Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Digitally Enabled Accounts and Unsolicited Requests for Money: Exposure and Payment Response among Phone Owners in 75 Economies

Faria Zahan Sarna

faria.sarna@metrouni.edu.bd

Metropolitan University

NHM Hassan Imam Chowdhury

Standard Islami Bank PLC

Abdullah Al Himel

Military Institute of Science and Technology

Research Article

Keywords: Consumer fraud, Financial inclusion, Consumer vulnerability, Mobile money, Scams, Global Findex

Posted Date: October 12th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11315629/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

Digitally enabled accounts may make consumers in developing economies easier to reach and more able to pay when asked for money. The 2025 Global Findex survey asked mobile phone owners in 75 economies whether an unknown person had called or texted them in the past year asking for money, and whether they sent it. The items record requests and payments, not verified fraud, scam prevalence or monetary loss. In survey-weighted fixed-effects models weighting economies by sample size, holders of digitally enabled accounts had a standardised probability of sending money that was 1.83 times as high as that of other phone owners (2.24% vs 1.22%; 95% CI for the risk ratio 1.45–2.31; n = 61,963). Holders were more often targeted (23.2% vs 19.4%; n = 62,761) and, once targeted, more often paid (9.3% vs 6.8%; risk ratio 1.37, 95% CI 1.14–1.65; n = 13,904). A model-dependent two-part decomposition places 63% (95% CI 43–73%) of the estimated gap at the payment stage; the interval includes values below half, and the stage-specific risk ratios do not differ significantly. Accounts not used for digital payments also showed premiums, not significantly different from digitally enabled ones. The payment-stage association, conditional on being targeted, was stable as observed controls were added but could reflect strong unobserved selection. Phone locks were not associated with lower payment, nor requests with account dormancy or distrust. These cross-sectional associations suggest that consumer protection linked to account access should examine the payment stage as well as the point of contact.

Highlights

• Adjusted payment probability was 1.83 times as high among digital account holders

• Holders were both targeted more often and, once targeted, paid more often

• A model-based split puts 63% (95% CI 43–73%) of the gap at the payment stage

• Accounts not used digitally also showed premiums; locks not linked to lower payment

1 Introduction

Over the past decade, mobile money and card-linked bank accounts have brought millions of adults in low- and middle-income economies into formal finance. The gains are documented: in Kenya, access to mobile money was followed by higher consumption and lower poverty (Suri & Jack, 2016). The same period has drawn attention to the consumer-protection problems that accompany inclusion, among them fraud (Buku & Mazer, 2017; Garz et al., 2021). An account that can release money on request is useful to a fraudster as well as to a family member.

Most population evidence on consumer fraud comes from high-income countries. Recent work in this journal has examined fraud victimisation and susceptibility in the United States (Raval, 2021; Robb & Wendel, 2023), mistreatment and fraud in financial services (Lim & Letkiewicz, 2023), and financial vulnerability, digital payments and inclusion in Norway and the United Kingdom (Seldal & Nyhus, 2022;

Vik et al., 2024). Victim surveys of cybercrime in Europe differ widely in how they measure victimisation (Reep-van den Bergh & Junger, 2018), and comparable microdata for developing economies have been scarce. The 2025 round of the Global Findex survey closes part of this gap: in 75 economies it asked mobile phone owners whether an unknown person had contacted them asking for money and whether they sent it (Klapper et al., 2025). These are unsolicited requests for money, not verified scams, and sending money is a payment response, not a measured loss. We treat them as proxies for potential scam exposure and payment and use "scam" only for the wider literature and policy context.

This paper asks whether consumers who hold financial accounts are more likely to send money in response to such requests and, if so, at which stage the difference arises: being reached, or deciding to pay once reached. Huang et al. (2026) recently showed in Chinese household data that the two stages can move in opposite directions. What is missing is evidence on how account access, the main instrument of financial inclusion policy, relates to each stage across many developing economies. The distinction matters for policy: if holders pay more often only because they are contacted more, remedies lie upstream, in call filtering, number registration and data protection; if they also pay more often once contacted, remedies may also lie at the point of payment.

We report adjusted standardised probabilities at three margins: being targeted, sending money once targeted (conversion), and sending money among all phone owners (overall payment). In the pooled sample, with economies weighted by sample size, holders of digitally enabled accounts had a standardised probability of sending money 1.83 times as high as that of other phone owners. In a two-part decomposition both margins contribute positive parts to the gap, although the stage-specific risk ratios do not differ significantly. Owners of accounts not used for digital payments also show premiums, so the evidence does not isolate a role for digital payment use as such. The payment-stage association is conditional on being targeted and could be produced by strong unobserved selection. All estimates are cross-sectional associations.

The paper makes three contributions. First, it provides multi-economy survey evidence on unsolicited requests for money and payment responses from developing economies, which the consumer-fraud literature has rarely covered. Second, it proposes a stage-specific analytical framework for vulnerability associated with account access (Section 2.1), and shows what single-stage measures miss. Third, it finds no association in these data between the requests and two common participation indicators, account dormancy and stated distrust, which matters for how inclusion outcomes are monitored.

Sections 2 to 7 present the framework, data, empirical strategy, results, discussion and conclusion.

2 Framework and Hypotheses

2.1 Consumer Vulnerability across Stages

We build on the view of consumer vulnerability as a situational state, not a fixed trait of particular groups. Baker et al. (2005) define vulnerability as a state of powerlessness that arises from an imbalance in

marketplace interactions, and Hill and Sharma (2020) review how such states arise from restricted control over resources and circumstances. Helberger et al. (2022) extend the argument to digital markets: because choice architectures shape what every consumer sees and can do, digital vulnerability is in principle universal and depends on the architecture as much as on personal characteristics (see also Dodsworth et al., 2023).

A consumer who receives an unsolicited request for money passes through a sequence: access to a means of payment, exposure to the request, the decision whether to comply, and the payment itself. Criminology separates the attempt from the outcome (Titus et al., 1995; Holtfreter et al., 2008), and consumer-vulnerability research locates vulnerability in consumers' circumstances or in market architecture, but neither asks whether a feature of the payment environment, such as holding an account, operates at more than one stage. Inclusion indicators, for their part, track account ownership and use rather than the stages at which holders may be exposed. We therefore propose a stage-specific analytical framework with three propositions. P1: a feature of the payment environment can be associated with vulnerability at exposure, at payment, or at both. P2: the associations at the two stages can differ in size and in their determinants, so vulnerability observed at one stage need not indicate it at the other. P3: because consumer-protection instruments act at one stage (call filtering at exposure, payment safeguards at payment), assessing protection requires measuring both. The framework organises outcomes; it is not a theory of the mechanisms that produce them. The survey observes the request and the payment, not the decision between them. We draw on one established theory for each stage (Fig. 1).

2.2 Exposure: Routine Activities and Targeting

Lifestyle–routine activity theory holds that victimisation requires a motivated offender, a suitable target and the absence of a capable guardian, brought together by everyday routines (Cohen & Felson, 1979). Yar (2005) examined how far the theory carries over to online crime, and later studies have linked online routines to fraud targeting (Pratt et al., 2010), identity theft (Reyns, 2013) and online consumer fraud victimisation (van Wilsem, 2013), while showing that the explanatory power of routine-activity elements differs across types of cybercrime (Leukfeldt & Yar, 2016).

Financial routines can raise target suitability in two ways. Holding an account makes a consumer a feasible source of funds, and using it leaves traces (registered numbers, transaction messages, agent interactions) that may make the consumer visible to offenders. If routines drive exposure, the association should rise with intensity of use and should be specific to contacts that seek money rather than to unwanted contact in general.

H1: Holders of digitally enabled accounts are more likely than other phone owners to receive unsolicited requests for money.

H2: Among holders, the likelihood of such requests rises with the frequency of account transactions.

H3: The account premium is larger for requests for money than for unwanted messages that do not seek money.

2.3 Conversion: The Decision to Pay

Lea et al. (2009) describe scam compliance as an error of judgement that scammers provoke through persuasion, and studies of online fraud victimisation examine which individual characteristics predict susceptibility (Norris et al., 2019; Whitty, 2019). Experiments show that susceptibility at the decision moment can be changed by training (Robb & Wendel, 2023) or by inserting time before a response (Waschka & Cunha, 2026), while scam identification ability can be measured and varies across consumers (Kubilay et al., 2023). Two features of account access could raise compliance once contacted: holders have funds in a form that a remote request can reach, and, for digitally enabled accounts, they can transfer money without visiting an agent or a branch, which removes natural pauses between request and payment. The data do not measure either feature, so they motivate the hypotheses but cannot be tested as mechanisms.

H4: Once targeted, holders of digitally enabled accounts are more likely than other phone owners to send money.

H5: In a two-part model of overall payment, the conversion margin contributes a positive part of the holder premium.

H5 is a decomposition objective with a sign prediction only: we predict a positive conversion part, not which part is larger.

Routine activity theory also predicts that capable guardianship lowers victimisation. A phone lock is the guardianship measure available in the data, but it protects the device against others, not the owner against persuasion. We therefore report it as a diagnostic, not as a hypothesis.

2.4 Account Participation

Trust shapes financial participation (Guiso et al., 2008), and exposure to fraud can reduce it: after a large investment fraud, residents of more exposed communities withdrew assets from investment advisers (Gurun et al., 2018). Because the survey measures requests, account activity and distrust over overlapping periods, it cannot establish whether requests precede disengagement. We therefore pose an associational research question rather than a hypothesis.

RQ: Are unsolicited requests for money associated with (a) account dormancy and (b) distrust of financial institutions as a reason for not holding an account?

3 Data and Measures

3.1 Survey and Sample

We use the Global Findex 2025 microdata (Development Research Group, Finance and Private Sector Development Unit, 2025), collected by Gallup in 2024 from nationally representative samples of adults aged 15 and older (Klapper et al., 2025). The public file holds 144,090 respondents in 140 economies. The digital-safety module was asked of mobile phone owners in 75 economies (64,663 respondents). Of the 75 economies, 73 are classified as low or middle income, one (Panama) as high income, and one (Venezuela) is unclassified; 34 are in Sub-Saharan Africa and 16 in developing Latin America and the Caribbean, so the pooled estimates draw heavily on these two regions. After excluding "don't know" and refused answers and requiring complete covariates, the analysis sample contains 62,761 phone owners, of whom 14,043 were targeted and 1,201 sent money (Online Resource 1, Table A1). Table 1 describes the analysis sample. The exposure models in Section 5.2 do not require the phone-lock item or a valid answer to the payment question and use 62,897 respondents, and the intensity analysis uses the 31,066 holders in that sample who reported transaction frequencies. The payment models use 13,904 targeted respondents and 61,963 phone owners because one economy with no reported payment drops out (Section 4.1).

Table 1
Descriptive statistics of the analysis sample, by digitally enabled account ownership

Variable	All	Account holders	Other phone owners
Targeted by a request for money, %	21.6	28.5	14.5
Sent money, % of those targeted	8.4	9.2	6.8
Sent money, % of all phone owners	1.8	2.6	1.0
Digitally enabled account, %	50.3	100.0	0.0
Any account, %	64.2	100.0	27.9
Women, %	49.3	46.0	52.7
Age, years (mean)	36.5	35.4	37.7
Aged 60 or older, %	10.5	7.6	13.4
In the workforce, %	62.9	71.8	53.9
Rural, %	59.4	55.4	63.5
Primary education or less, %	43.3	31.2	55.6
Tertiary education, %	9.3	14.1	4.3
Main phone is a smartphone, %	67.9	75.0	60.7
Online activities, count 0–8 (mean)	2.9	3.6	2.2
Uses the internet daily, %	53.2	61.5	44.8
Phone locked (PIN, password or fingerprint), %	59.7	69.8	49.4
Respondents (unweighted)	62,761	32,871	29,890

Survey-weighted means in the analysis sample. Unweighted counts for the conversion row are 14,043 targeted respondents (9,633 holders, 4,410 others). "Other phone owners" include 27.9% who hold an account not used for digital payments. Global Findex 2025, 75 economies.

3.2 Outcomes

The targeting item reads: "In the past 12 months, did you receive a phone call or SMS or text message on your mobile phone from someone you didn't know asking you to send money?" Respondents who answered yes were asked: "Did you send the money to this person?" Neither question uses the word "scam", although the producer's variable labels do. We therefore call the first outcome an unsolicited request for money and the second a payment response. The items do not establish deception, record the amount sent or identify the payment channel, so they cannot measure scam prevalence or monetary harm. Some requests may have been benign, for instance from relatives or acquaintances using unfamiliar numbers, and remittance networks could generate both such requests and payments; Section

5.4 examines this. Conversion is defined among targeted respondents. Overall payment is defined among all phone owners and equals one for respondents who were targeted and sent money. Online Resource 1, Table A2 lists all items and codings.

For the specificity check (H3) we use the module item on receiving unwanted and offensive messages, photos or videos, which shares the channel and the reporting format but does not seek money. For the research question, dormancy is defined for owners of an account at a financial institution and equals one if no money was deposited or withdrawn in the past year; distrust equals one if a phone owner without such an account cites lack of trust in financial institutions as a reason, an item asked in 43 economies.

3.3 Account Ownership and Controls

Our main exposure is the Findex indicator of a digitally enabled account, meaning a mobile money account or an account at a bank or similar institution from which the respondent makes digital payments using a card or phone. Half of the weighted sample hold such an account (Table 1). To separate account access from digital use, we also distinguish three groups: no account, an account not used for digital payments, and a digitally enabled account. For H2, transaction intensity is the most frequent of five reported transaction types (deposits and withdrawals for financial-institution accounts; deposits, transfers and cash-outs for mobile money), coded never, less than monthly, monthly and weekly.

Controls fall into three blocks. Demographics are sex, age and its square, workforce participation, rural residence, education and within-economy income quintile. Connectivity is the frequency of phone and internet use. Visibility is whether the main phone is a smartphone, the number of eight online activities performed on a phone (for example, social media use or job search), and whether the respondent has ever sent a text message. The conversion and overall payment models also include the phone lock; because the lock could be a consequence of account ownership, we report estimates without it as well. All models include economy fixed effects, so comparisons are made between consumers in the same economy.

4 Empirical Strategy

4.1 Estimation, Weighting and Inference

For each margin we estimate a logit model of the outcome on the account indicator, the controls and economy fixed effects, weighted by the survey weights supplied with the data. Within each economy the weights sum to the number of respondents, so the pooled estimand weights economies by their sample sizes (a median of 840 phone owners per economy, and 2,124 in India), not by their populations; Online Resource 1 reports population-scaled estimates. Standard errors are clustered by economy, the level at which national samples are drawn independently, and inference uses the t distribution with G − 1 degrees of freedom, where G is the number of economies (Cameron & Miller, 2015). Because the public file does not identify sampling strata or primary sampling units, these are economy-clustered standard errors, not

full design-based variances. One economy reported no payment and drops out of the fixed-effects payment models; a linear probability model that retains all 75 economies is reported as a check. For each margin we report the standardised probability for holders and for others, that is, the weighted mean predicted probability with the account indicator set to one and to zero for every respondent, together with their difference, their ratio and the odds ratio, with delta-method confidence intervals.

4.2 Decomposing the Overall Gap

The overall gap can be split into stages only within a model in which overall payment is the product of the two stages. We therefore use a two-part g-formula. Let p(a, X) be the predicted probability of being targeted and c(b, X) the predicted probability of paying once targeted, for account status a and b, from the targeting and conversion models, and let Eab be the weighted mean of p(a, X)·c(b, X) over all phone owners. The overall gap is E11 − E00. Its targeting part is the average of (E10 − E00) and (E11 − E01), and its conversion part the average of (E01 − E00) and (E11 − E10); the two parts sum exactly to the gap. Intervals come from an economy-level cluster bootstrap with 999 replications, in which whole economies are resampled and duplicated economies receive their own fixed effects. Only a product of stage models can be split into stage parts, so we decompose the two-part model rather than the separately estimated overall payment model, which remains the primary estimate (Table 3). The two-part model implies a smaller overall risk ratio because the specifications differ in functional form, and the cross-world terms (E10, E01) are model-based quantities, not observed interventions; Online Resource 1, Tables A8 and A8b report both, and three alternative decompositions. The decomposition is a descriptive accounting of how the estimated gap is distributed across stages under this model; it does not identify causal pathways or show which intervention would be most effective.

4.3 Sensitivity Analysis

The estimates are associations conditional on observed characteristics. We assess how much unobserved confounding would be needed to explain them with E-values computed from the standardised risk ratios (VanderWeele & Ding, 2017), the robustness value of Cinelli and Hazlett (2020), and coefficient-stability bounds (Oster, 2019). Because economy fixed effects absorb much of the explained variance, we compute the bounds with R^2 net of the fixed effects and report them over a grid of maximum R^2 values, from Oster's proportional benchmark (1.3 times the full model) to absolute values of 0.1 to 0.5. The comparison of requests for money with unwanted messages is a specificity check in the spirit of negative-control outcomes (Lipsitch et al., 2010); the two outcomes may differ in prevalence and recognition as well as in their link to accounts, so it can support specificity but not identify an effect.

Because conversion is observed only among the targeted, conditioning on targeting could create a spurious conversion premium if an unobserved trait affects both margins (Elwert & Winship, 2014). We simulate this mechanism with a true conversion effect of zero, base rates matched to the data and a targeting premium matched to the observed one, varying the trait's effect on each margin from − 2 to + 2 latent standard deviations (2,000,000 draws per scenario, with Monte Carlo standard errors). To calibrate

these magnitudes, we compare them with the latent-scale effects of the observed covariates. A bivariate selection model was uninformative because the available exclusion restriction is weak (Online Resource 1, Section A12).

Further checks, reported in Online Resource 1, include augmented inverse-probability weighting (Robins et al., 1994), a specification curve of 36 models (Simonsohn et al., 2020; Fig. S3), a restricted wild cluster bootstrap (Roodman et al., 2019), alternative weighting schemes (Solon et al., 2015), random-effects meta-analysis of economy-level estimates (DerSimonian & Laird, 1986), missing-indicator coding, leave-one-region-out samples, remittance controls and every analysis in the internal analysis plan, which was not preregistered. Online Resource 1, Table A0 states the role of each analysis (primary estimate, hypothesis test, decomposition, sensitivity, specificity or exploratory analysis) and what it can and cannot establish. Across the four hypothesis tests (H1–H4) and the two participation associations we apply Holm and Benjamini–Hochberg corrections (Benjamini & Hochberg, 1995; Holm, 1979).

4.4 Software, Reproducibility and Use of AI Tools

All analyses were run in Python from the raw public file; the scripts reproduce every table and figure (Online Resource 2). A large language model (Claude, Anthropic; used in October 2026) helped to write analysis code and draft text. It did not generate or alter data: every estimate was computed by the scripts from the survey file. The authors specified the analyses, checked the code and every reported number against the output, revised the text and take full responsibility for the content.

5 Results

5.1 Descriptive Patterns

About one phone owner in five reported an unsolicited request for money in the past year, and 8.4% of those targeted sent money. Rates vary widely by region: 26.9% of phone owners in Sub-Saharan Africa were targeted and 11.3% of the targeted paid, against 9.8% and 15.4% in South Asia and 25.0% and 3.7% in Latin America and the Caribbean (Online Resource 1, Table A3). These contrasts are descriptive and may reflect differences in offender strategies, payment systems or reporting. Scaled to adult populations, the rates imply that roughly 40 million adults sent money in response to such a request in the past year; an approximate, secondary figure based on population weights (Online Resource 1, Table A10).

Figure 2 shows the unadjusted profile, using all valid responses for each outcome (so rates differ slightly from Table 1; for example, 28.4% of holders were targeted, against 28.5% in the analysis sample). Holders of digitally enabled accounts were targeted at about twice the rate of adults without any account (28.4% vs 14.0%). Among age groups, adults aged 60 and older reported the lowest rates of both targeting (16.1%) and payment (6.9%); this concerns only unsolicited requests for money, not other frauds. Among education groups, the most educated were the most often targeted (27.1%) but the least

likely to pay (6.4%), while those with primary education or less were targeted least (18.9%) and paid most often (10.1%).

5.2 Exposure

Table 2 reports the exposure models. With economy fixed effects only, holders had 1.85 times the odds of being targeted. The odds ratio falls to 1.58 with demographics, to 1.49 with connectivity and to 1.32 (95% CI 1.24–1.42) with the visibility block; the average marginal effect in the main model is 4.1 percentage points. Much of the raw association therefore reflects who holds accounts and how they use their phones.

Table 2
Digitally enabled account ownership and being targeted (adjusted estimates)

Model or test	Estimate	95% CI
Panel A: Control build-up (odds ratios)		
Economy fixed effects only	1.85	1.72–2.00
+ demographics	1.58	1.46–1.70
+ phone and internet use	1.49	1.39–1.60
+ visibility (main model)	1.32	1.24–1.42
Main model, average marginal effect (pp)	4.1	3.1–5.0
Panel B: Routine-activity tests		
H2: trend per step of transaction intensity, holders (OR)	1.10	1.03–1.17
H3: unwanted and offensive messages (OR)	1.14	1.04–1.25
H3: ratio of ORs, request for money vs unwanted messages	1.16	1.05–1.28
Panel C: Sensitivity of the main model		
E-value of the standardised risk ratio (CI limit)	1.72	(1.58)
Cinelli–Hazlett robustness value	4.3%	

N = 62,897 phone owners in 75 economies (H2: 31,066 holders with transaction frequencies). Survey-weighted logit models with economy fixed effects; standard errors clustered by economy. The main model includes demographics, phone and internet use, smartphone, online activities and texting. Coefficient-stability bounds: Table A6b.

The pattern is consistent with the routine-activity account. Among holders, the odds of being targeted rose by 10% per step of transaction intensity (H2; p = 0.005), and predicted probability rose from 26.5% for those who never transact to 30.0% for weekly users (Online Resource 1, Fig. S6). The three intensity

categories are jointly significant (p = 0.028), although none differs significantly from "never" on its own, so H2 rests on the trend. Transaction intensity combines different transaction types and may proxy for employment, resources or connectivity, so the gradient is consistent with a visibility mechanism but does not test it. Account ownership was also associated with unwanted messages that do not seek money, but less strongly: the odds ratio for requests for money was 1.16 times that for unwanted messages (p = 0.003; H3). This specificity comparison shows that the association is not the same for the two outcomes, although they may also differ in how readily respondents recognise and report them, and the check does not rule out confounding. Related outcomes, such as identity-document misuse, are reported in Online Resource 1, Table A6.

The exposure association is less secure than these tests suggest. The coefficient falls by more than half as controls are added. With R^2 net of fixed effects, Oster's δ for a zero effect is 1.79 under the proportional benchmark but falls below one once the maximum R^2 is twice the full-model value or more (Online Resource 1, Table A6b). The E-value and robustness value are modest (Table 2, Panel C). We therefore read H1 to H3 as supported in the sense of a risk marker, a consistent pattern in who is targeted, not as evidence that account ownership causes targeting.

5.3 Conversion and Overall Payment

Table 3 and Fig. 3 present the core results. Once targeted, holders sent money more often than other phone owners: the standardised probability was 9.3% against 6.8%, a difference of 2.5 percentage points and a risk ratio of 1.37 (95% CI 1.14–1.65). This association, consistent with H4, is conditional on selection into targeting: among consumers who received a request, holders were more likely to pay, an adjusted association among targeted respondents, not a causal effect of account ownership on compliance. Combining both margins, 2.24% of holders and 1.22% of other phone owners sent money in response to an unsolicited request, a difference of 1.0 percentage point and a risk ratio of 1.83 (95% CI 1.45–2.31). Without the phone lock, which may itself follow from account ownership, the conversion risk ratio is 1.39 (95% CI 1.15–1.67). Full model results are in Online Resource 1, Table A9.

Table 3
Adjusted, marginally standardised probabilities at each margin, digitally enabled account holders vs other phone owners

Population	Targeting	Conversion	Overall payment
	Phone owners	Targeted	Phone owners
N (events); economies	62,761 (14,043); 75	13,904 (1,201); 74	61,963 (1,201); 74
Probability, holders (%)	23.2	9.3	2.24
Probability, other phone owners (%)	19.4	6.8	1.22
Difference, pp (95% CI)	3.8 (2.8–4.8)	2.5 (1.1–3.9)	1.0 (0.7–1.4)
Risk ratio (95% CI)	1.20 (1.14–1.26)	1.37 (1.14–1.65)	1.83 (1.45–2.31)
Odds ratio (95% CI)	1.30 (1.22–1.40)	1.44 (1.16–1.79)	1.87 (1.47–2.38)
E-value (CI limit)	1.68 (1.54)	2.08 (1.53)	3.06 (2.26)

Adjusted, marginally standardised estimates; conversion is estimated among targeted respondents only. Survey-weighted logit models with economy fixed effects, all controls and the phone lock; one economy without any reported payment drops from the payment models. Probabilities are marginally standardised; intervals are delta-method intervals from economy-clustered standard errors. Conversion RR ÷ targeting RR = 1.14 (95% CI 0.95–1.37), p = 0.15; cluster bootstrap (999 replications) interval for the log difference − 0.040 to 0.314, bootstrap p = 0.14. The targeting estimates differ slightly from Table 2 because the phone lock is added and respondents without a valid answer on payment are excluded.

Table 4 shows how the gap divides between the stages in the two-part model. The model implies an overall gap of 0.84 percentage points (risk ratio 1.65). Of this gap, 0.31 percentage points (37%) falls at the targeting margin and 0.53 percentage points (63%) at the conversion margin. Alternative decompositions give conversion shares between 52% and 64% (Online Resource 1, Table A8b). These figures depend on the model and describe the estimated gap; they are not shares of consumer harm. Their use is descriptive: they show that the holder gap is not confined to exposure, so indicators that measure only contact would miss part of it. The conversion part is positive and its interval excludes zero, which supports H5. The share's interval includes values below half and the conversion risk ratio is not significantly larger than the targeting risk ratio, so the evidence does not show that the payment stage accounts for more of the gap than targeting; nor, since the two ratios refer to different populations, that the stages are equivalent.

Table 4
Model-based two-part decomposition of the overall payment gap between holders and other phone owners

Quantity	Estimate	95% CI
Overall probability, holders (E11, %)	2.13	1.73–2.55
Overall probability, others (E00, %)	1.29	1.02–1.62
Gap, E11 – E00 (pp)	0.84	0.49–1.18
Targeting part (pp)	0.31	0.21–0.43
Conversion part (pp)	0.53	0.23–0.81
Conversion share of the gap	63%	43–73%

Two-part g-formula over all phone owners (Section 4.2): Eab is the weighted mean of p(a, X)·c(b, X), where p is the predicted probability of being targeted and c of paying once targeted. Economy-cluster bootstrap with 999 replications (percentile intervals). Cross-world terms: E10 = 1.55%, E01 = 1.77%. The 63% share refers to this two-part model only; the separately estimated overall payment model (Table 3) implies a larger gap (1.0 pp; RR 1.83) and is not decomposed here.

The two margins also differ in how they respond to added controls. The conversion coefficient barely moves (2.6 to 2.5 percentage points in the linear model with economy fixed effects), and with R^2 net of fixed effects Oster's δ for a zero effect is 51.7 under the proportional benchmark and 7.8 when the maximum R^2 is three times the full-model value; for targeting the corresponding values are 1.79 and 0.27 (Online Resource 1, Table A6b). Observed controls explain little of conversion, however, and with absolute maximum R^2 of 0.2 or more both associations could be explained by unobserved selection. Robustness values (3.6% and 4.3%) and E-values at the confidence limit (1.53 and 1.54) are similar. The difference in robustness between the margins therefore holds under proportional benchmarks but should not be overstated. These bounds concern observed covariates; selection into targeting is examined in Section 5.4.

5.4 Account Type, Remittances and Selection

Table 5 separates account access from digital use. At every margin, owners of accounts not used for digital payments had higher odds than consumers without an account, and the direct contrast between digitally enabled and non-digital accounts is not significant (conversion OR 1.10, 95% CI 0.79–1.53; overall payment 1.35, 0.92–1.98). The premium is therefore associated with holding an account; the data do not show an additional premium for digital use, although the wide intervals for the contrast cannot rule one out. This limits claims about digital payment use as such; Section 6.1 sets out the explanations the data cannot separate.

Table 5
Account type and the three margins (adjusted odds ratios, 95% CI)

Comparison	Targeting	Conversion	Overall payment
Account not used for digital payments vs no account	1.28 (1.14–1.42)	1.48 (1.03–2.12)	1.59 (1.10–2.30)
Digitally enabled account vs no account	1.40 (1.30–1.51)	1.62 (1.26–2.07)	2.15 (1.66–2.77)
Digitally enabled vs non-digital account	1.10 (0.98–1.23)	1.10 (0.79–1.53)	1.35 (0.92–1.98)
Standardised probability: no / non-digital / digital account (%)	18.4 / 21.8 / 23.2	6.1 / 8.6 / 9.3	1.08 / 1.69 / 2.25

Survey-weighted logit models with economy fixed effects and all controls; three-category exposure. N as in Table 3. Respondents in the analysis sample: no account 20,775; non-digital account 9,115; digitally enabled account 32,871. Targeted respondents in the conversion model: 2,931; 1,391; 9,582. Standardised probabilities come from the three-category models and can differ slightly from Table 3.

Remittance networks are a possible source of benign requests and of payments. Half of phone owners sent or received a domestic remittance or received an international one in the past year. Adding remittance use as a control leaves the conversion odds ratio at 1.42 (95% CI 1.16–1.74), and the premium does not differ between remitters and non-remitters (ratio of odds ratios 1.04, 95% CI 0.68–1.59, p = 0.86). Estimated separately among non-remitters, however, it is smaller and imprecise (OR 1.16, 95% CI 0.86–1.57; 4,449 targeted respondents), so we cannot exclude that part of the association runs through remittance relationships (Online Resource 1, Table A4c).

Selection into targeting is the main threat to the conversion result. In the collider simulation (Online Resource 1, Fig. S5), an unobserved trait whose effects on both margins are up to 0.5 latent standard deviations, larger than the effect of any single observed covariate on conversion (the largest, for infrequent phone use, is 0.41), produces spurious risk ratios of at most 1.03 (Monte Carlo SE ≤ 0.02). A trait twice as strong produces up to 1.21, which would leave an adjusted risk ratio of 1.13 (95% CI 0.94–1.36), and stronger traits with opposite effects on the two margins can produce the whole association. The simulation is a sensitivity analysis, not a correction: selection as strong as the observed covariates would not produce the association, but the data cannot show that actual selection lies in that range.

The association holds without survey weights, with equal weights per economy, with region instead of economy fixed effects, in a linear probability model that keeps all 75 economies (2.46 percentage points; wild cluster bootstrap p = 0.002), for each account definition and with missing-indicator coding (Online Resource 1, Table A4 and Fig. S4). The economy-level estimates pool to 1.9 percentage points with little detectable heterogeneity (I^2 = 7%), and none is significantly negative (Fig. 4; named economies in Figs. S1–S2), although this does not imply the same association in every economy. Precision varies by region:

without Sub-Saharan Africa, which removes 34 of the 75 economies and more than half of the targeted respondents, the risk ratio of 1.34 (95% CI 0.98–1.82) is not significant. Population-scaled weights give larger estimates (conversion risk ratio 2.14; Online Resource 1, Table A4b), largely because India accounts for a third of the adult population of the 75 economies and has a large but imprecise premium; without India the population-weighted risk ratio is 1.65 (95% CI 1.20–2.26). The estimated association was positive in all examined subgroups, although its precision varied and we found no statistically significant differences between subgroups (Online Resource 1, Table A5).

5.5 Guardianship and Capability at Conversion

A phone lock was not associated with lower payment. Targeted consumers whose phone was locked (PIN, password or fingerprint) were more likely to send money (OR 1.36, 95% CI 1.09–1.70), and in no specification is the lock associated with lower payment (Online Resource 1, Table A7). Besides the reason given in Section 2.3, intensive phone users may be more likely both to lock phones and to receive and act on requests; the data cannot separate these readings. Formal education and income offered at most weak protection at conversion (Online Resource 1, Table A9).

5.6 Association with Account Participation

Table 6 reports the research question. Being targeted was not associated with dormancy among financial-institution account owners (OR 0.97, 95% CI 0.84–1.13) or with citing distrust as a reason for not having such an account (OR 1.01, 0.84–1.20). This is absence of evidence, not evidence of absence. Given the minimum detectable odds ratios in Table 6, moderate associations are inconsistent with the data, while smaller ones cannot be ruled out. Among digital account holders, being targeted was associated with more frequent use (weekly use OR 1.14, 95% CI 1.05–1.25), which fits the intensity gradient in Section 5.2.

Table 6
Unsolicited requests for money and account participation (adjusted odds ratios)

Outcome (population)	Exposure	N (economies)	Base rate	OR (95% CI)	Detectable OR (80% power)
Dormant account (financial-institution account owners)	Targeted	30,000 (75)	10.8%	0.97 (0.84–1.13)	≥ 1.23 or ≤ 0.82
	Sent money	29,997 (75)	10.8%	0.96 (0.70–1.32)	≥ 1.56 or ≤ 0.64
Distrust as reason for no account (phone owners without one)	Targeted	13,981 (43)	29.2%	1.01 (0.84–1.20)	≥ 1.28 or ≤ 0.78
	Sent money	13,980 (43)	29.2%	0.78 (0.43–1.40)	≥ 2.26 or ≤ 0.44
Weekly use (digital account holders)	Targeted	31,112 (75)	41.7%	1.14 (1.05–1.25)	
	Sent money	31,108 (75)	41.7%	1.12 (0.92–1.37)	

Survey-weighted logit models with economy fixed effects and all controls; standard errors clustered by economy. The distrust item was asked in 43 economies. Detectable ORs are minimum detectable effects at 80% power for the null results. The weekly-use sample comprises digital account holders with reported transaction frequencies. Measures refer to overlapping periods, so the table reports associations, not sequences. Targeted rows for dormancy and distrust are the research-question tests (RQa, RQb) in the Holm correction; other rows are supplementary. The analysis plan was not preregistered.

After Holm correction across the four hypothesis tests and the two participation associations, H1 to H4 remain significant (largest adjusted p = 0.014) and both participation associations remain null (Online Resource 1, Table A11).

6 Discussion

6.1 What the Results Show

It helps to separate three levels. What the data show is that account holders are more likely to send money in response to unsolicited requests: in the pooled sample they are targeted more often and, among the targeted, pay more often, and the payment-stage part of the estimated gap is positive in the two-part model. The interpretation we draw is that this pattern is consistent with situational vulnerability

associated with account access at the payment stage as well as at contact; it is not a direct observation of fraud susceptibility, and scam vulnerability remains a possible interpretation of the outcomes, not what they measure. What remains unobserved is the mechanism. Easier access to funds, greater susceptibility to persuasion among holders, benign requests within remittance networks, or strong unmeasured selection into targeting could each contribute, and the data contain no measure of transfer speed, time to payment, payment channel, warnings or the consumer's relationship to the requester.

For consumer-vulnerability research, the contribution is the stage-specific framework of Section 2.1, not a new theory or a validated mechanism. The results show what single measures would miss. Overall payment alone would hide that the premium is present at both stages; exposure alone would rank the most educated as most at risk, although they paid least once targeted; and ownership statistics alone would count holders only as beneficiaries of inclusion. For research design, the framework implies collecting contact and response separately, estimating each stage and reporting the overall gap as an accounting of both. Where the stage associations differ, it indicates which class of instrument to test first even when mechanisms are unknown; it does not show that any instrument works. Vulnerability located in circumstances (Baker et al., 2005) or architecture (Helberger et al., 2022) should therefore also be located by stage. Consistent with P1, account holders show premiums at both stages, the second being a conditional association among the targeted; consistent with P2, a group can be more exposed but less likely to pay, as the most educated were in the unadjusted profile (Fig. 2). The account-type results fit three explanations that the data cannot separate: access to funds that a remote request can reach; digital payment capability, whose additional role the wide intervals cannot exclude; and selection, if account ownership proxies for income, work, social networks or financial needs that affect both stages. The data test none of these mechanisms, nor a situational account against one based on personal deficits.

The participation results caution against relying on inclusion statistics alone. Unlike the investment-fraud evidence from the United States (Gurun et al., 2018), we find no association between requests and dormancy or distrust. Effects may be smaller than we can detect, appear on other outcomes or take longer to emerge. Either way, the two participation indicators examined here were not associated with the reported requests in this dataset, so they may not be a sufficient signal of this kind of problem.

6.2 Policy Implications

The findings suggest where policy attention and testing could go; they do not show which interventions work. First, because the payment-stage part of the estimated gap is positive, payment-stage safeguards are priorities for testing alongside upstream measures against scam calls and messages. Regulators in high-income markets have moved in this direction: the United Kingdom requires reimbursement of authorised push payment fraud victims (Payment Systems Regulator, 2023), and the European Union requires payment service providers to offer verification of the payee's name (Regulation (EU) 2024/886, 2024). These measures are in force elsewhere; their effects in developing economies, like those of confirmation prompts, delays or warnings in mobile money, are untested, and designs would differ across agent-based mobile money, bank accounts and instant payments. Because accounts not used for

digital payments also showed premiums, any safeguards tested would need to cover agent-assisted and over-the-counter transfers, not only app-based payments. Second, any added friction carries a cost for inclusion: delays and confirmations slow legitimate transfers such as remittances, which half of phone owners make or receive, so safeguards targeted at first payments to unknown recipients may be less costly than general delays; this too is a question for testing. Third, device locks, which were not associated with lower payment, should not be presented as a substitute for transaction-level protection, although they remain relevant to consumer protection. Fourth, inclusion monitoring could add periodic direct measures of unsolicited requests and payments, as the Findex module does, because the two participation indicators examined here showed no association with them.

Consumer education remains relevant: scam-identification ability varies (Kubilay et al., 2023), and training improved detection in a US experiment, although its effect depended on the channel and faded (Robb & Wendel, 2023). Formal education offered at most weak protection at conversion here.

6.3 Limitations

The main limitation is the design: cross-sectional data cannot identify effects of account ownership, and the sensitivity analyses bound, but do not remove, that problem. The targeting association, and through it the overall payment association, is sensitive to unobserved selection; the conversion association is conditional on targeting and not robust to selection much stronger than the observed covariates. We cannot separate the capacity to pay from susceptibility to persuasion, or rule out that part of the association reflects benign requests within remittance networks. The outcomes are self-reported over 12 months, refer to requests from unknown persons, and do not record deception, amounts or payment channels. Misreporting unrelated to account ownership would bias the estimates toward zero; if holders recall requests more readily, or remember payments better because accounts leave records, the associations would be overstated. Standard errors are not full design-based variances. The pooled estimand weights economies by sample size; population-weighted estimates are larger and depend on India, and the conversion estimate is imprecise without Sub-Saharan Africa. Coverage is limited to phone owners in the 75 economies where the module was fielded, which are concentrated in Sub-Saharan Africa and Latin America.

7 Conclusion

Across 75 economies, phone owners with digitally enabled accounts had a standardised probability of sending money in response to an unsolicited request that was 1.83 times as high as that of others, and owners of accounts not used for digital payments also showed premiums, so the findings do not identify a risk specific to digital channels or payment speed. Both stages contribute: holders were targeted more often and, once targeted, paid more often, and in the two-part model the payment stage accounts for about 63% of the estimated gap, a model-dependent figure whose interval includes values below half and which does not measure consumer harm. These are associations among phone owners in economies concentrated in Sub-Saharan Africa and Latin America, weighted by sample size and less precise without Sub-Saharan Africa, which need not hold with the same magnitude in every economy,

and the payment-stage result could be explained by strong unobserved selection into targeting. Read through the proposed stage-specific framework, they suggest that consumer protection linked to account access should examine the payment stage as well as the point of contact. Panel data that follow consumers through contact, payment and recovery, and trials of payment-stage safeguards in developing markets, would test the mechanisms that this cross-section can only point to.

Declarations

Author Contribution

F.Z.S. led the conceptualisation of the study, contributed consumer-vulnerability and consumer-policy expertise, conducted the statistical analyses, and drafted the manuscript. N.H.I.C. contributed digital banking, payment-systems, and cybersecurity expertise, co-designed the methodology, and undertook critical review and editing. A.A.H. carried out the literature search and data curation, prepared and formatted the manuscript, and contributed to shaping its overall structure and revision. All authors read and approved the final manuscript.

Data Availability

The Global Findex 2025 microdata (WLD_2024_FINDEX_v02_M) are available from the World Bank Microdata Library (https://doi.org/10.48529/bk9n-8r43). The licence does not permit redistribution, so the data are not included with the submission. The analysis scripts that reproduce every table and figure from the raw file are provided as Online Resource 2. The internal analysis plan was not preregistered; all planned analyses, including those not used as evidence, are reported in Online Resource 1.

References

1. Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building understanding of the domain of consumer vulnerability. *Journal of Macromarketing*, *25*(2), 128–139. https://doi.org/10.1177/0276146705280622
2. Benjamini, Y., & Hochberg, Y. (1995). Controlling the false discovery rate: A practical and powerful approach to multiple testing. *Journal of the Royal Statistical Society: Series B (Methodological)*, *57*(1), 289–300. https://doi.org/10.1111/j.2517-6161.1995.tb02031.x
3. Buku, M., & Mazer, R. (2017, April). *Fraud in mobile financial services: Protecting consumers, providers, and the system* [Brief]. CGAP. https://documents1.worldbank.org/curated/en/249151504766545101/pdf/119208-BRI-PUBLIC-Brief-Fraud-in-Mobile-Financial-Services-April-2017.pdf
4. Cameron, A. C., & Miller, D. L. (2015). A practitioner's guide to cluster-robust inference. *Journal of Human Resources*, *50*(2), 317–372. https://doi.org/10.3368/jhr.50.2.317

5. Cinelli, C., & Hazlett, C. (2020). Making sense of sensitivity: Extending omitted variable bias. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, *82*(1), 39–67. https://doi.org/10.1111/rssb.12348
6. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589
7. DerSimonian, R., & Laird, N. (1986). Meta-analysis in clinical trials. *Controlled Clinical Trials*, *7*(3), 177–188. https://doi.org/10.1016/0197-2456(86)90046-2
8. Development Research Group, Finance and Private Sector Development Unit (2025). *The Global Findex Database 2025: Connectivity and financial inclusion in the digital economy* (WLD_2024_FINDEX_v02_M) [Data set]. World Bank, Development Data Group. https://doi.org/10.48529/bk9n-8r43
9. Dodsworth, T., Riefa, C., Saintier, S., & Twigg-Flesner, C. (2023). Editorial: Digital vulnerability. *Journal of Consumer Policy*, *46*(4), 413–417. https://doi.org/10.1007/s10603-023-09555-6
10. Elwert, F., & Winship, C. (2014). Endogenous selection bias: The problem of conditioning on a collider variable. *Annual Review of Sociology*, *40*, 31–53. https://doi.org/10.1146/annurev-soc-071913-043455
11. Garz, S., Giné, X., Karlan, D., Mazer, R., Sanford, C., & Zinman, J. (2021). Consumer protection for financial inclusion in low- and middle-income countries: Bridging regulator and academic perspectives. *Annual Review of Financial Economics*, *13*, 219–246. https://doi.org/10.1146/annurev-financial-071020-012008
12. Guiso, L., Sapienza, P., & Zingales, L. (2008). Trusting the stock market. *The Journal of Finance*, *63*(6), 2557–2600. https://doi.org/10.1111/j.1540-6261.2008.01408.x
13. Gurun, U. G., Stoffman, N., & Yonker, S. E. (2018). Trust busting: The effect of fraud on investor behavior. *The Review of Financial Studies*, *31*(4), 1341–1376. https://doi.org/10.1093/rfs/hhx058
14. Helberger, N., Sax, M., Strycharz, J., & Micklitz, H. W. (2022). Choice architectures in the digital economy: Towards a new understanding of digital vulnerability. *Journal of Consumer Policy*, *45*(2), 175–200. https://doi.org/10.1007/s10603-021-09500-5
15. Hill, R. P., & Sharma, E. (2020). Consumer vulnerability. *Journal of Consumer Psychology*, *30*(3), 551–570. https://doi.org/10.1002/jcpy.1161
16. Holm, S. (1979). A simple sequentially rejective multiple test procedure. *Scandinavian Journal of Statistics*, *6*(2), 65–70. https://www.jstor.org/stable/4615733
17. Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189–220. https://doi.org/10.1111/j.1745-9125.2008.00101.x
18. Huang, W., Hafizuddin-Syah, B. A. M., Yaacob, M. H., & Yao, C. (2026). The offender's selection paradox: Why the financially vulnerable are targeted less but victimized more in China's telecom fraud. *Crime Law and Social Change*, *84*(1). Article 8. https://doi.org/10.1007/s10611-025-10262-1
19. Klapper, L., Singer, D., Starita, L., & Norris, A. (2025). The Global Findex Database 2025: Connectivity and financial inclusion in the digital economy. *World Bank*. https://doi.org/10.1596/978-1-4648-

2204-9

20. Kubilay, E., Raiber, E., Spantig, L., Cahlíková, J., & Kaaria, L. (2023). Can you spot a scam? Measuring and improving scam identification ability. *Journal of Development Economics*, *165*, 103147. https://doi.org/10.1016/j.jdeveco.2023.103147
21. Lea, S. E. G., Fischer, P., & Evans, K. M. (2009). *The psychology of scams: Provoking and committing errors of judgement* (Report OFT1070). Office of Fair Trading. http://hdl.handle.net/10871/20958
22. Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409
23. Lim, H., & Letkiewicz, J. C. (2023). Consumer experience of mistreatment and fraud in financial services: Implications from an integrative consumer vulnerability framework. *Journal of Consumer Policy*, *46*(2), 109–135. https://doi.org/10.1007/s10603-023-09535-w
24. Lipsitch, M., Tchetgen Tchetgen, E., & Cohen, T. (2010). Negative controls: A tool for detecting confounding and bias in observational studies. *Epidemiology (Cambridge, Mass.)*, *21*(3), 383–388. https://doi.org/10.1097/EDE.0b013e3181d61eeb
25. Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231–245. https://doi.org/10.1007/s11896-019-09334-5
26. Oster, E. (2019). Unobservable selection and coefficient stability: Theory and evidence. *Journal of Business & Economic Statistics*, *37*(2), 187–204. https://doi.org/10.1080/07350015.2016.1227711
27. Payment Systems Regulator (2023, June). *Fighting authorised push payment fraud: A new reimbursement requirement* (Policy Statement PS23/3). https://www.psr.org.uk/media/rxtlt2k4/ps23-3-app-fraud-reimbursement-policy-statement-june-2023.pdf
28. Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296. https://doi.org/10.1177/0022427810365903
29. Raval, D. (2021). Who is victimized by fraud? Evidence from consumer protection cases. *Journal of Consumer Policy*, *44*(1), 43–72. https://doi.org/10.1007/s10603-020-09466-w
30. Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, *7*(1). Article 5. https://doi.org/10.1186/s40163-018-0079-3
31. Regulation, E. U. 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro. (2024). *Official Journal of the European Union*, L, 2024886. https://eur-lex.europa.eu/eli/reg/2024/886/oj
32. Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238. https://doi.org/10.1177/0022427811425539

33. Robb, C. A., & Wendel, S. (2023). Who can you trust? Assessing vulnerability to digital imposter scams. *Journal of Consumer Policy*, *46*(1), 27–51. https://doi.org/10.1007/s10603-022-09531-6
34. Robins, J. M., Rotnitzky, A., & Zhao, L. P. (1994). Estimation of regression coefficients when some regressors are not always observed. *Journal of the American Statistical Association*, *89*(427), 846–866. https://doi.org/10.1080/01621459.1994.10476818
35. Roodman, D., Nielsen, M. Ø., MacKinnon, J. G., & Webb, M. D. (2019). Fast and wild: Bootstrap inference in Stata using boottest. *The Stata Journal*, *19*(1), 4–60. https://doi.org/10.1177/1536867X19830877
36. Seldal, M. M. N., & Nyhus, E. K. (2022). Financial vulnerability, financial literacy, and the use of digital payment technologies. *Journal of Consumer Policy*, *45*(2), 281–306. https://doi.org/10.1007/s10603-022-09512-9
37. Simonsohn, U., Simmons, J. P., & Nelson, L. D. (2020). Specification curve analysis. *Nature Human Behaviour*, *4*(11), 1208–1214. https://doi.org/10.1038/s41562-020-0912-z
38. Solon, G., Haider, S. J., & Wooldridge, J. M. (2015). What are we weighting for? *Journal of Human Resources*, *50*(2), 301–316. https://doi.org/10.3368/jhr.50.2.301
39. Suri, T., & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. *Science*, *354*(6317), 1288–1292. https://doi.org/10.1126/science.aah5309
40. Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. *Crime & Delinquency*, *41*(1), 54–72. https://doi.org/10.1177/0011128795041001004
41. van Wilsem, J. (2013). Bought it, but never got it': Assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178. https://doi.org/10.1093/esr/jcr053
42. VanderWeele, T. J., & Ding, P. (2017). Sensitivity analysis in observational research: Introducing the E-value. *Annals of Internal Medicine*, *167*(4), 268–274. https://doi.org/10.7326/M16-2607
43. Vik, P. M., Kamerāde, D., & Dayson, K. T. (2024). The link between digital skills and financial inclusion—Evidence from consumers survey data from low-income areas. *Journal of Consumer Policy*, *47*(3), 373–393. https://doi.org/10.1007/s10603-024-09567-w
44. Waschka, L., & Cunha, M. (2026). Reducing consumer fraud and scam victimization through incubation. *Journal of Consumer Policy*, *49*(2). Article 15. https://doi.org/10.1007/s10603-026-09619-3
45. Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095
46. Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Figures

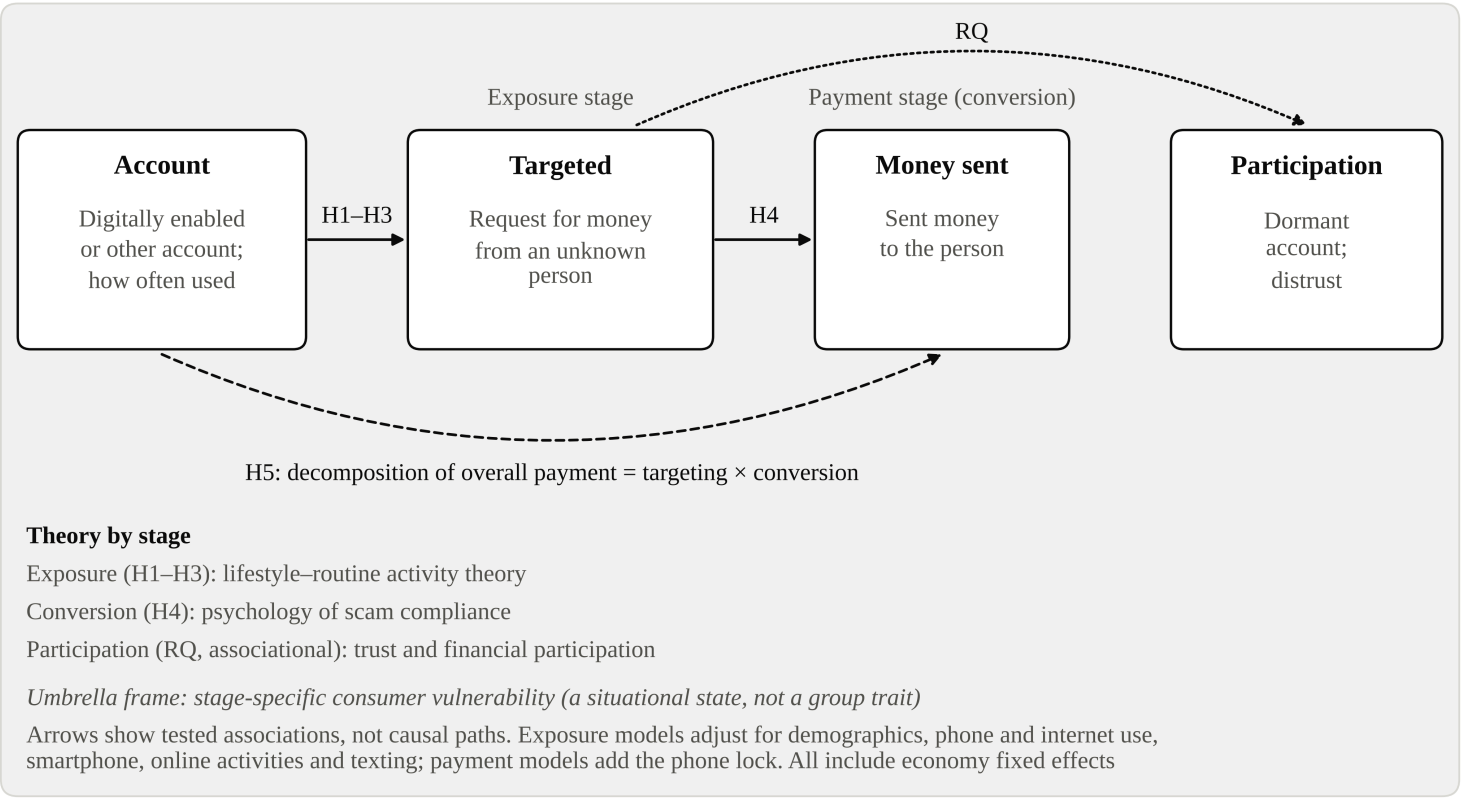


Figure 1

Conceptual framework. Holding an account is linked to sending money in response to an unsolicited request through being targeted (exposure, H1–H3) and paying once targeted (conversion, H4); payment among all phone owners combines the two margins and is decomposed under H5. The research question (RQ) concerns the association of being targeted with account participation. Arrows denote tested associations, not causal effects

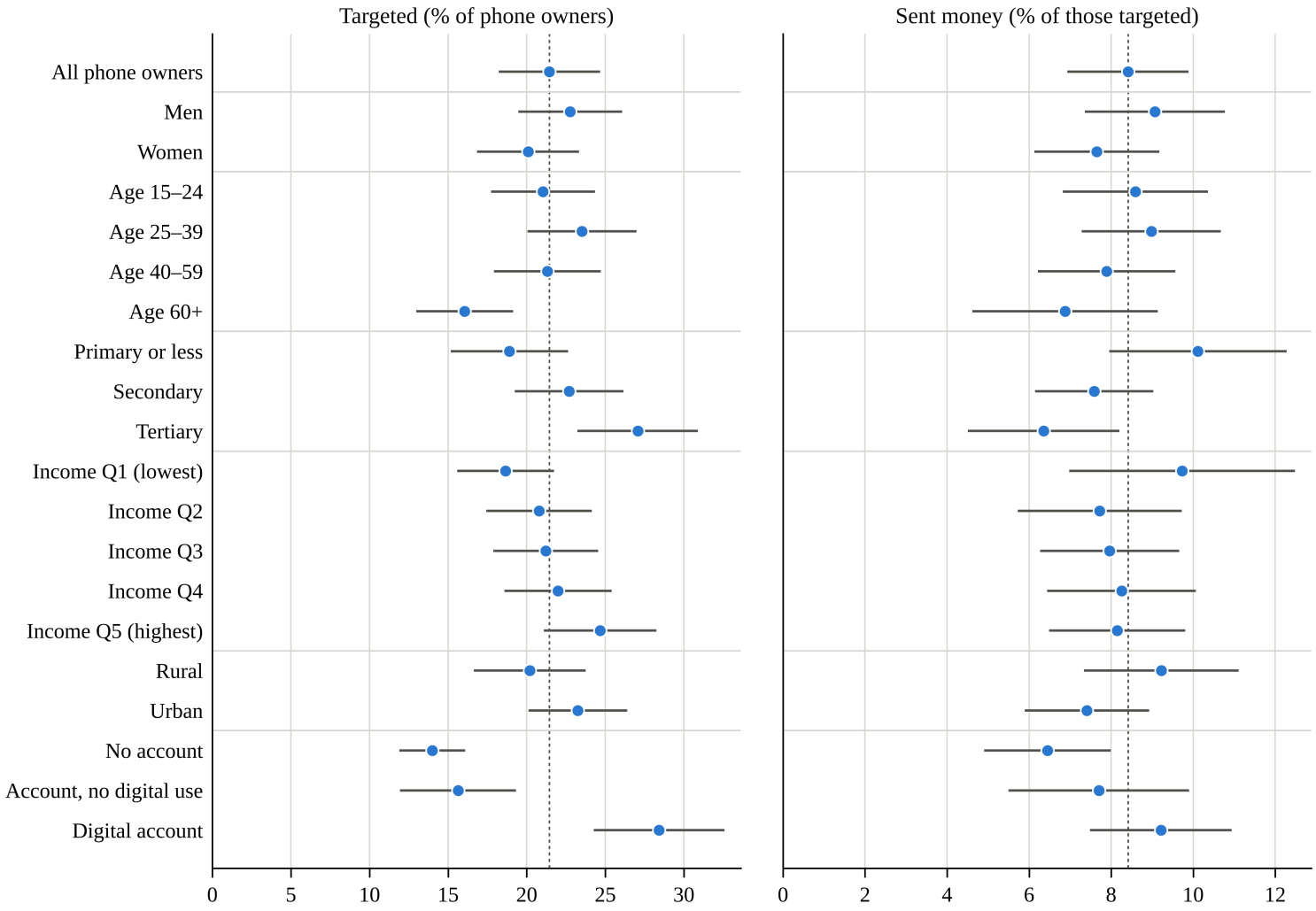


Figure 2

Unadjusted share of phone owners targeted by an unsolicited request for money, and share of the targeted who sent money, by group. Survey-weighted percentages with economy-clustered 95% confidence intervals, using all valid responses for each outcome; the dotted line marks the overall rate

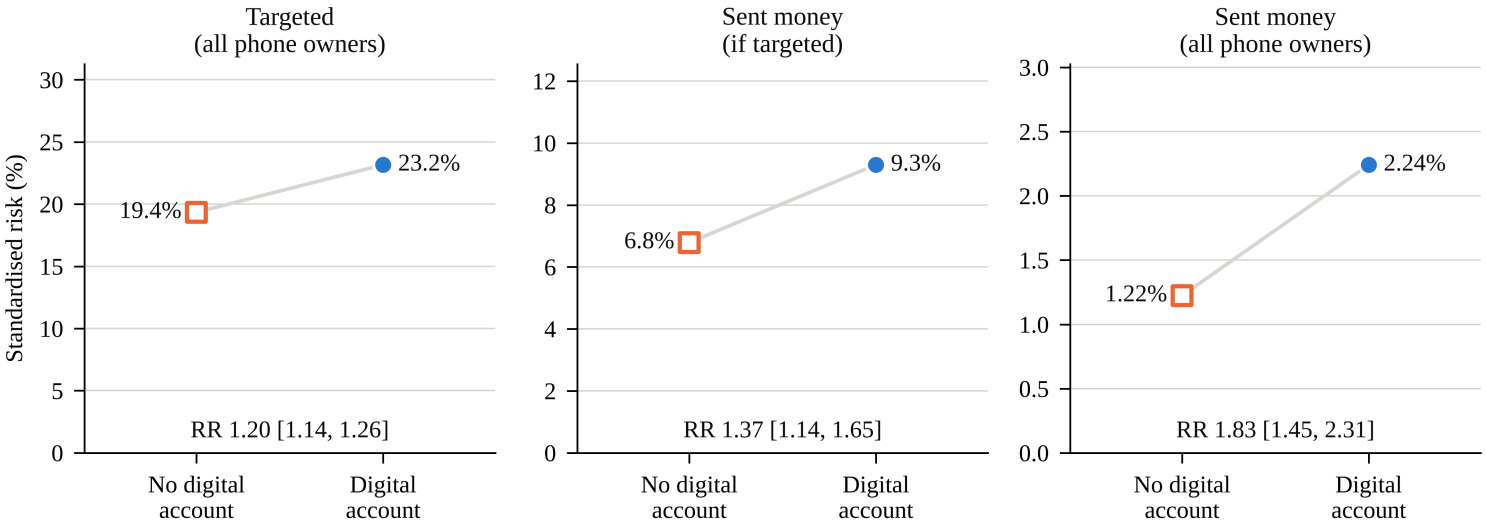


Figure 3

Adjusted, marginally standardised probability of being targeted and of sending money, by digitally enabled account ownership. Survey-weighted logit models with economy fixed effects and all controls; risk ratios with economy-clustered 95% confidence intervals. The comparison group includes adults with accounts not used for digital payments; vertical scales differ across panels

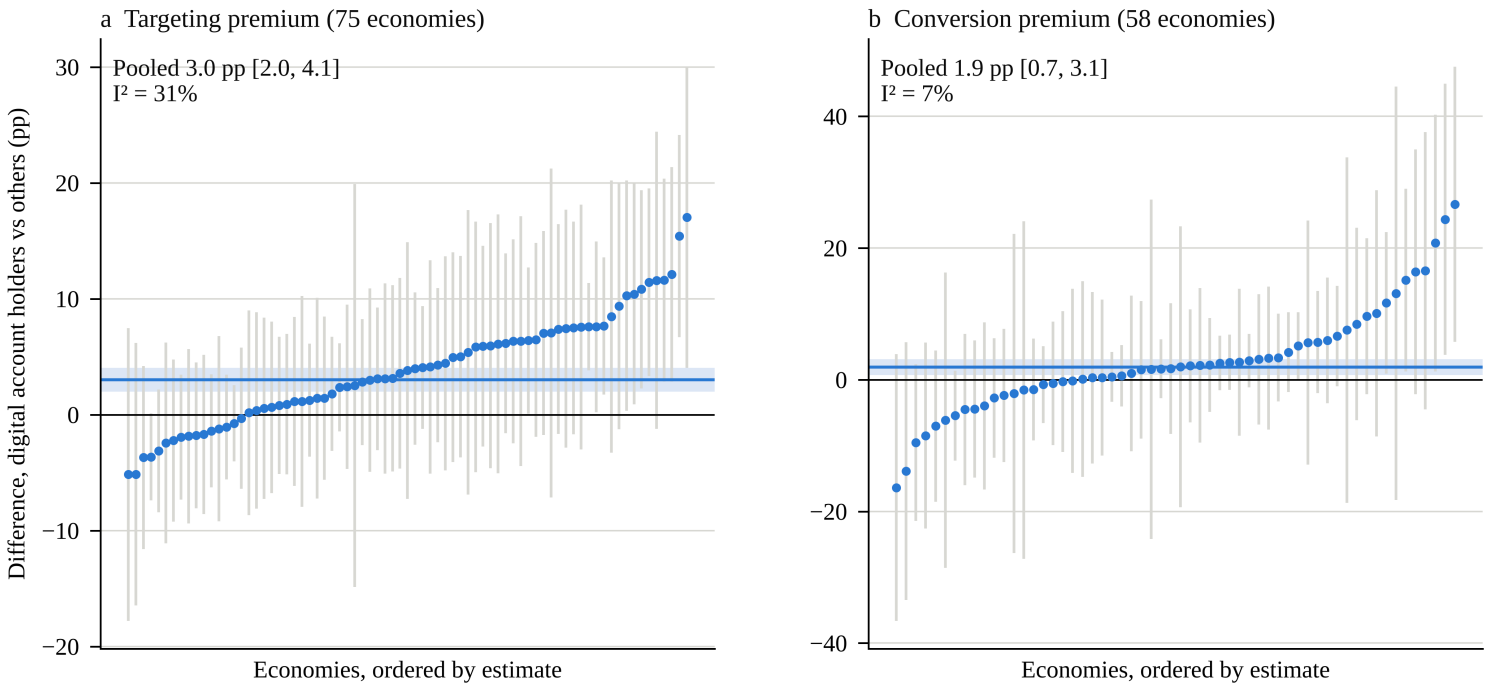


Figure 4

Digitally enabled account premium by economy: a targeting, b conversion. Within-economy differences in percentage points from weighted linear probability models with the main controls and 95% confidence intervals, ordered by estimate. The blue line and band show the random-effects pooled estimate and its 95% confidence interval

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- JCPOnlineResource1.docx
- JCPOnlineResource2.zip