their knowledge, due to the fact that their watch did not have a PIN. In Interview #2, P15 said they had figured out how to add a PIN to their watch, and after doing so they proceeded with the setup of Samsung Pay.

3.4 Limitations

To protect external validity, it was important that participants understood that they were not required to set up Pay, use Pay, form an implementation intention, or follow their implementation intention. We iterated on the design of our interview protocol until we arrived at language which we thought communicated this clearly to participants. However, although setting up Pay was not required to receive compensation for Interview #1 and Survey #2, participants who never set up Pay were not invited to Interview #2 or Survey #3. Although we tried to disguise the qualification criteria for Interview #2 and Survey #3 from participants, participants may have inferred that some action on their part would be required to qualify, and some asked us directly in the interview. To ensure this was not a threat to validity in our controlled experiment, we emphasized that participants' compensation would not be affected by their use or non-use of Pay.

The generalizability of our findings might be impaired by our relatively small sample size ($n = 20$) and recruitment from the geographic area around our institution. To mitigate this, we used purposive sampling to recruit a diverse set of participants. Further, we recruited a much larger set of participants in our controlled experiment (§ 4).

4 Controlled Experiment

The primary goal of the second part of our study was to determine whether participants presented with a PMT-only nudge and a PMT with implementation intention nudge would be more likely to use mobile payments than those who were not presented with these nudges. Thus, we designed and conducted a randomized controlled experiment with a sufficient number of participants ($n = 411$) to determine statistical significance. Our experimental design was influenced by the results of our qualitative interviews. In particular, over the course of our interviews we iterated on the design of our nudges and we compiled a list of common questions and misconceptions which we sought to correct in our experiment. For ease of recruitment and to reduce the complexity of our protocol, we choose to focus on Apple Pay.

4.1 Protocol

Our design included three experimental conditions. In our control group, we did not try to motivate participants to use Apple Pay. In our PMT group, we presented participants with information about the threat of card fraud (Figure 9) and the mitigation of using Apple Pay (Figure 10 and Figure 11) in order to motivate them to use Apple Pay. This motivational intervention was based on protection motivation theory [43], as described in § 3.1. In our PMT+II group, we presented participants with the motivational intervention of the PMT group in addition to an opportunity to form an implementation intention. This opportunity took the form of a template we designed to help participants plan where they could use Apple Pay, as shown in Figure 12 in the appendix. We did not test an implementation intention intervention without a PMT intervention because the literature suggests that implementation intentions are only effective when participants are motivated [19].

Our study consisted of three surveys hosted on Qualtrics using recruitment from Prolific (see Figure 8 and § 8.6–8.8 in the appendix). Survey #1 was designed to determine eligibility for Survey #2 and Survey #3. The only requirements for taking Survey #1 were that participants live in the United States, speak English, be at least 18 years old, and have an iPhone. We thought our nudges would have the largest impact on people who were not actively using Apple Pay, but whose phones were compatible with Apple Pay and who were likely to have opportunities to use Apple Pay in the week ahead. Thus, to be eligible for participation in Survey #2 and #3, participants must have purchased their iPhone in the United States, owned an iPhone model compatible with Apple Pay (iPhone 6 or newer), must have had a version of iOS compatible with Apple Pay (iOS 12.2 or higher), in the last week must have made an in-person payment in a physical location using their credit or debit card, in the last week must not have made an in-person payment in a physical location using Apple Pay, and they must have passed a simple attention check.

Shortly after completing Survey #1, participants were invited to Survey #2, which contained our randomly assigned experimental conditions. The control group saw only a short description of Apple Pay. The PMT group was provided with a description of the threat of credit and debit card information theft and fraud, and information about the mitigation of using Apple Pay. This information included written instructions about how to set up and use Apple Pay, a short video showing how to use Apple Pay, and an FAQ addressing questions participants asked in our qualitative interviews. We encouraged participants to set up Apple Pay if they wanted to, but we reassured participants that their compensation would not be affected if they did not set it up. The PMT+II group received the same information as the PMT group, but was also given a chance to form a plan to use Apple Pay. Near the end of the survey, participants in the treatment groups were given links to the information about Apple Pay and their plan for using Apple Pay, with the option to request that these links be sent to them via Prolific. Participants in all treatment groups were asked demographic questions and questions related to their perceptions of Apple Pay and card fraud.

Survey #3 was sent to participants one week after they completed Survey #2 in order to measure whether they had used Apple Pay. We asked participants whether they had registered a card in Apple Pay, whether they had made an in-person payment using Apple Pay, and about other details related to their use of Apple Pay and other payment methods.

Our goal was to pay participants \$12/hour, so compensation was determined based on estimated duration of our surveys. Survey #1 was estimated to take five minutes, so compensation was \$1. Survey #2 was estimated to take up to 30 minutes (accounting for time potentially spent outside the survey setting up Apple Pay), so compensation was \$6. Survey #3 was estimated to take five minutes, so compensation was \$1. Participants only received compensation for Survey #2 and Survey #3 if they completed both surveys within three days of being invited.

We conducted an a priori power analysis using G*Power to determine our target number of participants [16]. We planned three chi-square tests of independence to compare the use of Apple Pay between the three treatment groups. In order to detect a small to medium effect size ($w = 0.2357$, informed by the effect size seen in our interviews), with a Bonferroni corrected $\alpha = 0.05 \div 3 = 0.01667$, power=0.9, and df=1, we determined that we needed 122 participants in each treatment.

Treatments	% that used Pay	Odds Ratio	p-value
Control vs PMT+II	8.7% vs 27.2%	3.92	<0.001
Control vs PMT	8.7% vs 18.3%	2.35	0.020
PMT vs PMT+II	18.3% vs 27.2%	1.67	0.085

Table 1: Comparisons between the percent of participants who reported using Apple Pay in each of our treatment conditions. Per convention, the reported odds ratios correspond to large, medium, and small effect sizes, respectively [66].

We preregistered our protocol on The Open Science Framework prior to collecting any data (§ 7).

4.2 Analysis

We collected 670 valid responses to Survey #1, and invited 430 qualifying participants to participate in Survey #2. Of the 430 participants invited to Survey #2, 418 completed Survey #2 and 411 went on to complete Survey #3, for an overall dropout rate of 4%.

After completing data collection, we conducted our preregistered hypothesis tests to compare use of Apple Pay between our three treatment conditions, and we report these findings in § 4.3. Next, we conducted a series of exploratory analyses, which we report in § 4.4.

4.3 Results

We conducted three chi-square tests of independence to compare the use of Apple Pay between our three treatment groups, as shown in Table 1. We used the Holm-Bonferroni method to control Type I error.[2] Participants in the PMT+II group, who saw our PMT with implementation intention nudge, were 3.92x more likely to use Apple Pay than our control group ($p < 0.001$). Participants in the PMT group, who saw only the PMT nudge, were 2.35x more likely to use Apple Pay than our control group ($p = 0.020$). Both of these differences were statistically significant at $\alpha = 0.05$. However, we did not find a statistically significant difference in use of Apple Pay between the PMT and PMT+II groups ($p = 0.085$).

Therefore, we have evidence that our interventions in both the PMT+II and PMT groups had large and medium effects

[2] In our preregistration, we described using a Bonferroni correction. We switched to the Holm-Bonferroni method because it controls the experiment's Type I error rate at the same level as a Bonferroni correction, while having a lower Type II error rate [1, 73]. Using a simple Bonferroni correction, only our Control vs PMT+II comparison would have been found significant. See [11] for further discussion of the Bonferroni correction.

on participants' use of Apple Pay, respectively. Since the treatment conditions only differed in their inclusion of our educational materials (Figures 9, 10, and 11) and our implementation intention template (Figure 12), we can conclude that these differences are what made participants more likely to report using Apple Pay. Although we did not find statistically significant differences between the PMT and PMT+II groups, our findings suggest ($p = 0.085$) that the inclusion of the implementation intention plan had a small effect on increasing the PMT+II participants' use of Apple Pay.

4.4 Results of Exploratory Analyses

Although our primary research questions were about the effect of our nudges on participants' use of Apple Pay, the data we collected gave us the opportunity to explore additional questions. Note that these exploratory analyses were not part of our preregistered study design. In this section, we describe the effect of our nudges on participants' attitudes, how expressed intention differed from reported behavior, exactly when participants reported setting up Apple Pay, and additional factors associated with use of Apple Pay.

Effects of Interventions on Attitudes

After testing for the effect of our interventions on participants' use of Apple Pay (§ 4.3), we decided to test for other potential effects, as shown in Table 2. We used Kruskal-Wallis tests for all variables except whether participants registered a card, where we used a chi-square test of independence. Details of the statistically significant results are shown in Figures 1, 2, and 3. Effect sizes are given as epsilon-squared (ε^2) estimates [38, 68]. Insignificant results are included in Figures 13–17 in the appendix. Post-hoc Dunn tests significant at $\alpha = 0.05$ after Holm-Bonferroni correction are bolded.

As shown in Figure 1, our treatments had a dramatic effect on participants' agreement that Apple Pay would protect them from card fraud ($\varepsilon^2 = 0.241$, $p < 0.001$). In the control group, only 37% of participants agreed that Apple Pay would protect them, whereas in both treatment groups over 84% agreed. Thus, we have strong evidence that our information was effective at correcting people's misconceptions about Apple Pay's security [22]. As illustrated in Figure 2, our treatments increased participants' expressed intentions to use Apple Pay, and implementation intentions were even more effective at increasing intention than PMT alone ($\varepsilon^2 = 0.172$, $p < 0.001$). Finally, Figure 3 shows that our treatments had a small effect on participants' belief that Apple Pay would be useful for making payments ($\varepsilon^2 = 0.015$, $p = 0.047$).

Intention vs Behavior

Comparing participants' Survey #2 responses to their Survey #3 responses gave us insight into how participants' stated intentions to act did or did not translate to actual behavior.

Variable	**p-value**
Perception of threat severity	0.932
Perception of threat susceptibility	0.881
Perception of self-efficacy	0.523
Perception of response-efficacy	**<0.001**
Expressed intention to use Pay	**<0.001**
Perception of Pay's usefulness	**0.047**
Self-consciousness using Pay	0.628
Registered card by end of study	0.237

Table 2: The results of hypothesis tests measuring whether these variables differed between our treatment groups. p-values significant at $\alpha = 0.05$ are bolded, representing tests where the null hypothesis was rejected.

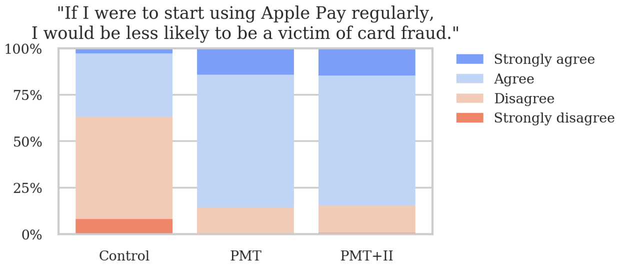


Figure 1: Participants in our treatment groups expressed greater agreement that Apple Pay would protect them from card fraud (i.e., response efficacy). Post-hoc tests: **Control vs PMT**, $\mathbf{p < 0.001}$; **Control vs PMT+II**, $\mathbf{p < 0.001}$; PMT vs PMT+II, $p = 0.880$.

First, we measured how stated intention to register a credit or debit card in Apple Pay translated to actually setting up Apple Pay. As shown in Figure 4, while half of those who expressed a strong intention to register a card did so, those who expressed weaker intentions were correspondingly less likely to register a card. In particular, note that less than half of the participants who responded with "Agree" actually set up Apple Pay by the time of Survey #3.

Next, we compared stated intention to use Apple Pay to actual use of Apple Pay. We performed a chi-square test of independence and found that those who indicated they intended to use Apple Pay in the week ahead were more likely to use Apple Pay than those who did not ($p < 0.001$). However, as shown in Figure 5, many participants who expressed an intention to use Apple Pay did not do so. This reinforces our belief that it is important to ask participants about their actual behavior, rather than only measuring their intentions.

Finally, we took a closer look at the behavior of participants in the PMT+II group, who were given the opportunity to make a plan for using Apple Pay. 96.3% of participants in the PMT+II group wrote plans in Survey #2. Of those who wrote plans, 88.5% visited a location in their plan, 25.2%

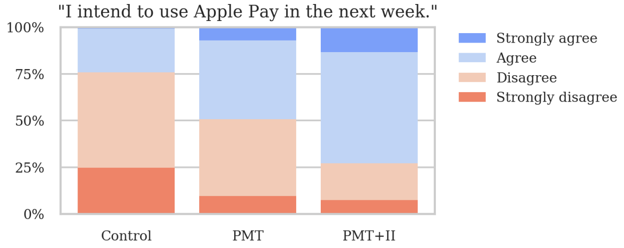


Figure 2: Participants in our treatment groups expressed stronger intentions to use Apple Pay. Further, participants who received the implementation intention treatment expressed even stronger intentions to use Apple Pay than did participants who only received the PMT treatment. Post-hoc tests: **Control vs PMT, $\mathbf{p < 0.001}$; Control vs PMT+II, $\mathbf{p < 0.001}$; PMT vs PMT+II, $\mathbf{p = 0.001}$**.

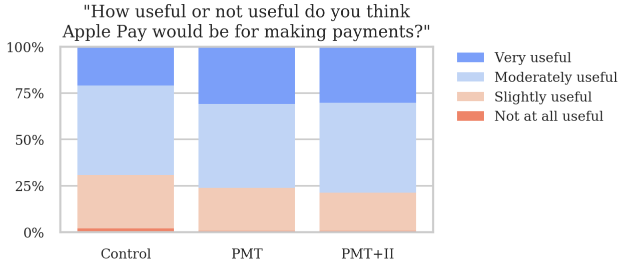


Figure 3: Our treatments had an effect on participants' belief that Apple Pay would be useful for making payments. Post-hoc tests: Control vs PMT, $p = 0.046$; Control vs PMT+II, $p = 0.026$; PMT vs PMT+II, $p = 0.856$.

used Apple Pay at a location in their plan, and 87% used other payment methods at a location in their plan. Of those who wrote plans, 83.2% checked a box indicating "I strongly intend to try to use Apple Pay at these locations!" Of these participants, 89.9% visited a location in their plan, 30.3% used Apple Pay at a location in their plan, and 87.2% used other payment methods at a location in their plan.

In conclusion, although intention to set up and use Apple Pay was associated with actually doing so, many participants who expressed intentions did not follow through. This suggests nudges like implementation intentions may help participants follow through on their intentions. This also demonstrates the importance of measuring actual behavior in addition to intention when evaluating the effectiveness of nudging techniques.

When Did Participants Set Up Apple Pay?

As shown in Figure 6, 35% of participants had set up Apple Pay before Survey #2. In Survey #2, we encouraged the participants in our treatment groups to set up Apple Pay, but only 2.9% reported setting it up during Survey #2. However, an additional 10.5% reported setting up Apple Pay when we asked again in Survey #3. Overall, about half of participants had Apple Pay set up by the end of our study.

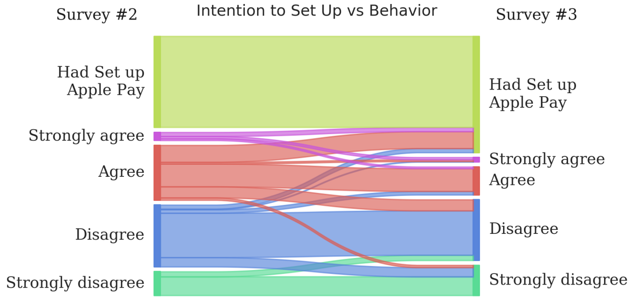


Figure 4: In both Survey #2 and Survey #3, we asked participants whether they had registered a card in Apple Pay. Those who had not were asked to rate their level of disagreement or agreement with the statement: "I intend to register a credit or debit card in Apple Pay in the next week."

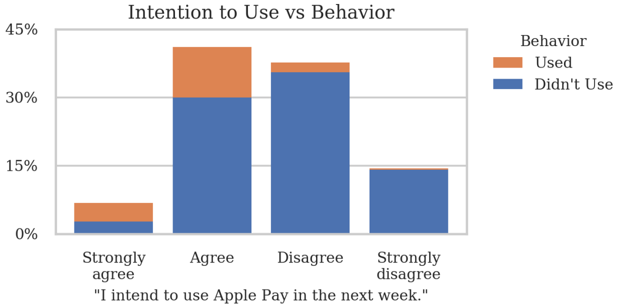


Figure 5: In Survey #2 we asked participants to rate their intention to use Apple Pay in the week ahead. We compared those responses to whether participants reported using Apple Pay in Survey #3.

Note that most of the participants who set up Apple Pay during our study did so after completing Survey #2. The same pattern held in our qualitative interviews (§ 3.3). This suggests the importance of an experimental design like ours, in which information is given to participants, but participants are allowed time to think about that information and potentially conduct additional research before taking action.

Factors Associated with Use of Apple Pay

Having found that our treatments were associated with participants using Apple Pay, we trained three logistic regression models to identify additional factors associated with using Apple Pay.

First, we trained a model on all participants who completed all three of our surveys ($n = 411$). Our model contains the

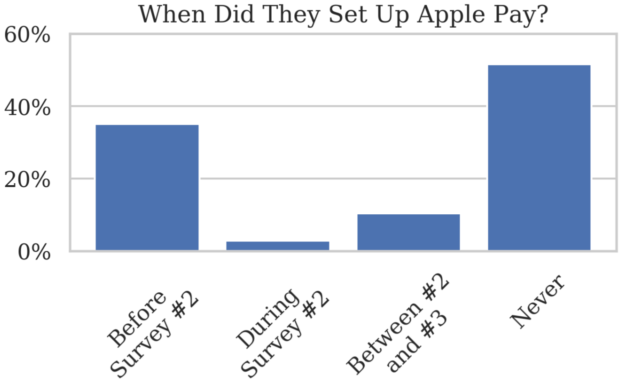


Figure 6: Participants could choose to set up Apple Pay at any point in our study, or not at all. More participants set up Apple Pay after Survey #2 than during Survey #2, suggesting the importance of giving participants time to think about the information we gave them.

following 17 variables: treatment condition, security attitudes (SA-6) [15], age, Computer Science (CS) background, prior experience with card fraud, phone biometric (Face ID or Touch ID), gender, expressed intention to use Apple Pay, whether the participant knew anyone who used Apple Pay, whether the participant owned an Apple Watch, whether the participant had used Apple Pay before the study, and the participants' perceptions of response efficacy, self-efficacy, threat severity, threat susceptibility, self-consciousness, and Apple Pay's usefulness. Our model is shown in Table 6 in the appendix. The model suggests that those with a computer science background and those who have experienced card fraud before are less likely to use Apple Pay (0.24x and 0.45x as likely, respectively). Perhaps those with a computer science background generally know more about Apple Pay, making those eligible for our experiment more likely to have consciously decided not to use it in advance of our interventions. This possibility is supported by Survey #1 from the qualitative interviews showing a positive association between having a CS background and having previously used Pay. The model also suggests that those whose phones are compatible with Face ID (2.1x), those who are non-female (2.4x), those who have used Apple Pay before (3.7x), and those who express an intention to use Apple Pay (6.1x) are more likely to use it.

Next, we trained a model on only the participants in the PMT+II group ($n = 136$). Our model contains the same variables as our first model, with the removal of treatment and the addition of these variables: whether the participant checked the box indicating that they strongly intended to follow their plan, whether the participant requested they be sent information about Apple Pay, whether the participant requested they be sent their plan, and whether the participant visited at least one location in their plan. Our model is shown in Table 7 in the appendix. Like our first model, this model suggests that those who experienced card fraud before are less likely to use Apple Pay (0.22x), and that those who used Apple Pay before are more likely to use it again (4.0x). Perhaps counterintuitively, the model also suggests that those who express self-consciousness about using Apple Pay in public are *more likely* to use it (5.1x). It is possible that participants' increased self-consciousness was due to their greater engagement with the plan, which could have made them more likely to use Apple Pay. There is also some evidence that whether the participant visited a location in their plan was associated with using Apple Pay (30x, $p = 0.058$).

Variable	**β**	e^{β}	**p-value**
age	-0.002	0.998	0.813
Face_ID	0.365	1.441	0.080
own_watch	1.035	2.815	**<0.001**
Intercept	-1.539	0.215	**<0.001**

Table 3: The variables in our regression model for predicting use of Apple Pay in the week prior to Survey #1 ($n = 590$). e^{β} indicates the change in odds of using Apple Pay for a one unit change in the variable (or when the variable is true). p-values significant at $\alpha = 0.05$ are bolded. Cox & Snell $R^2 = 0.051$.

Finally, we trained a model on the data we collected in Survey #1 to identify factors associated with people having used Apple Pay in the week before our study. We eliminated participants whose phones were incompatible with Apple Pay and who failed our attention check, leaving us with 590 participants. Due to the limited number of questions we asked participants in Survey #1, our model only contains age, phone compatibility with either Face ID or Touch ID, and Apple Watch ownership. The variables in our model are shown in Table 3. Overall, 23.7% of participants reported using Apple Pay in the past week. Our model shows a strong association between owning an Apple Watch and using Apple Pay, with Apple Watch owners being more than 2.8x more likely to use Apple Pay than non-owners. It is difficult to know the reason for this association, but one possible explanation might be that it's easier to use Apple Pay with an Apple Watch.

4.5 Limitations

One limitation of our study is our reliance on self-reported data. In particular, it is possible that participants did not accurately report whether they used Apple Pay between taking Survey #2 and #3. To encourage honesty, at the beginning of Survey #2 and Survey #3 we included text which encouraged participants to answer honestly and reassured them that there were no right or wrong answers. We also included attention checks in all our surveys. Fifteen participants (2%) failed our Survey #1 attention check and so were not invited to the subsequent surveys, but no participants failed our Survey #2 or Survey #3 attention checks. Another threat to validity is the possibility that some participants may have thought that setting up or using Apple Pay was not optional. To avoid that misconception, we included text assuring participants that setting up or using Apple Pay was not required and would have no effect on their compensation. One threat to the generalizability of our findings is the fact that crowd workers have been shown to differ from the general population. Our use of Prolific was informed by recent findings that Prolific workers are more diverse and honest than Mechanical Turk workers [49]. See Table 5 in the appendix for a summary of demographic information about our participants.

5 Discussion and Future Work

Our results have implications for both practitioners and researchers. First, banks, card issuers, and mobile payment operators could use our nudges to increase use of mobile payments instead of less secure, physical card payments. More widespread adoption of secure mobile payments has the potential to reduce card fraud, saving companies and customers both time and money. Second, our findings advance the field of nudging research. Our PMT and implementation intention nudges corrected participants' misconceptions and increased intention to and actual use of mobile payments. In particular, we believe our PMT-inspired description of Apple Pay's security (Figure 10) was instrumental in correcting participants' misconception that mobile payments are less secure than physical card payments. Our implementation intention nudge was designed to help participants remember to use mobile payments when they visited certain locations. Although we did not find sufficient evidence to conclude that our implementation intention nudge increased *use of Apple Pay* compared to the PMT nudge (Table 1), we did find strong evidence that it increased *intention to use Apple Pay* (Figure 2). This discrepancy is due to the fact that many participants who expressed an intention to use Apple Pay did not actually use it (Figure 5). This shows the importance of an experimental design which measures both intention to use and actual behavior, as we did in our study. Our results also show the need for additional research into techniques that may help people translate their intentions to act in a secure manner into actual behavior.

Our study suggests several possible areas for future work. First, it would be useful to compare our PMT and implementation intention nudges in an experiment with a larger sample size. This would allow us to conclusively determine whether implementation intentions yield improvements over PMT alone. Second, testing variations of PMT and implementation intention nudges could yield insight into what exactly makes these nudges effective. Knowing the most essential elements of these nudges could help translate them into a form suitable for large-scale messaging campaigns. Relatedly, people's receptivity to such messaging campaigns may depend on the entities conducting the campaigns, making a study of such messenger effects worthwhile. Third, PMT and implementation intentions should be tested for their potential to increase adoption of other secure technologies and for encouraging adherence to security best practices.

6 Conclusions

Despite the security benefits they offer, adoption of mobile payments in the United States remains low, at least in part due to the belief that mobile payments are less secure than payments with physical cards [22, 50]. Our nudges addressed this misconception and increased adoption of mobile payments: participants in our PMT and PMT with implementation intention treatment groups were 2.4x and 3.9x more likely, respectively, to use Apple Pay than those in our control group. Our qualitative interviews suggested additional factors which may limit adoption of mobile payments, including lack of availability and usability challenges.

Our findings show that it is possible to increase real-world adoption of security-enhancing technologies using carefully crafted informational interventions. At the same time, many people who express an intention to adopt such technologies may fail to do so. This suggests the need for further research into interventions which can help people translate intention into action. Implementation intentions are designed to do this. In our study, we found only weak evidence of a small improvement (1.67x) from adding implementation intentions to our PMT intervention. However, implementation intentions might become more helpful as mobile payments become more available and other barriers to adoption are removed. Clearly, there is no single solution for increasing adoption of security-enhancing technologies, but PMT and implementation intention nudges are two tools that may help.

7 Preregistration and Materials

We preregistered our controlled experiment on the Open Science Framework [64]. After preregistering but before collecting any data, we made two small edits to the survey text. Also, before collecting any Survey #3 data, we added a "using another payment method" option to Q18, Q19, and Q20 in Survey #3. In our preregistration, we described using a Bonferroni correction, but switched to the Holm-Bonferroni method as it controls the experiment's Type I error rate at the same level as a Bonferroni correction, while having a lower Type II error rate [1, 73]. Otherwise, we conducted our study as preregistered. To view the final version of all study materials, see our study page [65].

Acknowledgments

We thank Yuanyuan Feng, Hana Habib, Linda Moreci, Yaxing Yao, and Yixin Zou for their assistance with our work. This research was supported in part by grants from the National Science Foundation's Secure and Trustworthy Computing program (CNS-1330596, SES-1513957, CNS-1801316). The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF or the U.S. Government.

References

[1] Hervé Abdi. Holm's Sequential Bonferroni Procedure. *Encyclopedia of research design*, pages 1–8, 2010.

[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, January 2015.

[3] Alessandro Acquisti and Jens Grossklags. Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy*, 3(1):26–33, 2005.

[4] Alessandro Acquisti, Manya Sleeper, Yang Wang, Shomir Wilson, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, and Florian Schaub. Nudges for Privacy and Security. *ACM Computing Surveys*, 50(3):1–41, August 2017.

[5] Elham Al Qahtani, Mohamed Shehab, and Abrar Aljohani. The Effectiveness of Fear Appeals in Increasing Smartphone Locking Behavior among Saudi Arabians. *SOUPS @ USENIX Security Symposium*, 2018.

[6] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. "...better to use a lock screen than to worry about saving a few seconds of time" - Effect of Fear Appeal in the Context of Smartphone Locking Behavior. *Symposium on Usable Privacy and Security*, 2017.

[7] Hazim Almuhimedi. Helping Smartphone Users Manage their Privacy through Nudges. Technical Report CMU-ISR-17-111, December 2017.

[8] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015.

[9] Apple. Apple Pay coming to Target, Taco Bell and more top US retail locations, Jan 2019. https://www.apple.com/newsroom/2019/01/apple-pay-coming-to-target-taco-bell-and-more-top-us-retail-locations.

[10] Apple. Apple Pay security and privacy overview, Oct 2019. https://support.apple.com/en-us/HT203027.

[11] Richard A Armstrong. When to use the Bonferroni correction. *Ophthalmic and Physiological Optics*, 34(5):502–508, April 2014.

[12] Pamela Briggs, Debbie Jeske, and Lynne Coventry. Behavior change interventions for cybersecurity. In *Behavior Change Research and Theory*, pages 115–136. Elsevier, 2017.

[13] Kevin Cash. Credit card vs. debit card: Which is safer online?, Sep 2015. https://www.nerdwallet.com/blog/credit-cards/credit-card-vs-debit-card-safer-online-purchases/.

[14] Michael Fagan and Mohammad Maifi Hasan Khan. Why Do They Do What They Do? - A Study of What Motivates Users to (Not) Follow Computer Security Advice. *Symposium on Usable Privacy and Security*, 2016.

[15] Cori Faklaris, Laura A Dabbish, and Jason I Hong. A Self-Report Measure of End-User Security Attitudes (SA-6). *SOUPS @ USENIX Security Symposium*, 2019.

[16] Franz Faul, Edgar Erdfelder, Albert-Georg Lang, and Axel Buchner. G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39(2):175–191, May 2007.

[17] Alisa Frik, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. A Promise Is A Promise. In *the 2019 CHI Conference*, pages 1–12, New York, New York, USA, 2019. ACM Press.

[18] Vindu Goel and Rachel Abrams. Card Data Stolen From 5 Million Saks and Lord & Taylor Customers, Apr 2018. https://www.nytimes.com/2018/04/01/technology/saks-lord-taylor-credit-cards.html.

[19] Peter M Gollwitzer. Implementation intentions: strong effects of simple plans. *American Psychologist*, 54(7), 1999.

[20] Google. Google Pay may be preinstalled on your phone, May 2020. https://support.google.com/pay/answer/7644010.

[21] Google. How payments work, Jan 2020. https://support.google.com/pay/merchants/answer/6345242?hl=en.

[22] Jun Ho Huh, Saurabh Verma, Swathi Sri V Rayala, Rakesh B Bobba, Konstantin Beznosov, and Hyoungshick Kim. I Don't Use Apple Pay because it's less secure...: perception of security and usability in mobile tap-and-pay. *Proceedings of the Workshop on Usable Security*, 2017.

[23] Joseph Keller. How to stop Apple Pay from pestering you into signing up, Apr 2018. https://www.imore.com/how-stop-apple-pay-pestering-you.

[24] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. Standardizing privacy notices - an online study of the nutrition label approach. *CHI*, page 1573, 2010.

[25] Brian Krebs. Chip Card ATM 'Shimmer' Found in Mexico, Aug 2015. https://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/.

[26] Brian Krebs. All About Skimmers, Jun 2016. https://krebsonsecurity.com/all-about-skimmers/.

[27] Brian Krebs. Comment on Credit Card Breach at Buckle Stores, Jun 2017. https://krebsonsecurity.com/2017/06/credit-card-breach-at-buckle-stores/#comment-433940.

[28] Brian Krebs. Data: E-Retail Hacks More Lucrative Than Ever, Apr 2019. https://krebsonsecurity.com/2019/04/data-e-retail-hacks-more-lucrative-than-ever/.

[29] Brian Krebs. Sale of 4 Million Stolen Cards Tied to Breaches at 4 Restaurant Chains, Nov 2019. https://krebsonsecurity.com/2019/11/sale-of-4-million-stolen-cards-tied-to-breaches-at-4-restaurant-chains/.

[30] Brian Krebs. Wawa Breach May Have Compromised More Than 30 Million Payment Cards, Jan 2020. https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards/.

[31] Linda Lee, David Fifield, Nathan Malkin, Ganesh Iyer, Serge Egelman, and David Wagner. A Usability Evaluation of Tor Launcher. *Proceedings on Privacy Enhancing Technologies*, 2017(3):257–20, June 2017.

[32] Howard Leventhal, Robert Singer, and Susan Jones. Effects of fear and specificity of recommendation upon attitudes and behavior. *American Psychologist*, 2(1):20–29, 1965.

[33] Gen-Yih Liao and Chia-Min Wang. Exploring the Influences of Implementation Intention on Information Security Behaviors. *AMCIS*, 2011.

[34] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Zhang, Norman Sadeh, Alessandro Acquisti, and Yuvraj Agarwal. Follow My Recommendations - A Personalized Privacy Assistant for Mobile App Permissions. *Symposium on Usable Privacy and Security*, 2016.

[35] Ben Luthi. Is Apple Pay Safe?, Apr 2019. https://creditcards.usnews.com/articles/is-apple-pay-safe.

[36] Mary Madden and L Rainie. Americans' attitudes about privacy, security and surveillance. Pew Research Center, May 2015.

[37] James E Maddux and Ronald W Rogers. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, 19(5):469–479, 1983.

[38] Salvatore S. Mangiafico. Kruskal–wallis test, Feb 2020. https://rcompanion.org/handbook/F_08.html.

[39] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM Human-Computer Interaction*, pages 1–23, August 2019.

[40] Katherine L Milkman, John Beshears, James J Choi, David Laibson, and Brigitte C Madrian. Using implementation intentions prompts to enhance influenza vaccination rates. *Proceedings of the National Academy of Sciences*, 108(26), 2011.

[41] Katherine L Milkman, John Beshears, James J Choi, David Laibson, and Brigitte C Madrian. Planning prompts as a means of increasing preventive screening rates. *Preventive Medicine*, 56(1):92–93, January 2013.

[42] Sarah Milne, Sheina Orbell, and Paschal Sheeran. Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, 7(2):163–184, May 2002.

[43] Sarah Milne, Paschal Sheeran, and Sheina Orbell. Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, 30(1):106–143, January 2000.

[44] David W Nickerson and Todd Rogers. Do You Have a Voting Plan? *Psychological Science*, 21(2):194–199, January 2010.

[45] Patricia A Norberg, Daniel R Horne, and David A Horne. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41(1):100–126, June 2007.

[46] Sheina Orbell, Sarah Hodgkins, and Paschal Sheeran. Implementation intentions and the theory of planned behavior. *Personality and Social Psychology Review*, 23(9):945–954, 1997.

[47] Sheina Orbell and Paschal Sheeran. Motivational and Volitional Processes in Action Initiation: A Field Study of the Role of Implementation Intentions1. *Journal of Applied Social Psychology*, 30(4):780–797, 2000.

[48] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's Go in for a Closer Look. In *the 2017 ACM SIGSAC Conference*, pages 295–310, New York, New York, USA, 2017. ACM Press.

[49] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 70(C):153–163, May 2017.

[50] Pew. Are Americans Embracing Mobile Payments? pages 1–22, October 2019.

[51] PYMNTS.com. Apple Pay Adoption Stats, Jan 2020. https://www.pymnts.com/apple-pay-adoption/.

[52] Steve Ragan. What you need to know about the Home Depot data breach, Sep 2014. https://www.csoonline.com/article/2604320/what-you-need-to-know-about-the-home-depot-data-breach.html.

[53] Lee Rainie. Americans' complicated feelings about social media in an era of privacy concerns. *Pew Research Center*, March 2018.

[54] Ronald W Rogers. A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, 91(1):93–114, 1975.

[55] Ronald W Rogers and Steven Prentice-Dunn. Protection motivation theory. 1997.

[56] Todd Rogers, Katherine L Milkman, Leslie K John, and Michael I Norton. Beyond good intentions: Prompting people to make plans improves follow-through on important tasks. *Behavioral Science & Policy*, 1(2):33–41, 2015.

[57] Kate Rooney. Mobile payments have barely caught on in the US, despite the rise of smartphones, Aug 2019. https://www.cnbc.com/2019/08/29/why-mobile-payments-have-barely-caught-on-in-the-us.html.

[58] Samsung. How secure is Samsung Pay?, Jan 2020. https://www.samsung.com/us/support/answer/ANS00043932/.

[59] Samsung. Set up Samsung Pay on your phone, May 2020. https://www.samsung.com/us/support/answer/ANS00045081/.

[60] Ruth Shillair, Shelia R Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, and Nora J Rifon. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48(C):199–207, July 2015.

[61] Mikko Siponen, M Adam Mahmood, and Seppo Pahnila. Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2):217–224, March 2014.

[62] Teodor Sommestad, Henrik Karlzén, and Jonas Hallberg. A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behavior. *Dewald Roode Information Security Research Workshop*, pages 1–32, May 2014.

[63] Birgit Steller. *Vorsätze und die Wahrnehmung günstiger Gelegenheiten [Implementation intentions and the detection of good opportunities to act]*. tuduv-Verlag-Ges., 1992.

[64] Peter Story and Daniel Smullen. Apple services study: Preregistration, Dec 2019. https://osf.io/k3nrd.

[65] Peter Story and Daniel Smullen. Apple services study: Study page, Dec 2019. https://osf.io/srwyk.

[66] Gail M Sullivan and Richard Feinn. Using Effect Size—or Why the PValue Is Not Enough. *Journal of Graduate Medical Education*, 4(3):279–282, September 2012.

[67] Richard H Thaler and Cass R Sunstein. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. J. Wiley and Sons, 2008.

[68] Maciej Tomczak and Ewa Tomczak. The need to report effect size estimates revisited. An overview of some recommended measures of effect size. pages 1–7, July 2014.

[69] Jordi van den Breekel, Diego A Ortiz-Yepes, Erik Poll, and Joeri de Ruiter. EMV in a nutshell. Technical report, June 2016.

[70] Gregory Wallace. Target credit card hack: What you need to know, Dec 2013. https://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/index.html.

[71] Rick Wash and Emilee J Rader. Influencing mental models of security - a research agenda. *NSPW*, page 57, 2011.

[72] Alma Whitten and J D Tygar. Why Johnny can't encrypt: a usability case study of PGP 5. *USENIX Security Symposium*, August 1999.

[73] Wikipedia. Holm–bonferroni method, Nov 2019. https://en.wikipedia.org/wiki/Holm-Bonferroni_method.

[74] Kim Witte and Mike Allen. A meta-analysis of fear appeals: Implications for effective public health campaigns. *Personality and Social Psychology Review*, 27(5):591–615, 2000.

8 Appendix

Table 4: Final Codebook With Code Frequencies

Code	Description	Interview #1 (n=20)	Interview #2 (n=10)	Survey #2 (n=20)	Survey #3 (n=10)	Overall (n=20)
accidental_activation	Accidentally activating Pay (e.g., by double-tapping the home button, proximity of NFC devices, etc.).	1	3	1	0	4
additional_research	Performing additional research about Pay (e.g., asking others for their opinion about it, doing Google searches, etc.).	5	3	1	0	7
curiosity_availability	Wondering which places will accept Pay.	10	0	0	0	10
curiosity_information_theft	Wondering how their card information was stolen or could be stolen, how fraud occurred, why a data breach occurred, etc.	9	1	0	0	9
curiosity_reviewing_transactions	Wondering whether they will still be able to review their past transactions if they start using Pay.	1	0	0	0	1
curiosity_technology	Wondering about specific technologies behind Pay (e.g., how NFC works, how the cryptography works, etc.), what cards can be added, how to activate it, how it works, its business model, etc.	16	4	3	1	16
experience_card_fraud	People's own (or others') experiences with card fraud. Any fraudulent purchase made to a card is card fraud.	19	1	0	0	19
experience_card_information_theft	People's own (or others') experiences with card info theft.	10	0	0	0	10
experience_card_theft	People's own (or others') experiences with their physical card being stolen.	5	0	0	0	5
experience_no_card_fraud	People having no experiences of their own (or others') to recount about card fraud.	1	0	0	0	1
experience_no_card_information_theft	People having no experiences of their own (or others') to recount about card info theft.	5	0	0	0	5
experience_other	Security-related experiences that don't fit into the other codes.	2	1	0	0	3
experience_unsure	People saying they are unsure whether their card information has been stolen or whether they have been the victim of fraud.	4	0	0	0	4

Continued on the next page

Code	Description	Interview #1 (n=20)	Interview #2 (n=10)	Survey #2 (n=20)	Survey #3 (n=10)	Overall (n=20)
implementation_intention_ clarified_understanding	Forming the implementation intention clarified the person's understanding of Pay (e.g., realizing it won't work at gas stations).	4	0	0	0	4
implementation_intention_ forgotten	The participant not being able to remember their plan.	0	4	0	0	4
implementation_intention_ helpful	Participants' reasons why the implementation intention would or did help them remember to set up or use Pay.	10	6	1	0	13
implementation_intention_ remembered	The participant remembering their plan.	0	8	1	0	8
implementation_intention_ unhelpful	Participants' reasons why the implementation intention would not help them remember to use Pay, why it is hard to form a plan, etc.	12	7	0	0	15
influenced_positive_self_report	The participant saying that the interview made them more likely to use or set up Pay.	10	1	0	0	10
misconception_affiliation	Thinking that we are working for or being funded by a company behind one of the technologies we're discussing (e.g., are you guys working for Google?).	4	0	0	0	4
misconception_always_resolved	Thinking that fraudulent purchases will always be resolved (e.g., they will always get their money back).	2	0	0	0	2
misconception_cost	Thinking or wondering if Pay costs something to use.	3	0	0	0	3
misconception_opening_app	Thinking that using Pay requires opening the Pay app by tapping on its icon.	1	0	0	0	1
misconception_other	Other misconceptions.	2	2	0	0	4
misconception_required	Thinking that using Pay or following the plan is a required part of the study.	1	0	0	0	1
misconception_rewards	Thinking that they won't get rewards, points, or cash back if they use Pay.	4	0	0	0	4
misconception_screen_scan	Thinking that Pay works by scanning the user's phone or watch screen, rather than by using NFC.	4	0	0	0	4
misconception_square_pos	Thinking that Pay only works at Square POSs, or that Pay is the software running on those Square POS iPads. It is not a misconception that Pay works at most Square POSs.	2	0	0	0	2

Continued on the next page

Code	Description	Interview #1 (n=20)	Interview #2 (n=10)	Survey #2 (n=20)	Survey #3 (n=10)	Overall (n=20)
mitigation_description_helpful	Participants' reasons why the description of Pay or the instructions for how to set up and use Pay are helpful to them.	6	2	1	0	6
protection_action_RFID_wallet	Using an RFID-blocking wallet to protect your card information.	1	0	0	0	1
protection_action_account_access	Protect access to your account (e.g., password, 2FA).	6	2	1	0	8
protection_action_avoid_disclosure	Avoid giving information to others, whether prompted or not; avoiding falling for phishing, etc.	5	0	0	0	5
protection_action_avoid_merchant	Avoid transactions at untrusted merchants, only use trusted merchants, etc.	4	0	0	0	4
protection_action_avoid_online	Avoid making purchases online, avoid putting card information online, etc.	3	0	0	0	3
protection_action_certification_logo	Looking for certification logos (e.g., Trustee, Verisign, McAfee), browser plugin indicators (e.g., Web of Trust), TLS certificates, or any other symbols that attest to security in some way.	4	0	0	0	4
protection_action_corporate_resolution	Reporting fraudulent purchases to the card issuer, getting a new card, etc.	19	0	0	0	19
protection_action_data_retention	Preventing a card from being saved on a website either in whole or in part (e.g., not allowing the CVC to be saved).	2	0	0	0	2
protection_action_law_enforcement	Reporting card fraud or theft to law enforcement.	1	0	0	0	1
protection_action_monitor_statements	Looking for unauthorized transactions on card statements.	8	0	0	0	8
protection_action_monitoring_service	Lifelock, credit monitoring, etc.	4	2	2	1	4
protection_action_network	Using a secure network connection (e.g., home Wi-Fi, a VPN when on public Wi-Fi, etc.), avoiding insecure networks, avoiding public computers, etc.	2	0	0	0	2
protection_action_other	Other actions people take to protect themselves from card info theft and fraud.	7	1	0	0	8
protection_action_physical_awareness	Looking for card skimmers, hiding PIN, putting things in a place so they won't be stolen, paying close attention to what a shopkeeper does, checking receipts, etc.	10	1	0	1	11

Continued on the next page

Code	Description	Interview #1 (n=20)	Interview #2 (n=10)	Survey #2 (n=20)	Survey #3 (n=10)	Overall (n=20)
protection_action_use_cash	Using cash.	6	0	0	0	6
protection_action_use_chip	Using the chip in their card (as opposed to the magnetic stripe).	1	0	0	0	1
protection_action_use_credit	Using a credit card, since getting refunded is easier, etc.	6	1	1	0	7
protection_action_use_debit	Using a debit card or using a debit card as a credit card.	1	0	0	0	1
protection_action_use_other_payment_service	Using PayPal, Venmo, or another payment service other than Pay.	2	1	1	1	4
protection_action_use_pay	Using Apple Pay, Google Pay, or Samsung Pay (coded only when brought up prior to us suggesting that they use Pay).	2	0	0	0	2
reasons_for_not_setting_up	People's reasons for not setting up Pay.	14	0	9	0	16
reasons_for_not_using	People's reasons why they don't want to or did not use Pay.	7	1	4	6	12
response_efficacy_security_convinced	Reasons why participants are convinced that Pay will protect them.	12	4	2	1	14
response_efficacy_security_unconvinced	Reasons why participants think Pay will not protect them.	8	2	1	0	8
response_efficacy_security_unsure	Reasons why participants are unsure whether Pay will protect them.	12	4	0	0	14
self_efficacy_negative_battery	Using Pay requires a charged phone.	1	0	0	0	1
self_efficacy_negative_learning	Using or setting up Pay requires practice, learning, or attention to detail.	7	1	1	0	7
self_efficacy_negative_limited_availability	Not all places accept Pay. It may be unclear whether a given place accepts it.	7	7	2	0	12
self_efficacy_negative_limited_card_compatibility	Not all cards can be added to Pay.	1	2	0	0	3
self_efficacy_negative_opportunities	Not going shopping, not having any money, etc., and so not having opportunities to use Pay.	4	4	5	3	11
self_efficacy_negative_other	Other challenges to using Pay, negative experiences using it, and things that make using it more difficult.	7	5	2	2	9
self_efficacy_negative_overspending	The convenience of Pay makes the participant more inclined to wastefully or accidentally spend money.	4	0	0	0	4

Continued on the next page

Code	Description	Interview #1 (n=20)	Interview #2 (n=10)	Survey #2 (n=20)	Survey #3 (n=10)	Overall (n=20)
self_efficacy_negative_payment_failure	Pay payments not going through or taking too long/timing out.	2	6	2	2	6
self_efficacy_negative_remembering	Difficulty remembering to use Pay.	5	3	2	1	9
self_efficacy_negative_setup	Difficulty or irritation setting up Pay.	9	2	6	0	14
self_efficacy_negative_time	It taking too long or a long time to use Pay.	1	4	1	2	6
self_efficacy_other	Other comments about Pay usability, that are neither positive nor negative.	2	2	0	0	4
self_efficacy_positive_easy_to_use	Fast, simple, convenient, etc. to make transactions.	14	6	4	1	15
self_efficacy_positive_extensive_availability	Many or enough places accept Pay.	4	1	0	0	4
self_efficacy_positive_initiative	People taking the initiative to determine whether Pay is accepted (e.g., asking if Pay is accepted, or attempting to use it if they're unsure). Not coded if people said they didn't take the initiative.	0	1	0	0	1
self_efficacy_positive_no_wallet	If you use Pay, you won't have to carry your wallet, carry your cards, or pull out your cards or wallet.	7	5	2	3	10
self_efficacy_positive_novelty	Using or setting up Pay due to curiosity, wanting to see if it works.	9	2	5	1	10
self_efficacy_positive_only_option	Being more likely to use or using Pay because it's an option if you forget another payment method, another payment method doesn't work, you don't have your cards with you, etc. Also includes making Pay more accessible than cards (e.g., by burying cards in your purse and leaving phone on top).	7	5	1	0	10
self_efficacy_positive_opportunities	Going shopping, etc., and so having opportunities to use Pay. Includes inferred opportunities (e.g., if someone says they used Pay, that implies they had opportunities).	15	10	5	3	18

Continued on the next page

Code	Description	Interview #1 (n=20)	Interview #2 (n=10)	Survey #2 (n=20)	Survey #3 (n=10)	Overall (n=20)
self_efficacy_positive_other	Other non-security perks to using Pay, positive experiences using it, good things about Pay, etc.	4	1	0	0	5
self_efficacy_positive_other_reminders	Other things reminding people to use Pay. Not including the setup instructions or implementation intention plan template we offer users. Not including it being the only option.	1	6	1	0	7
self_efficacy_positive_setup	Positive things said about the setup process (easy, etc.).	14	4	1	0	17
self_efficacy_practice	Wanting to practice (or actually practicing) using Pay in a low-pressure situation (e.g., a vending machine, a self-checkout, etc.).	0	1	1	0	2
threat_severity_card_type	The severity of fraud would depend on what type of card was affected by the fraud (e.g., fraud on credit vs debit card).	2	0	0	0	2
threat_severity_high_concern_gets_worse	When fraud or information theft occurs, this might be a precursor to something worse (e.g., a worse hack, more lost money, etc.).	10	0	0	0	10
threat_severity_high_concern_hassle	Resolving the situation would be time-consuming, stressful, irritating, etc.	10	0	0	0	10
threat_severity_high_concern_lost_money	Being concerned about losing money, either from purchases not being refunded, or not being refunded for overdraft or other fees.	6	0	0	0	6
threat_severity_high_concern_other	Other reasons why people perceive the severity to be higher.	7	0	0	0	7
threat_severity_high_concern_violation	People feel violated, helpless, angry, etc. when they suffer from card fraud or information theft.	3	0	0	0	3
threat_severity_low_concern_other	Other reasons why people perceive the severity to be lower.	2	0	0	0	2
threat_severity_low_concern_resolution	It would be possible to resolve the situation.	11	0	0	0	11
threat_severity_other	Other things that impact perceptions of threat severity.	1	0	0	0	1
threat_severity_purchase_size	The severity of fraud would depend on the size of the fraudulent purchase which was made.	6	0	0	0	6
threat_susceptibility_comparison	Participants comparing the relative likelihood of one type of card (information) theft/fraud to another type of event. For example, it being more likely for debit information to be stolen than credit information.	11	0	0	0	11

Continued on the next page

Code	Description	Interview #1 (n=20)	Interview #2 (n=10)	Survey #2 (n=20)	Survey #3 (n=10)	Overall (n=20)
threat_susceptibility_high_ likelihood	Reasons participants perceive the likelihood of encountering the threat to be higher.	12	0	0	0	12
threat_susceptibility_low_ likelihood	Reasons participants perceive the likelihood of encountering the threat to be lower or non-existent (e.g., it's never happened to me before, it's never going to happen, etc.).	9	0	0	0	9
threat_susceptibility_other	Other things that impact perceptions of threat susceptibility. Also includes participants expressing that they are unsure about their threat susceptibility.	2	0	0	0	2

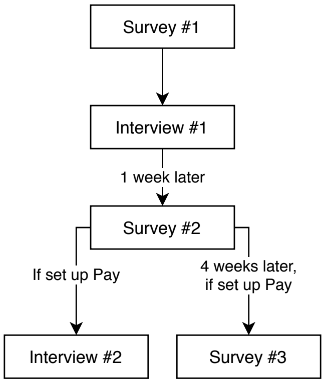


Figure 7: The process of administering surveys and interviews in the qualitative portion of our study (§ 3).

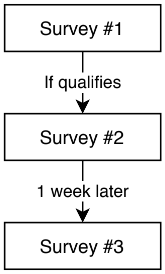


Figure 8: Our controlled experiment contained three online surveys (§ 4).

Demographic	**Values**	
Age	Minimum	18
	Median	32
	Mean	34.7
	Maximum	71
Gender	Female	58%
	Male	41%
	Other	1%
Employment	Working	74%
	Student	11%
	Not employed	10%
	Other	6%
Education	High school or less	18%
	College or associate	56%
	Graduate degree	18%
	Professional degree	4%
	Other	3%
Worked or Studied in a Computer-related Field	Yes	25%
	No	75%
Household Income	Median	$60,000 to $79,999

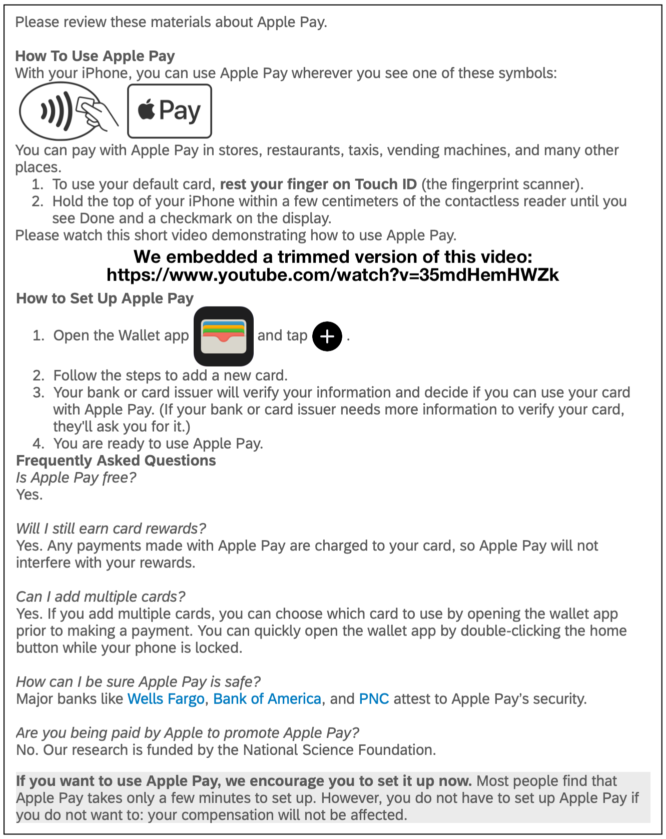
Table 5: Demographics for the 411 participants who completed all parts of our controlled experiment.

There have been many big hacks where credit and debit card information was stolen from retailers. For example, Target [70] was hacked in 2013, Home Depot [52] was hacked in 2014, and Saks Fifth Avenue [18] was hacked in 2018. Information about millions of cards was stolen in these hacks. If criminals get your credit or debit card information, they might use that information to make fraudulent purchases. If you notice fraudulent purchases on your credit card, you can probably get refunded. But if the purchases are made on your debit card, you might not be able to get your money back [13]. In any case, you would need to get a replacement card with a new number, which would be inconvenient.

Figure 9: In our experiment, participants in the PMT and PMT+II groups were shown this text to inform them about the threat of card fraud. This text was included in order to help participants develop accurate perceptions of threat susceptibility and threat severity, two elements of PMT [43].

Thankfully, there are steps you can take to prevent your card information from being stolen and to protect yourself from card fraud. One of the best things you can do is to start using Apple Pay. Instead of paying by swiping or inserting your card, you can make payments through your phone, which adds an extra layer of security. Payments made with Apple Pay will still be charged to your credit or debit card, but because the payments go through Apple Pay, your card number is not shown to or recorded by retailers [10]. This means that your card number cannot be stolen from transactions made with Apple Pay. If your phone is stolen, the thief will not be able to make payments because Apple Pay is protected by your fingerprint and lock screen PIN. Although no system is perfectly secure, security experts generally agree that Apple Pay is more secure than paying with credit or debit cards [35]. Apple Pay takes just a few minutes to set up, and is widely accepted. As of this year, Apple Pay is accepted in 65% of retail locations [9] in the United States. For example, ALDI grocery, CVS pharmacy, and Starbucks all accept Apple Pay.

Figure 10: In our experiment, participants in the PMT and PMT+II groups were shown this text to inform them about how using Apple Pay can protect them from card fraud. This text was included in order to help participants understand how Apple Pay may help protect them from card fraud and to give them confidence that they would have opportunities to use Apple Pay, influencing perceptions of response efficacy and self-efficacy, two additional elements of PMT [43].



Please review these materials about Apple Pay.

How To Use Apple Pay
With your iPhone, you can use Apple Pay wherever you see one of these symbols:

You can pay with Apple Pay in stores, restaurants, taxis, vending machines, and many other places.

1. To use your default card, **rest your finger on Touch ID** (the fingerprint scanner).
2. Hold the top of your iPhone within a few centimeters of the contactless reader until you see Done and a checkmark on the display.

Please watch this short video demonstrating how to use Apple Pay.

We embedded a trimmed version of this video:
https://www.youtube.com/watch?v=35mdHemHWZk

How to Set Up Apple Pay

1. Open the Wallet app and tap + .
2. Follow the steps to add a new card.
3. Your bank or card issuer will verify your information and decide if you can use your card with Apple Pay. (If your bank or card issuer needs more information to verify your card, they'll ask you for it.)
4. You are ready to use Apple Pay.

Frequently Asked Questions
Is Apple Pay free?
Yes.

Will I still earn card rewards?
Yes. Any payments made with Apple Pay are charged to your card, so Apple Pay will not interfere with your rewards.

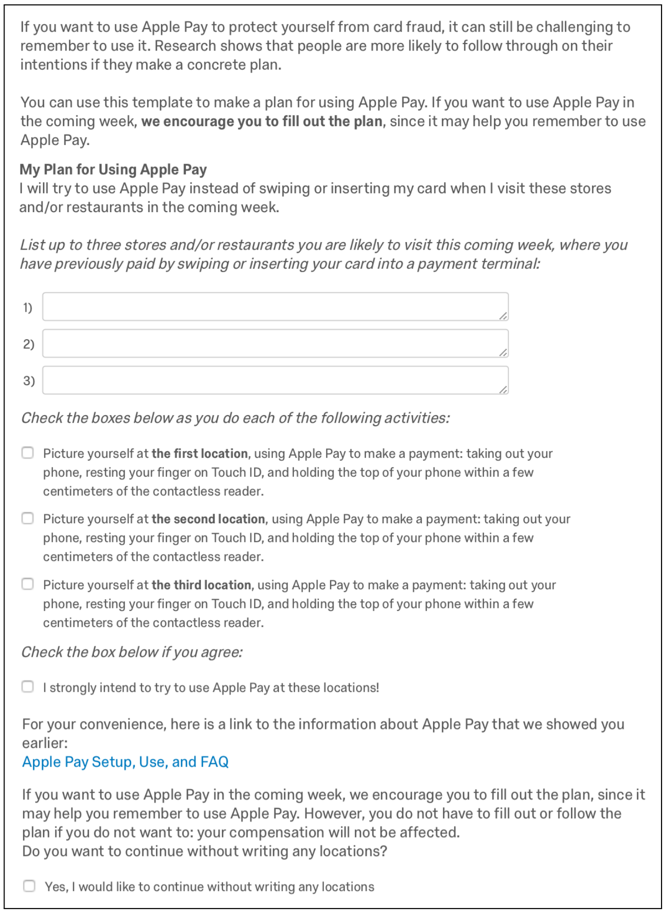
Can I add multiple cards?
Yes. If you add multiple cards, you can choose which card to use by opening the wallet app prior to making a payment. You can quickly open the wallet app by double-clicking the home button while your phone is locked.

How can I be sure Apple Pay is safe?
Major banks like Wells Fargo, Bank of America, and PNC attest to Apple Pay's security.

Are you being paid by Apple to promote Apple Pay?
No. Our research is funded by the National Science Foundation.

If you want to use Apple Pay, we encourage you to set it up now. Most people find that Apple Pay takes only a few minutes to set up. However, you do not have to set up Apple Pay if you do not want to: your compensation will not be affected.

Figure 11: In our experiment, participants in the PMT and PMT+II groups were shown these details about Apple Pay. The instructions contained information about either Touch ID or Face ID, based on which technology the participant's phone was compatible with. These instructions were designed to positively influence perceptions of self-efficacy.



If you want to use Apple Pay to protect yourself from card fraud, it can still be challenging to remember to use it. Research shows that people are more likely to follow through on their intentions if they make a concrete plan.

You can use this template to make a plan for using Apple Pay. If you want to use Apple Pay in the coming week, **we encourage you to fill out the plan**, since it may help you remember to use Apple Pay.

My Plan for Using Apple Pay
I will try to use Apple Pay instead of swiping or inserting my card when I visit these stores and/or restaurants in the coming week.

List up to three stores and/or restaurants you are likely to visit this coming week, where you have previously paid by swiping or inserting your card into a payment terminal:

1) ______
2) ______
3) ______

Check the boxes below as you do each of the following activities:

□ Picture yourself at **the first location**, using Apple Pay to make a payment: taking out your phone, resting your finger on Touch ID, and holding the top of your phone within a few centimeters of the contactless reader.

□ Picture yourself at **the second location**, using Apple Pay to make a payment: taking out your phone, resting your finger on Touch ID, and holding the top of your phone within a few centimeters of the contactless reader.

□ Picture yourself at **the third location**, using Apple Pay to make a payment: taking out your phone, resting your finger on Touch ID, and holding the top of your phone within a few centimeters of the contactless reader.

Check the box below if you agree:

□ I strongly intend to try to use Apple Pay at these locations!

For your convenience, here is a link to the information about Apple Pay that we showed you earlier:
Apple Pay Setup, Use, and FAQ

If you want to use Apple Pay in the coming week, we encourage you to fill out the plan, since it may help you remember to use Apple Pay. However, you do not have to fill out or follow the plan if you do not want to: your compensation will not be affected.
Do you want to continue without writing any locations?

□ Yes, I would like to continue without writing any locations

Figure 12: In our experiment, participants in the PMT+II group were shown this implementation intention template. The template encourages participants to plan where they might use Apple Pay in the coming week and to mentally rehearse using Apple Pay in these locations. These activities should help mentally activate participants' plans to use Apple Pay when they are in these locations [19]. Finally, participants are given the opportunity to strongly commit to their plan [19, 63].

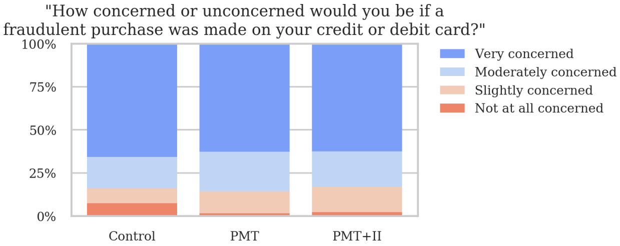


Figure 13: We did not find statistically significant evidence that our treatments affected perception of threat severity ($p = 0.932$).

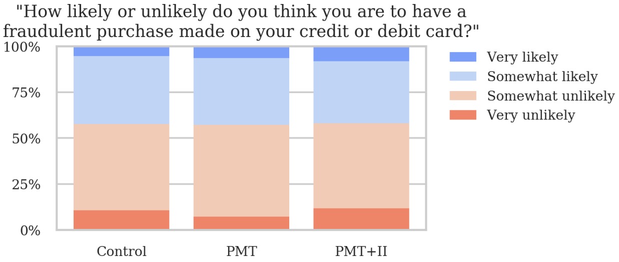


Figure 14: We did not find statistically significant evidence that our treatments affected perception of threat susceptibility ($p = 0.881$).

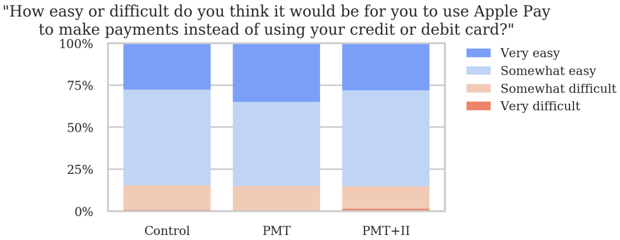


Figure 15: We did not find statistically significant evidence that our treatments affected perception of self-efficacy ($p = 0.523$).

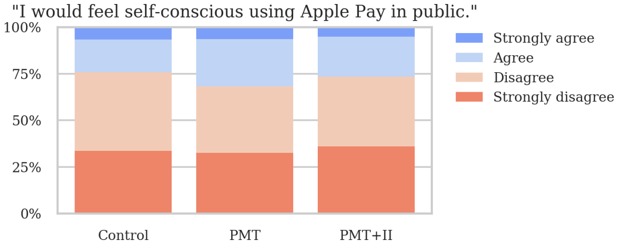


Figure 16: We did not find statistically significant evidence that our treatments affected self-consciousness ($p = 0.628$).

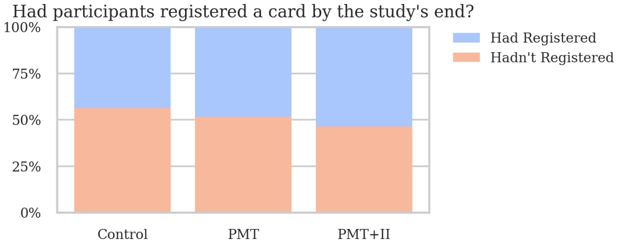


Figure 17: We did not find statistically significant evidence that our treatments affected whether participants would have a card registered in Apple Pay by the end of our study ($p = 0.237$).

Variable	**β**	**e^{β}**	**p-value**
CS_background	-1.438	0.237	**0.001**
experienced_fraud	-0.799	0.450	**0.024**
threat_severity	-0.353	0.703	0.414
knows_users	-0.041	0.960	0.911
age	0.010	1.010	0.527
SA6	0.042	1.043	0.259
response_efficacy	0.146	1.157	0.783
self_conscious	0.281	1.324	0.451
usefulness	0.368	1.445	0.509
self_efficacy	0.377	1.458	0.501
threat_susceptibility	0.383	1.466	0.296
own_watch	0.483	1.621	0.198
Face_ID	0.745	2.106	**0.022**
non-female_gender	0.870	2.387	**0.009**
prior_use	1.295	3.653	**<0.001**
intention	1.804	6.077	**<0.001**
treatment			0.297
PMT	0.390	1.477	0.394
PMT+II	0.698	2.010	0.123
Intercept	-4.856	0.008	**<0.001**

Table 6: Our logistic regression model for predicting use of Apple Pay by those who completed Survey #1, #2, and #3 ($n = 411$). e^{β} indicates the change in odds of using Apple Pay when the variable is true. p-values significant at $\alpha = 0.05$ are bolded. Cox & Snell $R^2 = 0.238$.

Variable	**β**	**e^{β}**	**p-value**
CS_background	-1.635	0.195	0.059
experienced_fraud	-1.519	0.219	**0.039**
response_efficacy	-1.326	0.266	0.245
messaged_info	-0.607	0.545	0.451
usefulness	-0.598	0.550	0.598
non-female_gender	-0.563	0.569	0.378
own_watch	-0.243	0.784	0.728
threat_severity	-0.118	0.889	0.904
SA6	-0.011	0.989	0.870
age	0.008	1.009	0.752
checked_intention	0.165	1.179	0.923
knows_users	0.463	1.589	0.461
Face_ID	0.902	2.464	0.207
messaged_plan	0.936	2.549	0.245
self_efficacy	1.032	2.805	0.267
prior_use	1.377	3.964	**0.028**
threat_susceptibility	1.458	4.297	0.058
self_conscious	1.639	5.148	**0.020**
visited_location	3.414	30.374	0.052
intention	20.768	1045582764.370	0.997
Intercept	-24.824	0.000	0.997

Table 7: Our logistic regression model for predicting whether those who received our implementation intention treatment used Apple Pay ($n = 136$). e^{β} indicates the change in odds of using Apple Pay when the variable is true. p-values significant at $\alpha = 0.05$ are bolded. Cox & Snell $R^2 = 0.385$.

8.1 Qualitative Interviews, Survey #1

Researchers at OMITTED are conducting a study to understand people's use of smartphones, credit cards, and debit cards to make payments.

All participants are asked to answer the screening questions below.

Based on your answers to the screening questions, we will determine your eligibility for our preliminary survey. If you are eligible, the preliminary survey will take about 10 minutes to complete. Only some of the participants who take this survey will be invited to participate in subsequent interviews and follow-up surveys. Participants will not be compensated for completing this survey: participants will only be compensated if they are selected to participate in subsequent parts of this study.

Do you live in the United States of America?
(Yes, No)

Do you speak English?
(Yes, No)

What is your age in years?
___

Are you able to visit OMITTED's campus for an interview?
(Yes, No)

Please review the details below:
[Consent Form]

Have you read and understood the information above?
(Yes, No)

Do you want to participate in this research and continue with the survey?
(Yes, No)

Do you use a smartphone?
(Yes, No, I don't know)

In which country did you purchase your smartphone?
(The United States, Other: ___, I don't know)

What kind of smartphone do you have? If you have multiple phones, answer based on the phone you use the most.
(iPhone, Samsung phone, Other Android phone, Other: ___, I don't know)

[Here we show the iPhone-specific text, but users saw text appropriate to the type of phone they selected.]
What **model of iPhone** do you have? For example, iPhone 4S, iPhone 5, etc. You can check your phone's model by opening the "Settings" app, going to "General", then "About". Your phone's "Model Name" should be listed on the "About" page.

______

What **version of iOS** is running on your phone? For example, 7.9, 10.3, etc. You can check your phone's iOS software version by opening the "Settings" app, going to "General", then "About". Your phone's "Software Version" should be listed on the "About" page.

______

Do you have an Apple Watch?
(Yes, No)

We would like to understand how you make payments at brick and mortar stores, restaurants, or other physical locations.

Do you have a **credit card**?
(Yes, No)

Do you have a **debit card**?
(Yes, No)

Please select **all options** which accurately complete the following statement: "**Sometime in the past**, I have made in-person payments in physical locations..."
... using cash
... using my credit card
... using my debit card
... using Apple Pay. Apple Pay allows you to make payments using your smartphone.
... using Google Pay. Google Pay allows you to make payments using your smartphone.
... using Samsung Pay. Samsung Pay allows you to make payments using your smartphone.

Please select **all options** which accurately complete the following statement: "**In the past month**, I have made in-person payments in physical locations..."
... using cash
... using my credit card
... using my debit card
... using Apple Pay. Apple Pay allows you to make payments using your smartphone.
... using Google Pay. Google Pay allows you to make payments using your smartphone.
... using Samsung Pay. Samsung Pay allows you to make payments using your smartphone.

Has your **credit or debit card information** ever been stolen?
(Yes, No, I don't know)

How **concerned or unconcerned** would you be if your credit or debit card information was stolen in the future?
(Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)

How **likely or unlikely** do you think you are to have your credit or debit card information stolen in the future?
(Very unlikely, Somewhat unlikely, Somewhat likely, Very likely)

Has a **fraudulent purchase** ever been made on your credit or debit card?
(Yes, No, I don't know)

How **concerned or unconcerned** would you be if a fraudulent purchase was made on your credit or debit card in the future?
(Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)

How **likely or unlikely** do you think you are to have a fraudulent purchase made on your credit or debit card in the future?
(Very unlikely, Somewhat unlikely, Somewhat likely, Very likely)

How did you find this study?
(OMITTED Participation Pool, Craigslist, Other: ___)

What gender do you identify with?
(Male, Female, Non-binary, Other: ___, Prefer not to answer)

What best describes your employment status?
(Working, paid employee; Working, self employed; Student; Not employed; Retired; Prefer not to answer)

Have you ever worked in or studied in a computer-related field? (Computer Science, IT support, etc.)
(Yes, No)

What is the highest level of school you have completed or degree you have earned?
(Less than high school, High school or equivalent, College or associate degree, Master's degree, Doctoral degree, Professional degree, Other: ___, Prefer not to answer)

Please estimate what your total household income will be for this year:
(Less than $10,000; $10,000 - $19,999; $20,000 - $39,999; $40,000 - $59,999; $60,000 - $79,999; $80,000 - $99,999; $100,000 or more; Prefer not to answer)

Have you ever lived outside the United States for more than 1 month?
(Yes, No, Prefer not to answer)

Where outside the United States have you lived the longest?

______

If you are eligible for participation in this study, we may email you with an invitation to participate in the study. Because we have a limited number of interview slots available, we may not be able to interview all eligible candidates.

Name:

______

Email address:

______

8.2 Qualitative Interviews, Interview #1 Script

Hello XXX, my name is YYY [and my assistant's name is ZZZ]. Thank you for agreeing to participate in Interview #1. [I will be asking most of the questions, and ZZZ will be taking notes.] [I am/We are] very interested in your thoughts about credit cards, debits cards, and smartphones. This interview will be recorded, but the audio will not be shared with the public. Your responses will be kept anonymous, but quotes from your responses may be shared with the public.

Prior to completing Survey #1, you expressed your consent to participate in this study. However, the interview is completely voluntary, and you are free to end it at any time. The interview will take up to an hour. Is it alright if I start the audio recording now?

Great! I will start the audio recording now.

Alright, let's get started! Remember that there are no right or wrong answers to any of my questions.

Could you explain how you typically pay when you make a purchase in a physical location, like a brick and mortar store or restaurant?

In the survey, you also indicated that you used [a credit card][a debit card][credit and debit cards] to make purchases.

If has credit and debit: Is there a reason why you use one card instead of another?

If fraudulent purchase: In the survey, you wrote that a fraudulent purchase had been made on your credit or debit card. What happened? [Was it your credit or debit card?] [What did you do?] [How do you think it happened?]

If no fraudulent purchase: In the survey, you wrote that a fraudulent purchase had not been made on your credit or debit card. Do you know anyone who has had a fraudulent purchase made on their credit or debit card? What happened?

If don't know: In the survey, you wrote that you weren't sure if a fraudulent purchase had been made on your credit or debit card. What did you mean by that? [What did you do?]

If card info was stolen: In the survey, you wrote that your credit or debit card information had been stolen before. What happened? [Was it your credit or debit card?] [What did you do?] [How do you think it happened?]

If card info wasn't stolen: In the survey, you wrote that your credit or debit card information had not been stolen before. Do you know anyone who has had their credit or debit card information stolen? What happened?

If don't know: In the survey, you wrote that you weren't sure if your credit or debit card information had been stolen. What did you mean by that? [What did you do?]

[I think most people carry their smartphones all the time, but this is a sanity check.]

What kind of smartphone do you use?

Do you carry your smartphone with you every day?

Are there any times when you do go out without your smartphone?

If Apple Watch: In the survey, you indicated that you have an Apple Watch. Do you wear it every day?

If they have an iPhone: [Pay] = [Apple Pay]

If they have a non-Samsung Android phone: [Pay] = [Google Pay]

If they have a Samsung phone:

If they previously used Google Pay and Samsung Pay:

In the survey, you said that you had previously used Google Pay and Samsung Pay, but haven't used either to pay in a physical location in the last month.

If you were going to use one of them again, which would you use? [Why?] [If you don't have a preference, that's okay, too.]

If they previously used Google Pay xor Samsung pay:

In the survey, you said that you had previously used [Google Pay][Samsung Pay], but haven't used it to pay in a physical location in the last month. Your phone is also compatible with [Samsung Pay][Google Pay], which can also be used to make payments through your phone.

If you were going to use Google Pay or Samsung Pay in the future, which would you use? [Why?] [If you don't have a preference, that's okay, too.]

If they haven't previously used Google Pay or Samsung pay:

In the survey, you indicated that you hadn't used either Google Pay or Samsung Pay to pay in a physical location before. Google Pay and Samsung Pay are both mobile payments systems that allow you to make payments in stores through your phone. Your phone is compatible with both Google Pay and Samsung Pay.

If you were going to start using one, which would you choose? [Why?] [If you don't know enough to choose, that's okay, too.]

If Samsung Pay: [Pay] = [Samsung Pay]

If Google Pay: [Pay] = [Google Pay]

Else: [Pay] = [Samsung Pay]

In that case, let's focus on [Pay] for the rest of the interview.

If they previously used [Pay], but haven't used it recently:

Omit if asked above: In the survey, you said that you had previously used [Pay], but haven't used it to pay in a physical location in the last month.

Tell me about your experiences using [Pay]. [When did you first use it? For how long did you use it? Was your experience using [Pay] good or bad?]

Is there a reason why you haven't used [Pay] recently?

If they have never used [Pay]:

Omit if asked above: In the survey, you indicated that you hadn't used [Pay] to pay in a physical location before. [Pay] is a mobile payments system that allows you to make payments in stores through your phone [Apple watch: or watch].

Had you heard of [Pay] before taking the survey?

If yes: How did you hear about [Pay]? Have you set it up on your phone [or watch]?

If yes: Have you tried using [Pay] before? Is there any reason why you haven't used it to make a payment before?

If no: Is there any reason why you haven't set it up?

There have been many big hacks where credit and debit card information was stolen from retailers. For example, Target was hacked in 2013, Home Depot was hacked in 2014, and Saks Fifth Avenue was hacked last year. Information about millions of cards was stolen in these hacks. If criminals get your credit or debit card information, they might use that information to make fraudulent purchases. If you notice fraudulent purchases on your credit card, you can probably get refunded. But if the purchases are made on your debit card, you might not be able to get your money back. In any case, you would need to get a replacement card with a new number, which would be inconvenient.

How concerned or unconcerned would you be if a fraudulent purchase was made on your credit or debit card [again]? Why?

[Concern Likert] On this scale, which option best reflects your answer?

How likely or unlikely do you think you are to have a fraudulent purchase made on your credit or debit card [again]? Why?

[Likelihood Likert] On this scale, which option best reflects your answer?

How concerned or unconcerned would you be if your credit or debit card information was stolen [again]? Why?
[Concern Likert] On this scale, which option best reflects your answer?

How likely or unlikely do you think you are to have your credit or debit card information stolen [again]? Why?
[Likelihood Likert] On this scale, which option best reflects your answer?

Do you know of anything you can do to prevent your credit or debit card information from being stolen? [Have you done anything to protect your card information?]

Thankfully, there are steps you can take to prevent your card information from being stolen and to protect yourself from card fraud. One of the best things you can do is to start using [Pay]. Instead of paying by swiping or inserting your card, you can make payments through your phone [or watch], which adds an extra layer of security. Payments made with [Pay] will still be charged to your credit or debit card, but because the payments go through [Pay], your card number is not shown to or recorded by retailers. This means that your card number cannot be stolen from transactions made with [Pay]. If your phone [or watch] is stolen, the thief will not be able to make payments because [Pay] is protected by your [Apple: fingerprint/Face ID and lock screen PIN][Other: lock screen]. Although no system is perfectly secure, security experts generally agree that [Pay] is more secure than paying with credit or debit cards. [Pay] takes just a few minutes to set up, and is widely accepted. Apple Pay: As of this year, Apple Pay is accepted in 65% of retail locations in the United States. For example, Giant Eagle, ALDI, Dunkin' Donuts, and CVS all accept Apple Pay. Google Pay: Google Pay is accepted at millions of locations. For example, Giant Eagle, ALDI, Dunkin' Donuts, and CVS all accept Google Pay. Samsung Pay: Samsung Pay is accepted at most retail locations in the United States.

These instructions show you how to set up [Pay] on your phone and how to make payments in stores.

If Apple Watch: Since you wear an Apple Watch, you might also be interested in the instructions for using Apple Pay on your watch. Using your watch might be more convenient than using your phone, and it's just as secure.

Please take a minute to review the instructions. If you want to set up [Pay], feel free to try it right now. If you run into any trouble, I would be happy to help you set it up. However, you do not have to set up [Pay] if you do not want to.

[Pass the handout to the participant]

[If they make a phone call: pause the recording to avoid recording their card number, SSN, or other sensitive information]

[Note whether they simply read the instructions, or tried to set up Pay. Ask if it's unclear.]

[Ask or observe what the participant had to do to verify their card (e.g., whether they had to call their bank, open the bank's app, etc.)]

[After pausing for at least 30 seconds, or however long it takes them to start setting up Pay]

[Remember to resume the recording, if it was paused]

After reviewing the instructions, do you have any questions about [Pay]?

If they simply reviewed the instructions:
How easy or difficult do you think it would be for you to set up [Pay]? Why?
[Difficulty Likert] On this scale, which option best reflects your answer?
Do you plan to try to set up [Pay] later, or would you rather not? Why?

If they tried to set up Pay:
Were you able to complete the setup of [Pay]?
If yes: How easy or difficult was it for you to set up [Pay]? Why?
[Difficulty Likert] On this scale, which option best reflects your answer?
If no: How easy or difficult was it for you try to set up [Pay]? Why?
[Difficulty Likert] On this scale, which option best reflects your answer?
Do you plan to try to set up [Pay] later, or would you rather not? Why?

How easy or difficult do you think it would be for you to use [Pay] to make payments instead of using your credit or debit card? Why?
[Difficulty Likert] On this scale, which option best reflects your answer?

[Agreement Likert] On this scale, please rate your level of disagreement or agreement with the following statement:
"If I were to start using [Pay], I would be less likely to have my card information stolen."
[And why do you choose that option?]

[Interest Likert] And on this scale, could you show me how interested or uninterested you are in using [Pay]? Why?

[Based on the person's stated level of interest and why they feel that way, I may skip the entire implementation intention section below.]

[To determine which handout to give the person. If they are ambivalent:
If they set up Apple Pay: handout corresponding to where they set it up
If they wear the Apple Watch all the time: watch handout
Else: iPhone handout]

Apple Watch: If you were going to start using Apple Pay, do you think you would be more likely to pay with your phone or with your watch? [Why?]

If you plan to use [Pay] in order to protect your credit or debit card information, one challenge might be simply remembering to use [Pay]. Forming a simple, concrete plan to use [Pay] can help you remember. If you like, you can use the plan template I have written on this handout.

[Hand the appropriate handout to the person]

Please take a minute to read through the plan. If you want to use [Pay] in the coming week, I encourage you to fill out the plan, since it may help you remember to use [Pay]. However, you do not have to fill out or follow the plan.

[Note the number of locations the person wrote and which boxes they checked]
[Number of locations written: ___]
[Number of boxes checked: ___ / 3]
[Final box checked? ___]

You are welcome to keep the plan and the instructions for using [Pay].

Do you want to use [Pay] in the coming week?

If they did not fill out the plan:
Is there a reason why you didn't fill out the plan?

If they did fill out the plan:
In the coming week, how likely or unlikely are you to visit at least one of the locations you listed? Why?
[Likelihood Likert] On this scale, which option best reflects your answer?

How likely or unlikely are you to try to use [Pay] at these locations? Why?
[Likelihood Likert] On this scale, which option best reflects your answer?

Do you think this plan will or will not help you remember to use [Pay]? Why?

Before we conclude the interview, do you have any other thoughts or questions?

Thank you for participating in this interview! In about one week, I will send you a short follow-up survey. After you complete that survey, I will email you a $15 Amazon e-Gift Card.

8.3 Qualitative Interviews, Survey #2

This survey is Survey #2 in the study "Use of Smartphones, Credit Cards, and Debit Cards" that you previously gave your consent to participate in. It will take about 10 minutes to complete this survey. If you complete this survey, we will email you a $15 Amazon e-Gift Card for your participation in our study.

Please answer the following questions about your experiences since our interview. There are no right or wrong answers to any of these questions, so please answer honestly.

You did not set up $PAY during our interview. Did you set up $PAY after the interview?
(Yes, No)

Please write a few sentences explaining why you [set up][did not set up] $PAY.

When did you set up $PAY?
(Today, Yesterday, A few days ago, Right after the interview)

Since our interview, have you **tried to use** $PAY to make a payment in a physical location?
(Yes, No)

Please write a few sentences explaining why you [tried][did not try] to use $PAY.

———

Since our interview, have you **successfully used** $PAY to make a payment in a physical location?
(Yes, No)

Please write a few sentences describing your experience [using][trying to use] $PAY.

Since our interview, have you done anything else to protect your credit or debit card information from being stolen, or to protect yourself from credit or debit card fraud?
(Yes, No)

Please write a few sentences explaining what other steps you have taken to protect yourself from card information theft or card fraud.

———

Are you interested in meeting for an additional 30 minute interview? If you participate in this interview, you will be compensated with an additional $15 Amazon e-Gift Card.
(Yes, No)

8.4 Qualitative Interviews, Interview #2 Script

Hello XXX, my name is YYY and my assistant's name is ZZZ. Thank you for coming to Interview #2. This interview is focused on your experiences since Interview #1. I will be asking most of the questions, and ZZZ will be taking notes. This interview will be recorded, but the audio will not be shared with the public. Your responses will be kept anonymous, but quotes from your responses may be shared with the public.

Prior to completing Survey #1, you expressed your consent to participate in this study. However, the interview is completely voluntary, and you are free to end it at any time. The interview will take roughly 30 minutes. Is it alright if I start the audio recording now?

Great! I will start the audio recording now.

Alright, let's get started! Remember that there are no right or wrong answers to any of my questions.

In interview #1, we discussed [Pay].

If setup after Interview #1: During our last interview, you did not [setup][complete the setup of] [Pay].

When did you set up [Pay]? What reminded you to set up [Pay]?

What did you have to do to set up [Pay]? [Did you have to call your bank?]

Did you try to use [Pay] since our last interview?

If yes:

These instructions show how to review the transactions you made with [Pay]. Please take a minute to review the transactions you made since our interview. [Hands handout]

What were your experiences trying to use [Pay]?

Where did using [Pay] work the best? What happened?

Where was using [Pay] the most difficult? What happened?

Are there any other experiences you'd like to share?

If no:

Did you have any opportunities to use [Pay]?

Did you visit any stores, restaurants, or other locations where you thought Pay might be accepted?

Why did you not end up using [Pay]?

Did you use [Pay] [if yes: more or] less than you thought you would?

Did anything about [Pay] surprise you?

Did you encounter any challenges trying to use [Pay]?

Do you plan to use [Pay] in the future? Why?

What is your overall impression of [Pay]?

During our last interview, we discussed making a concrete plan to help you remember to use [Pay].

If filled out in interview: You filled out the plan template during our last interview. Do you remember what the plan was?

If not filled out in interview: You did not fill out the plan template during our last interview. Did you fill out the plan after the interview? Do you remember what the plan was?

If filled out at some point: Part of the plan was listing three stores or restaurants you thought you might visit. Do you remember what stores or restaurants you listed?

If yes: Did you visit any of those locations? Did you try to use [Pay] there? Did you try to use [Pay] at any other locations?

Did you find the plan to be helpful or not helpful? [Did the plan help you remember to use [Pay]?] [Was the plan more or less helpful than you thought it would be?] [Do you think you would have remembered to use Pay if you hadn't made the plan? Why?] [Can you think of any other strategies to help you remember to use Pay?]

Did you do anything else to help you remember to use [Pay]?

Potentially ask for clarification about free-text responses to survey.

Before we conclude the interview, do you have any other thoughts or questions?

Thank you for participating in this interview! In the next couple days, I will email you a $15 Amazon e-Gift Card.

8.5 Qualitative Interviews, Survey #3

This survey is Survey #3 in the study "Use of Smartphones, Credit Cards, and Debit Cards" that you previously gave your consent to participate in. It will take about 10 minutes to complete this survey. If you complete this survey, we will email you a $5 Amazon e-Gift Card.

Please answer the following questions about your experiences in the past week. There are no right or wrong answers to any of these questions, so please answer honestly.

In the past week, did you **try to use** $PAY to make a payment in a physical location?
(Yes, No)

Please write a few sentences explaining why you [tried][did not try] to use $PAY.

______

In the past week, did you **successfully use** $PAY to make a payment in a physical location?
(Yes, No)

Please write a few sentences describing your experience [using][trying to use] $PAY.

______

How likely or unlikely are you to use $PAY in the future?
(Very unlikely, Somewhat unlikely, Somewhat likely, Very likely)

In the past week, have you done anything else to protect your credit or debit card information from being stolen, or to

protect yourself from credit or debit card fraud?
(Yes, No)

Please write a few sentences explaining what other steps you have taken to protect yourself from card information theft or card fraud. ______

8.6 Controlled Experiment, Survey #1

Researchers at OMITTED are conducting a study to understand people's use of Apple services.

All participants are asked to answer the screening questions below.

Based on your answers to the screening questions, we will determine your eligibility for our Survey #1. If you are eligible, Survey #1 will take about 5 minutes to complete. Only some of the participants who take Survey #1 will be invited to participate in two follow-up surveys (Surveys #2 and #3).

In what country do you currently reside?
(United States, Other country)

What operating system (OS) does your primary mobile phone have?
(iOS (iPhone), Other, I don't know)

Do you speak English?
(Yes, No)

What is your age in years?

___

Based on your answers to our screening questions, we have determined that you are eligible for Survey #1.

Please review the details below:
[Consent Form]

Have you read and understood the information above?
(Yes, No)

Do you want to participate in this research and continue with the survey?
(Yes, No)

In which country did you purchase your iPhone?
(United States, Other country ___, I don't know)

What model of iPhone do you have? For example, iPhone 4S, iPhone 5, etc. You can check your phone's model by opening the "Settings" app, going to "General", then "About". Your phone's "Model Name" should be listed on the "About" page.
(Original iPhone, iPhone 3G, ..., iPhone 11 (or 11 Pro or 11 Pro Max))

What version of iOS is running on your phone? For example, 7.9, 10.3, etc. You can check your phone's iOS software version by opening the "Settings" app, going to "General", then "About". Your phone's "Software Version" should be listed on the "About" page.

______

Do you own an Apple Watch?
(Yes, No)

Please select **all options** which accurately complete the following statement: "**Sometime in the past**, I have made in-person payments in physical locations..."
... using cash.
... using my credit card.
... using my debit card.
... using Apple Pay. Apple Pay allows you to make payments using your iPhone.

Please select **all options** which accurately complete the following statement: "**In the past week**, I have made in-person payments in physical locations..."
... using cash.
... using my credit card.
... using my debit card.
... using Apple Pay. Apple Pay allows you to make payments using your iPhone.

8.7 Controlled Experiment, Survey #2

Researchers at OMITTED are conducting a study to understand people's use of Apple services.

This survey is Survey #2 in the "Apple Services Study" that you previously gave your consent to participate in. It will take up to 30 minutes to complete this survey. If you complete **both** Survey #2 and Survey #3 **within 3 days of each survey invitation**, you will be compensated $7 total. We will invite you to Survey #3 one week after you complete Survey #2.

There are no right or wrong answers to any of our questions, so please answer honestly. Also, **please take the time to read the information in this survey carefully**.

[Control Group]
Apple Pay allows you to make payments in stores using your iPhone. Payments made with Apple Pay are charged to credit or debit cards that have been registered in Apple Pay.

[PMT and PMT+II Groups]
There have been many big hacks where credit and debit card information was stolen from retailers. For example, Target [70] was hacked in 2013, Home Depot [52] was hacked in 2014, and Saks Fifth Avenue [18] was hacked in 2018.

Information about millions of cards was stolen in these hacks. If criminals get your credit or debit card information, they might use that information to make fraudulent purchases. If you notice fraudulent purchases on your credit card, you can probably get refunded. But if the purchases are made on your debit card, you might not be able to get your money back [13]. In any case, you would need to get a replacement card with a new number, which would be inconvenient.

Thankfully, there are steps you can take to prevent your card information from being stolen and to protect yourself from card fraud. One of the best things you can do is to start using Apple Pay. Instead of paying by swiping or inserting your card, you can make payments through your phone, which adds an extra layer of security. Payments made with Apple Pay will still be charged to your credit or debit card, but because the payments go through Apple Pay, your card number is not shown to or recorded by retailers [10]. This means that your card number cannot be stolen from transactions made with Apple Pay. If your phone is stolen, the thief will not be able to make payments because Apple Pay is protected by your fingerprint and lock screen PIN. Although no system is perfectly secure, security experts generally agree that Apple Pay is more secure than paying with credit or debit cards [35]. Apple Pay takes just a few minutes to set up, and is widely accepted. As of this year, Apple Pay is accepted in 65% of retail locations [9] in the United States. For example, ALDI grocery, CVS pharmacy, and Starbucks all accept Apple Pay.

[See Figure 11]

[See Figure 12]

Please explain why you did not fill out the plan.

______

How **concerned or unconcerned** would you be if a fraudulent purchase was made on your credit or debit card?
(Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)

How **likely or unlikely** do you think you are to have a fraudulent purchase made on your credit or debit card?
(Very unlikely, Somewhat unlikely, Somewhat likely, Very likely)

How **easy or difficult** do you think it would be for you to use Apple Pay to make payments instead of using your credit or debit card?
(Very difficult, Somewhat difficult, Somewhat easy, Very easy)

Rate your level of **disagreement or agreement** with the following statement: "If I were to start using Apple Pay regularly, I would be **less likely** to be a victim of card fraud."
(Strongly disagree, Disagree, Agree, Strongly agree)

How **useful or not useful** do you think Apple Pay would be for making payments?
(Not at all useful, Slightly useful, Moderately useful, Very useful)

Rate your level of **disagreement or agreement** with the following statement: "I would feel self-conscious using Apple Pay in public."
(Strongly disagree, Disagree, Agree, Strongly agree)

Do you know anyone who uses Apple Pay?
(Yes, No, I'm not sure)

Do you have a credit or debit card registered in Apple Pay?
(Yes, No, I don't know)

When did you register a card in Apple Pay?
(Prior to taking this survey, While taking this survey)

Please explain why you do not know whether you have a credit or debit card registered in Apple Pay.

______

Rate your level of disagreement or agreement with the following statement: "I intend **to register** a credit or debit card in Apple Pay in the next week." (Strongly disagree, Disagree, Agree, Strongly agree)

Rate your level of disagreement or agreement with the following statement: "I intend **to use** Apple Pay in the next week."
(Strongly disagree, Disagree, Agree, Strongly agree)

What is your overall opinion of Apple Pay? (Please write a few sentences)

______

This is a link to the information about Apple Pay that we showed you earlier:
Apple Pay Setup, Use, and FAQ
Would you like us to send you a message on Prolific containing this link?
(Yes, No)

This is a link to your plan for using Apple Pay:
My Plan for Using Apple Pay
Would you like us to send you a message on Prolific containing this link?
(Yes, No)

Has a fraudulent purchase ever been made on your credit

or debit card?
(Yes, No, I don't know)

What gender do you identify with?
(Male, Female, Non-binary, Other: ___, Prefer not to answer)

What best describes your employment status?
(Working, paid employee; Working, self employed; Student; Not employed; Retired; Prefer not to answer)

Have you ever worked in or studied in a computer-related field? (Computer Science, IT support, etc.)
(Yes, No)

What is the highest level of school you have completed or degree you have earned?
(Less than high school, High school or equivalent, College or associate degree, Master's degree, Doctoral degree, Professional degree, Other: ___, Prefer not to answer)

Please estimate what your total household income will be for this year:
(Less than $10,000; $10,000 - $19,999; $20,000 - $39,999; $40,000 - $59,999; $60,000 - $79,999; $80,000 - $99,999; $100,000 or more; Prefer not to answer)

Each statement below describes how a person might feel about the use of security measures. Examples of security measures are laptop or tablet passwords, spam email reporting tools, software updates, secure web browsers, fingerprint ID, and anti-virus software.

Please indicate the degree to which you agree or disagree with each statement. In each case, make your choice in terms of how you feel **right now**, not what you have felt in the past or would like to feel.

There are no wrong answers.
(Strongly disagree, Somewhat disagree, Neither disagree nor agree, Somewhat agree, Strongly agree)

I seek out opportunities to learn about security measures that are relevant to me.

I am extremely motivated to take all the steps needed to keep my online data and accounts safe.

Generally, I diligently follow a routine about security practices.

I often am interested in articles about security threats.

I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.

I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.

8.8 Controlled Experiment, Survey #3

Researchers at OMITTED are conducting a study to understand people's use of Apple services.

This survey is Survey #3 in the "Apple Services Study" that you previously gave your consent to participate in. It will take up to 5 minutes to complete this survey. If you complete this survey **within 3 days of the survey invitation**, you will be compensated $7 total for completing Survey #2 and Survey #3.

There are no right or wrong answers to any of our questions, so please answer honestly. Also, **please take the time to read the information in this survey carefully**.

In Survey #2, you indicated that you [did not have][did not know whether you had] a credit or debit card registered in Apple Pay.

Since taking Survey #2 on $DATE, **have you registered a credit or debit card in Apple Pay**?
(Yes, No)

Please explain why you did not register a credit or debit card in Apple Pay.

______

Rate your level of disagreement or agreement with the following statement: "I intend **to register** a credit or debit card in Apple Pay in the next week."
(Strongly disagree, Disagree, Agree, Strongly agree)

Since completing Survey #2 on $DATE, have you made an in-person payment in a physical location using Apple Pay?
(Yes, No, I don't know)

Since completing Survey #2 on $DATE, how many payments have you made **with Apple Pay** in physical locations?

___

Please explain why you [used][did not use][do not know whether you used] Apple Pay.

______

Did you use Apple Pay in a location where you had previously paid with a credit or debit card?
(Yes, No, I don't know)

[PMT+II Group, if they wrote at least one location]
In Survey #2, you made a plan to use Apple Pay.

Since completing Survey #2 on $DATE, which of the locations in your plan, if any, **have you visited**?
($LOCATION_1, $LOCATION_2, $LOCATION_3)

Please select all options which accurately complete the following statement: "**Since completing Survey #2 on**

$DATE, I have made in-person payments at **$LOCATION_N**...”
...using cash
...using my credit card
...using my debit card
...using Apple Pay. Apple Pay allows you to make payments using your iPhone.
...using another payment method. Please specify: ___

How **concerned or unconcerned** would you be if a fraudulent purchase was made on your credit or debit card?
(Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)

How **likely or unlikely** do you think you are to have a fraudulent purchase made on your credit or debit card?
(Very unlikely, Somewhat unlikely, Somewhat likely, Very likely)

How **easy or difficult** do you think it would be for you to use Apple Pay to make payments instead of using your credit or debit card?
(Very difficult, Somewhat difficult, Somewhat easy, Very easy)

Rate your level of **disagreement or agreement** with the following statement: “If I were to start using Apple Pay regularly, I would be **less likely** to be a victim of card fraud.”
(Strongly disagree, Disagree, Agree, Strongly agree)

How **useful or not useful** do you think Apple Pay would be for making payments?
(Not at all useful, Slightly useful, Moderately useful, Very useful)

Rate your level of **disagreement or agreement** with the following statement: “I would feel self-conscious using Apple Pay in public.”
(Strongly disagree, Disagree, Agree, Strongly agree)

Rate your level of disagreement or agreement with the following statement: “I intend **to use** Apple Pay in the next week.”
(Strongly disagree, Disagree, Agree, Strongly agree)