

European Journal of Information and Knowledge Management (EJIKM)

**Recipient Information and Horizontal Relational Trust in
Platform-Mediated P2P Payments**



**CARI
Journals**

Recipient Information and Horizontal Relational Trust in Platform-Mediated P2P Payments



Theo Okafor, PhD.,

Vienna, Austria.

<https://orcid.org/0009-0007-3867-1431>

Accepted: 24th Aug, 2026, Received in Revised Form: 9th Sep, 2026, Published: 21st Sep, 2026



Abstract

Purpose: This study examines how users combine platform-generated recipient information with relational knowledge when assessing recipients, managing uncertainty and responding to problems in platform-mediated P2P payments.

Method: An exploratory cross-sectional survey produced 30 usable responses from PayPal, Revolut, Zelle and Wise users in North America and Europe. Closed-ended responses were analysed using descriptive statistics, while open-text responses were examined through framework analysis organised around assessment, action and resolution.

Findings: Respondents placed greatest weight on personal familiarity and previous successful payments when assessing recipients. Checking recipient identifiers was the most commonly reported protective action, whereas mutual contacts and test payments were used less often. Seventeen respondents reported at least one payment problem. Direct recipient contact and platform dispute procedures were the most common initial responses. Respondents expressed greater confidence in payment processing than in recovery rights or regulatory ordinance.

Unique Contribution to Theory, Practice, and Policy: The study treats recipient assessment as an information practice involving platform-generated identifiers, transaction records, interpersonal knowledge and external communication. It shows how horizontal relational trust may complement institutional assurance rather than replace it. The findings support clearer recipient information, verification tools, transaction warnings, privacy controls and dispute information. Claims remain limited by the small, non-probability sample and reliance on self-reported practices.

Keywords: *P2P Payments, Recipient Information, Horizontal Relational Trust, Platform Trust, Payment Verification*

1.1 Background and Context

Before completing a P2P payment, users judge whether recipient information is sufficient, consistent and credible, drawing on platform identifiers, past transactions, interpersonal knowledge and outside communication. Applications support reimbursing friends, splitting expenses, sending money to relatives, informal purchases and international transfers. US research estimates 69% of households used P2P in the previous year, 40% at least monthly (Hammerslough & Celik, 2026), while Visa's 2025 survey found 67% preferred digital transfers to a bank account via an application, citing speed, predictability, transparency and perceived security (Visa, 2025).

Revolut, PayPal, Zelle and Wise differ in coverage, account structure, funding, routing and purpose. Wise and Revolut support international and multi-currency transfers; PayPal combines personal and commercial payments; Zelle operates through US banks and credit unions (Center Forward, 2025). Revolut's licensed-bank status in 30 countries by end-2025 shows that a direct-looking mobile transfer may rest on extensive institutional structure (Revolut Group Holdings Ltd., 2026).

These services are not uniformly social networks. Their social character lies in the relationships surrounding payments: names, contact details, messages and past transactions gain meaning through family, friendship, employment, commercial or group ties. Platform-mediated P2P is used without assuming identical social or technical functions.

Directness does not remove financial intermediation. Transactions depend on providers, banks, card networks, account-to-account rails, identity checks, monitoring, contracts and regulation (Boston Consulting Group, 2025; The Payments Association, 2025). Authentication, fraud warnings, records and dispute procedures may support confidence, though users may focus more on recipient identity and existing relationships (Ghosh et al., 2025; Tan et al., 2025).

Although the theoretical discussion addresses platform-mediated P2P payments broadly, the empirical study covers only respondents in Europe and North America. Findings describe reported trust practices in this two-region sample and are not representative of either regional population or P2P users elsewhere.

1.2 Problem Statement and Research Gap

Digital-payment research links trust to platform adoption and use (Ghosh et al., 2025; Mombeuil & Jean Pierre, 2026; Tan et al., 2025), not recipient assessment. Provider and counterparty trust differ where users may trust the provider to process payments yet remain uncertain about the recipient, drawing on platform and relational cues. Limited evidence explains how users combine these when assessing recipients or managing uncertainty (Blanco-Oliver et al., 2025; Kiernan & Guzman, 2026; Zhang & Kim, 2025), a gap relevant to fraud (Center Forward, 2025; Federal Reserve Financial Services, 2026). This study addresses the gap through horizontal relational trust, defined as trust in another participant informed by recipient information, relational history, external communication, reciprocity and expected accountability. Reported practices are classified as assessment, action and resolution. These

domains organise retrospective survey responses rather than describe an observed sequence, and the study examines how respondents in Europe and North America use platform and relational information to assess recipients, manage uncertainty and respond to payment problems.

1.3 Relevance of the Study

This study distinguishes trust in a payment service from trust in the recipient. Existing research explains adoption, continued use and switching more readily than recipient-specific judgement (Ghosh et al., 2025; Mombeuil & Jean Pierre, 2026; Tan et al., 2025). It addresses this gap through horizontal relational trust, defined as willingness to accept payment-related vulnerability based partly on familiarity, previous exchanges, external confirmation, shared contacts and expected accountability.

From an information-management standpoint, recipient assessment involves selecting and interpreting information from several sources. Users may combine platform-generated identifiers and transaction records with relational knowledge and communication outside the payment service. The assessment-action-resolution framework classifies how this information enters reported payment practices without presenting the domains as an observed sequence.

The findings may inform the design of recipient information, verification tools, payment warnings, privacy controls and dispute procedures. These contributions remain limited by the small, non-representative sample, its restriction to Europe and North America, the cross-sectional design and reliance on self-reported behaviour.

2. Literature Review

2.1 Institutional, System and Platform Trust

Trust in platform-mediated payments operates at several levels. Institutional trust is about confidence in banks, regulators, legal rules and payment providers. Structural assurance arises from formal safeguards such as authentication, fraud monitoring, regulatory supervision, contractual protection and dispute procedures. Policy and technical safeguards can support trust even when users do not consciously assess them during each transaction (Shao et al., 2025).

System trust concerns confidence that the wider payment infrastructure will process transfers accurately, protect account information and maintain reliable transaction records. Users may hold this confidence without detailed knowledge of the banks, networks and technical systems involved. This matters because payment platforms, account-to-account networks and regulated financial institutions remain interconnected (Boston Consulting Group, 2025).

Platform trust is directed towards the service provider. For Revolut, PayPal, Zelle and Wise, it may depend on perceived security, reliability, transparency and responsiveness. These forms of trust overlap but are not interchangeable. A user may trust the payment infrastructure while distrusting a provider or recipient. Together, institutional, system and platform trust form the vertical assurance within which interpersonal payment decisions occur.

2.2 Interpersonal and Horizontal Relational Trust

Interpersonal trust concerns a person's willingness to accept vulnerability based on the expectation that another party will act responsibly. In P2P payments, this trust is directed towards the recipient rather than the payment provider. A user may trust Revolut, PayPal, Zelle or Wise to process a transfer accurately while remaining uncertain about the recipient's identity, intentions or willingness to correct an error. Platform trust and interpersonal trust are therefore distinct, even when both influence the same payment decision. Users may assess recipients through familiarity, previous payments, continued contact, mutual acquaintances and expectations of reciprocity. Research indicates that social-network support and tie strength can influence P2P payment use through trust, while perceived cybersecurity may affect this relationship (Wisker & Alani, 2026). Social influence has also been associated with P2P payment acceptance alongside perceived risk, platform trust and service quality (Aasheim & Wimmer, 2026).

Horizontal relational trust extends interpersonal trust by locating the payment within a wider network of relationships. It refers to willingness to accept payment-related vulnerability based partly on relational history, shared contacts, group membership, anticipated future interaction and expected accountability. Misconduct may carry interpersonal or reputational consequences within that network. Horizontal relational trust is not necessarily protective. Familiarity and strong ties may support verification and repayment, but they may also create false confidence or pressure to comply. It should therefore be treated as a socially informed basis for payment decisions rather than proof that a recipient is dependable.

2.3 Coexistence of Horizontal and Vertical Assurance

Horizontal and vertical assurance are related rather than competing sources of trust. Vertical assurance arises from regulatory, contractual, institutional and technical safeguards. Horizontal assurance rests on the payer-recipient relationship, including prior conduct, reciprocity, shared contacts and expected social accountability. A user may therefore trust the service to process a payment while relying on the recipient to fulfil an agreement or return money sent in error.

Recent research supports this interaction. Institution-based trust has been associated with continued platform use, particularly where users judge reliability through previous experience (Mombeuil & Jean Pierre, 2026). Social-network support and tie strength may also affect payment intentions through trust, with perceived cybersecurity influencing this relationship (Wisker & Alani, 2026). The relative importance of each form of assurance may vary by situation. Familiarity and previous exchanges may dominate routine payments to known recipients. Following an error or dispute, users may turn to transaction records, customer support, banks or formal complaint procedures. Institutional assurance may therefore remain in the background during routine use and become more visible when interpersonal resolution fails.

Neither form fully replaces the other. Relational familiarity offers no certain remedy for deception, account compromise or refused repayment. Formal controls may confirm that a transfer was authorised without determining whether the recipient acted fairly. Horizontal and

vertical assurance address different payment risks and may supplement, obscure or conflict with each other.

2.4 Social Cues and User Judgement Information

Platform-mediated payments require recipient assessment from limited information. Revolut, PayPal, Zelle and Wise may display names, account identifiers, contact details, profile information or past transactions. These cues aid identification, but their meaning depends on relational and transaction context. Research links digital-payment trust to security, social influence, prior experience and grievance procedures, but these do not prove recipient dependability (Aljaradat & Shukla, 2025; Tan et al., 2025). Identity and trust differ. A matching name or number may confirm account ownership, not honest conduct. Such details become relational signals when linked to past payments, saved contacts, shared relationships or prior communication. Consistent information may reduce uncertainty, but familiar identifiers can be copied, accounts compromised and messages crafted to imitate known contacts. Risk reporting identifies impersonation, credential compromise, account takeover and social engineering as recurring threats (Federal Reserve Financial Services, 2026; The Payments Association, 2025).

Previous transactions and personal relationships also inform judgement: successful exchanges may reduce later verification, while continued contact may create informal accountability. Friends, relatives, colleagues and shared groups can influence payment behaviour, though familiarity may also produce false confidence or pressure to comply (Blanco-Oliver et al., 2025; Zhang & Kim, 2025). Payment completion may thus reflect trust, habit, obligation or convenience. Users may verify requests outside the platform through calls, messaging, earlier payment details or mutual contacts. Labels such as “rent” or “invoice” can link a request to a known obligation, while unexpected urgency or changed details may prompt further checking.

Visibility raises further concerns where observable payment activity may affect conduct through peer comparison and impression management, though such functions differ across the four services (Kiernan & Guzman, 2026). Social information can also expose contacts, relationships and transactions. PayPal, for example, collects profile, contact, linked-account and transaction data, some visible to other users depending on account settings (PayPal, 2026). Social cues are therefore aids to judgement, not objective evidence of trustworthiness. Their weight depends on familiarity, prior experience, payment purpose, transaction value and the perceived consequences of refusing or proceeding.

2.5 Relational Networks, Reciprocity and Accountability

P2P payments transactions often happen within family, friendship, small business or group relationships. These networks provide information about a recipient’s previous conduct and likely response to a problem. Social-network support and tie strength may influence P2P payment use through trust, while perceived cybersecurity can affect this relationship (Wisker & Alani, 2026). Social influence has also been associated with payment acceptance alongside perceived risk, service quality and platform trust (Aasheim & Wimmer, 2026). Reciprocity may increase confidence where users expect recipients to acknowledge payments, meet later obligations or return funds sent in error. Continued interaction can also create informal

accountability because misconduct may affect the recipient's reputation within a shared network. However, relational ties can constrain judgement. Requests from friends, relatives or colleagues may be difficult to refuse despite uncertainty. Horizontal accountability therefore relies on reciprocity, reputation and social consequences rather than contractual enforcement. Its influence may vary according to relationship strength, transaction value, network visibility and the likelihood of future interaction.

2.6 Privacy, Social Pressure and Deception Risks

Relational information can support recipient identification while creating privacy risks. Names, contact details, profile information, payment references and transaction records may disclose relationships or activities beyond what is needed to complete a transfer. PayPal, for example, states that it collects contact, profile, linked-account and transaction information. Depending on account settings, selected information may be visible to other users or disclosed to parties involved in processing the transaction (PayPal, 2026). Social relationships may also pressure users to proceed. Refusing a request from a friend, relative or colleague can produce embarrassment, conflict or reputational cost. Payment visibility may similarly affect behaviour through peer observation and impression management (Kiernan & Guzman, 2026). Payment completion should therefore not always be interpreted as evidence of trust; it may reflect obligation or conformity.

Deception can exploit the same cues. Impersonators may use familiar names, urgent messages or claims of institutional authority to induce authorised transfers. Imposter scams generated reported losses of USD 3.5 billion in 2025, while payment-risk reporting continues to identify impersonation, social engineering and credential compromise as recurring threats (Federal Trade Commission, 2026; Federal Reserve Financial Services, 2026). Relational cues may therefore assist verification while also producing false confidence.

2.7 Trust across Transaction Information

Trust in P2P payments can be examined through three related analytical domains. **Assessment** concerns the recipient identifiers, previous transactions, relational history and payment purpose that users may consider. Social ties may increase confidence, although their influence can vary with perceived cybersecurity and transaction context (Wisker & Alani, 2026). **Action** concerns reported responses to recipient uncertainty. Users may proceed, seek confirmation through another communication channel, delay or reduce the payment, use another method, or refuse the transfer. These responses merit attention because authorised P2P payments may be difficult to recover, particularly where deception led the user to approve the transaction (Center Forward, 2025). **Resolution** concerns reported responses to delayed, misdirected, disputed, or deceptive payments. These may include contacting the recipient, involving a mutual contact, approaching a bank, or using the provider's dispute procedures. Assessment, action and resolution are treated as related domains rather than sequential phases. The survey compares respondents' retrospective accounts within each domain but does not observe individual transactions or changes in trust over time.

2.8 Research Gap and Proposed Framework

P2P payment research mainly examines adoption, continued use, switching intentions, perceived security and trust in service providers (Aasheim & Wimmer, 2026; Mombeuil & Jean Pierre, 2026). Although social influence and network ties have received attention, less is known about the recipient-specific cues users consider, their responses to uncertainty and the mechanisms used after payment problems. Existing studies also do not always distinguish trust in the platform from trust in the counterparty (Wisker & Alani, 2026).

This study addresses that gap through an **assessment-action-resolution framework**. **Assessment** covers reported reliance on identity information, familiarity, previous payments, shared contacts and external confirmation. **Action** includes verification, delay, modification, completion, or refusal. **Resolution** includes reported interpersonal, platform-based and banking responses to payment problems. The framework classifies questionnaire responses rather than modelling a sequential process. The cross-sectional data permit comparison of reported practices across the three domains but cannot establish temporal progression, trust repair, or causal effects of payment problems on subsequent behaviour. Horizontal relational trust is therefore examined alongside institutional and technical assurance within the limits of retrospective self-reporting.

3. Methodology

3.1 Research Design

This study adopted an exploratory cross-sectional survey design. The questionnaire combined categorical, ordinal, multiple-response and open-text items to examine recipient assessment, action under uncertainty, responses to payment problems, platform trust and privacy concerns. Closed-ended responses were used to identify descriptive patterns within the sample, while open-text responses provided contextual explanations of recipient trustworthiness, payment uncertainty, dispute resolution and trust in payment providers. The study was exploratory because it examined reported practices and applied the assessment-action-resolution framework rather than testing causal relationships or estimating population parameters. Data were collected at one point in time and relied on respondents' recollections and self-reported behaviour. The design therefore cannot establish causality, directly observe payment decisions, or determine how individual trust judgements developed or changed over time.

3.2 Case Scope and Platform Selection

The study included Revolut, PayPal, Zelle and Wise as examples of platform-mediated P2P payment services. These services differ in geographical coverage, payment routing, account structure, recipient information and dispute procedures. They were therefore neither treated as functionally equivalent nor classified uniformly as social networks. The analysis considered information available within each service alongside interpersonal relationships, shared contacts and communication outside the payment interface. The primary platform was treated as a contextual variable rather than as a basis for platform-wide conclusions. The empirical scope was limited to Europe and North America, where, of the 30 respondents, 17 resided in North

America and 13 in Europe. The findings therefore describe reported payment practices within this two-region sample. They do not represent the wider populations of either region or support reliable regional comparisons.

3.3 Sampling and Participant Recruitment

Non-probability purposive convenience sampling was used to recruit adults with relevant experience of platform-mediated P2P payments. Eligibility required respondents to be at least 18 years old and to have used Revolut, PayPal, Zelle, or Wise for personal payments during the preceding six months. The questionnaire link was distributed directly to known users and posted on an online forum with a public invitation to participate. Recruitment sought variation in age, gender, region, education, transaction frequency and primary platform.

Data collection ended after 31 submissions were received as one submission was excluded because it contained comments unrelated to the study, leaving 30 usable responses. The sample was considered adequate for the study's exploratory and descriptive purpose because it included users of all four services, respondents from Europe and North America and variation across demographic and usage characteristics. Adequacy was judged against the study's defined scope, participant relevance, data coverage and descriptive analytical approach rather than through statistical power calculations. Platform and regional comparisons were therefore interpreted descriptively rather than as statistically generalisable differences.

3.4 Questionnaire Design and Data Collection

Data were collected via Google Forms in 2026. Screening required respondents to be at least 18 and to have used Revolut, PayPal, Zelle or Wise for personal P2P payments in the previous six months. It covered six areas: service trust, recipient assessment, uncertainty, problems and resolution, platform functions and privacy, and written explanations. Grids addressed platform assurance, recipient cues and protective actions; checkboxes covered problems and dispute mechanisms; open-text items covered trust cues, uncertainty and resolution. A five-user pilot assessed clarity, options, routing and time. Wording was revised, duplicates removed, and pilot responses excluded. Completion took under ten minutes. No names, emails, account details, transaction references or screenshots were collected.

3.5 Data Analysis

Data was organised in Microsoft Excel and analysed in R 4.5.1 (RStudio). Excel supported coding and summary tables. Categorical responses were summarised as frequencies and percentages, with raw counts reported. Ordinal and multiple-response items were summarised by distribution and applicable respondent counts. Cross-tabulations covered primary platform, payment frequency, recipient verification, uncertainty, previous problems and resolution. Revolut, PayPal, Zelle and Wise comparisons were descriptive only, with no causal or population-level claims. Open-text responses underwent framework analysis using assessment-action-resolution categories, revised as needed. Contrary and overlapping responses were retained, and responses could fit multiple categories. A respondent-level matrix linked closed

answers with written explanations. Results used Excel frequency tables and R bar charts; cross-platform visuals appeared only where subgroup sizes allowed cautious interpretation.

3.6 Research Quality and Researcher Reflexivity

Research quality was supported through transparent documentation of questionnaire development, data processing and analysis. Items were mapped to the research questions and the analytical domains of assessment, action and resolution. Consistent rules were applied to missing, contradictory and multiple-response data. A coding record documented the analysis of open-text responses, including changes to categories and the reasons for those changes. Responses that contradicted or extended the proposed framework were retained. Closed-ended responses were compared with written explanations without treating either as inherently more accurate. Reflexive notes recorded assumptions concerning horizontal relational trust and institutional assurance, including their possible influence on questionnaire design, coding and interpretation. The analysis also considered the limits of self-reported data, including recall error, social-desirability bias and differences between reported practices and actual transactional behaviour.

3.7 Ethical Considerations

Participants read an information statement, confirmed they were at least 18-year-old and consented voluntarily. They were informed not to provide personal, financial or third-party identifiers. Open-text answers were checked and identifying details removed. Data were stored in a protected, researcher-only Google Drive account and no retention or deletion period was set.

4. Findings and Discussion

4.1 Respondent and Platform Profile

The survey produced 30 usable responses in which all respondents were at least 18 years old and had used PayPal, Revolut, Zelle or Wise for a personal P2P payment during the preceding six months from the time they responded. Table 1 summarises the sample.

Table 1: Respondent characteristics (n = 30)

Characteristic	Category	n	%
Gender	Female / Male / Non-binary	13 / 13 / 4	43.3 / 43.3 / 13.3
		8 / 11 / 6 /	26.7 / 36.7 / 20.0 /
Age group	18–24 / 25–34 / 35–44 / 45–54 / 55+	3 / 2	10.0 / 6.7
Region	Europe / North America	13 / 17	43.3 / 56.7
	Secondary / Vocational	5 / 5 / 15 /	16.7 / 16.7 / 50.0 /
Education	Undergraduate / Postgraduate	5	16.7
		8 / 8 / 7 /	26.7 / 26.7 / 23.3 /
Primary platform	PayPal / Revolut / Zelle / Wise	7	23.3
Payment		6 / 12 / 10	20.0 / 40.0 / 33.3 /
frequency	1–5 / 6–15 / 16–30 / >30	/ 2	6.7

The respondents were drawn from two regions where seventeen (56.7%) from North America and 13 (43.3%) in Europe. The sample therefore provides relatively balanced regional coverage, though it was not constructed through regional quotas or probability-based selection. Figure 1 shows a relatively even distribution across the four payment services. PayPal and Revolut were each used primarily by eight respondents, while Zelle and Wise were each selected by seven. This distribution arose from recruitment rather than stratified sampling and does not reflect the services' market shares.

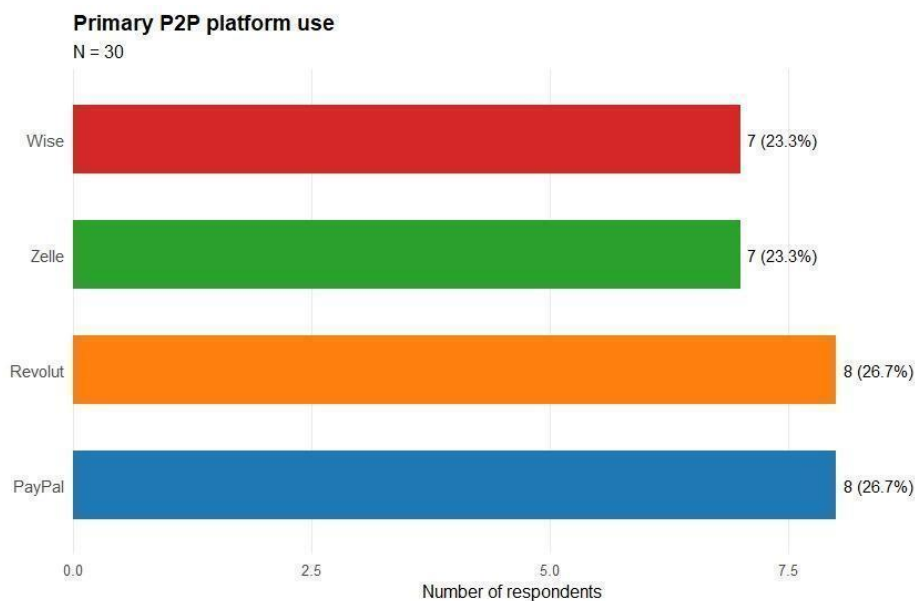


Figure 1: Primary platform use

Most respondents reported moderate payment activity. Twelve had made between six and 15 payments during the preceding six months, while ten had made between 16 and 30. Six reported between one and five payments and two reported more than 30. The sample was recruited through known users and an online forum rather than probability-based selection. Findings therefore describe patterns among these 30 respondents and cannot be generalised statistically. Platform comparisons also remain descriptive because each subgroup contained only seven or eight respondents. Rather, the distribution provides a basis for examining reported differences in platform trust, recipient assessment, action under uncertainty and problem resolution.

4.2 Platform Trust and Institutional Assurance

Figure 2 presents responses to five statements concerning platform accuracy, data protection, remedial support, payment recovery and regulatory awareness. Confidence was strongest in routine platform operation. Twenty-two respondents (73.3%) agreed or strongly agreed that their service processed payments accurately, while 21 (70.0%) expressed confidence in the protection of payment and account information.

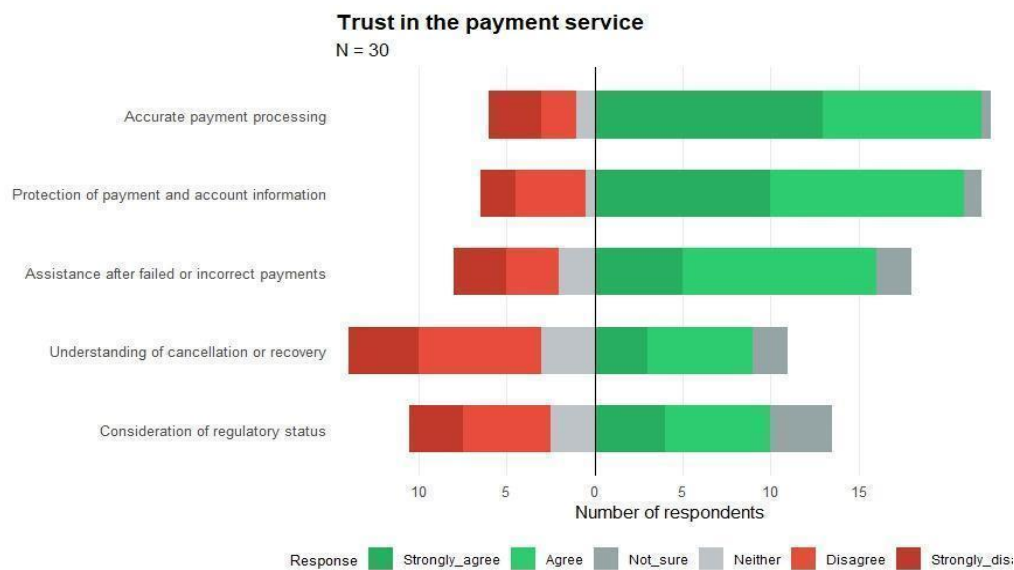


Figure 2: Distribution of responses on platform trust and institutional assurance, with disagreement shown to the left and agreement to the right.

Confidence weakened when respondents considered problems and remedies. Sixteen respondents (53.3%) expected assistance following a failed or incorrect payment, compared with six (20.0%) who disagreed. Knowledge of cancellation or recovery was lower: nine respondents (30.0%) reported understanding these conditions, while 11 (36.7%) disagreed and ten (33.3%) were neutral or unsure. Regulatory awareness followed a similar pattern. Ten respondents (33.3%) considered regulatory status or banking licences when using their primary service. Eight (26.7%) did not, while 12 (40.0%) were neutral or unsure.

The results indicate a distinction between operational confidence and awareness of institutional protection. Respondents generally trusted their service to complete routine payments securely, but were less certain about recovery rights, remedial support and regulatory arrangements. This suggests that vertical assurance remained present but was less visible in respondents' reported use than the platform's immediate operational performance. Neutral and uncertain responses indicate limited awareness rather than necessarily active distrust.

4.3 Recipient Assessment

Figure 3 presents the weight respondents assigned to eight factors when assessing a payment recipient. Personal familiarity received the greatest weight: 17 respondents (56.7%) rated it as a major factor and seven (23.3%) as a moderate factor. Previous successful payments followed, with 13 respondents (43.3%) rating them as a major factor and nine (30.0%) as a moderate factor.

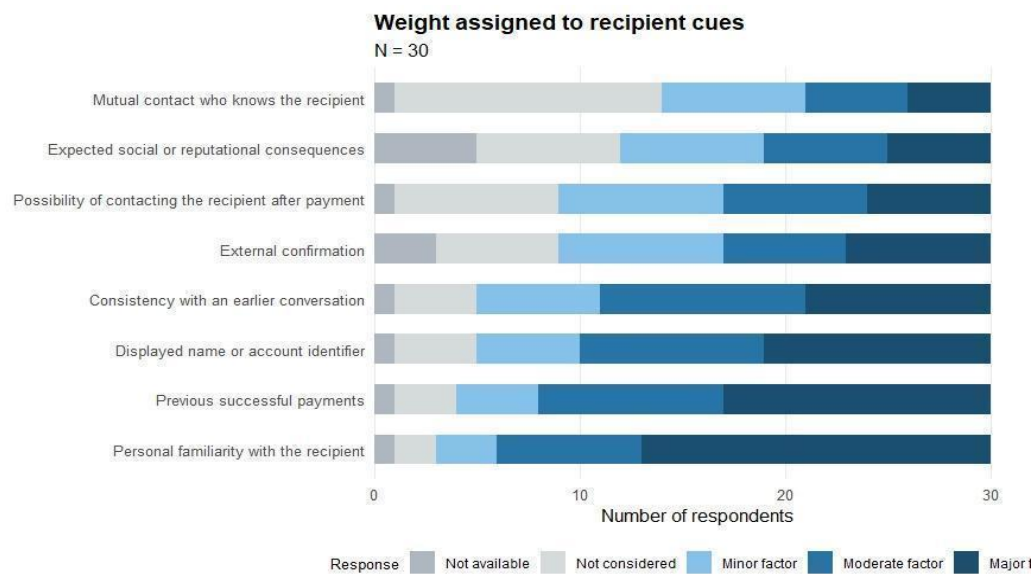


Figure 3: Weight assigned to recipient cues for assessing a payment

The recipient's displayed name or account identifier was also widely considered. Eleven respondents (36.7%) rated it as a major factor and nine (30.0%) as a moderate factor. Consistency with an earlier conversation received similar support, with nine respondents (30.0%) assigning it major weight and ten (33.3%) moderate weight. These cues appear to support recognition and verification when combined with prior knowledge. Indirect social cues carried less weight. Mutual contacts were rated as a major factor by four respondents (13.3%), while 13 (43.3%) did not consider them. Expected social or reputational consequences were a major factor for five respondents (16.7%), while 11 (36.7%) marked them as unconsidered or unavailable.

Table 2: Greatest influence on recipient assessment

Factor	n	%
Personal familiarity with the recipient	11	36.7
Previous successful payments	6	20
Matching recipient identity details	5	16.7
Confirmation outside the payment service	4	13.3
The stated purpose of the payment	2	6.7
The amount being transferred	1	3.3
The recipient's displayed name or account identifier	1	3.3

The results show a hierarchy in recipient assessment. Direct familiarity and previous payment experience were weighted more heavily than mutual contacts or reputational consequences. Platform-supplied identity information occupied a supporting position. Table 2 confirms this pattern: personal familiarity was most often selected as the greatest influence, followed by

previous successful payments and matching recipient details. The findings indicate reported reliance on direct relational knowledge rather than broad community endorsement.

4.4 Action under Information Uncertainty

Figure 4 presents the actions respondents reported taking when dealing with unfamiliar recipients or unusual payment requests. Checking the recipient's information such as name and account identifier was the most common practice, with 22 respondents (73.3%) doing so always or often. External confirmation was less consistent: 12 respondents (40.0%) contacted the recipient through another channel always or often, while nine (30.0%) did so rarely or never.

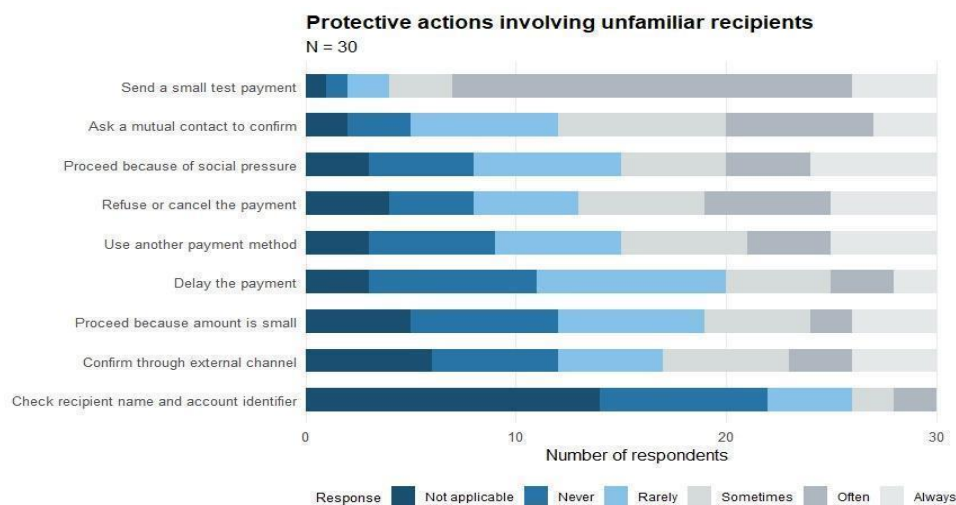


Figure 4: Protective actions involving unfamiliar recipients

More demanding or socially mediated checks were uncommon. Five respondents (16.7%) regularly consulted a mutual contact and only two (6.7%) regularly sent a test payment. By contrast, 11 respondents (36.7%) frequently delayed payment while seeking further information. Nine (30.0%) commonly used another payment method, while eight (26.7%) frequently refused or cancelled a payment. Not all uncertainty produced protective action. Twelve respondents (40.0%) reported proceeding always or often when the amount was small. Eight (26.7%) proceeded because of social pressure or obligation, with a further seven (23.3%) doing so sometimes. These responses distinguish trust from calculated risk acceptance and socially constrained compliance.

Table 3: Behavioural changes caused by uncertainty

Reported action	Number selecting	Percentage of respondents
I now check recipient details more carefully	14	46.7
I avoid paying unfamiliar recipients	12	40
I use a different payment service	3	10
I delay or pause payments more often	3	10
It did not change my behaviour	4	13.3

Note: Respondents could select more than one option, so, percentages do not sum to 100%.

Table 3 shows the broader behavioural changes associated with recipient uncertainty. As respondents could select several options, percentages do not total 100%. Overall, respondents relied more on direct identity checks and personal communication than on mutual contacts or test payments. The findings also show that payment completion did not necessarily indicate trust, since some respondents proceeded because the potential loss was limited or refusal carried a perceived social cost. These results concern self-reported practices rather than observed transactions.

4.5 Payment Problems and Resolution

Out of the 30 respondents, 17 reported at least one P2P payment problem. As shown in Figure 5, suspected impersonation or scams were reported by five respondents, followed by account-access or security problems reported by four. Wrong-recipient payments and payment disagreements were each selected by three respondents, incorrect payment amounts by two and delayed or failed payments by one. No respondent reported recipient denial of receipt or failure to return funds. Because respondents could select several options, these counts represent reported problem categories rather than distinct incidents and their combined total should not be interpreted as the number of payment problems experienced.

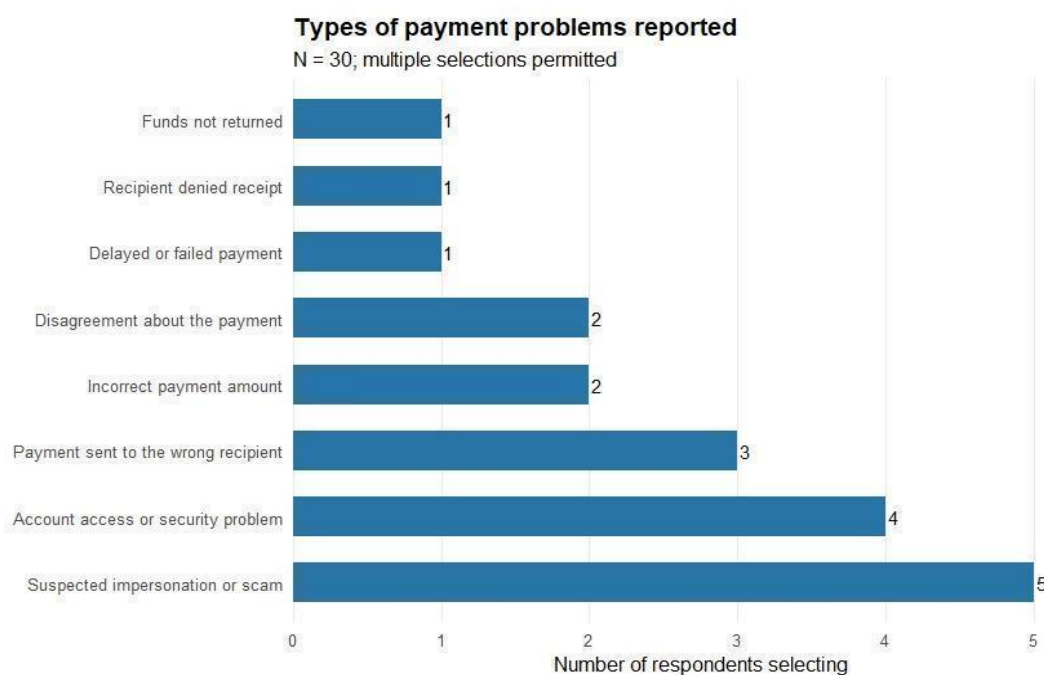


Figure 5: types of payment problems reported

The results place reported problems across both relational and institutional domains. Impersonation, misdirected payments and disagreements may involve recipient identification or interpretation of the transaction, whereas account-access problems concern technical and provider-level assurance. Horizontal and vertical risks may therefore arise within the same payment setting. Table 4 shows that six respondents first contacted the recipient directly and six used the platform's complaint or dispute procedure. Four contacted their bank or card provider, while one took no action. No respondent first approached mutual contact or public

authority. Seven respondents reported full resolution, five partial resolution and five no satisfactory resolution.

Table 4: Immediate response and resolution outcome for respondents reporting at least one payment problem

First response	n	%	Resolution outcome	n	%
Contacted the recipient directly	6	35.3	Fully resolved	7	41.2
Used the service's dispute or complaint procedure	6	35.3	Partly resolved	5	29.4
Contacted bank or card provider	4	23.5	Unresolved	5	29.4
Took no action	1	5.9	Ongoing	0	0
Contacted a mutual connection	0	0	Preferred not to say	0	0
Contacted an authority	0	0	—	—	—

Panel A (first response) and Panel B (resolution outcome) are presented side by side. Panel A, n = 17; Panel B, n = 17. Percentages may not sum to 100 due to rounding.

Figure 6 indicates that subsequent behavioural changes centred on greater caution. Seven respondents began checking recipient details more carefully and seven reported avoiding unfamiliar recipients. Two changed payment services, while two reported no change in their behaviour.

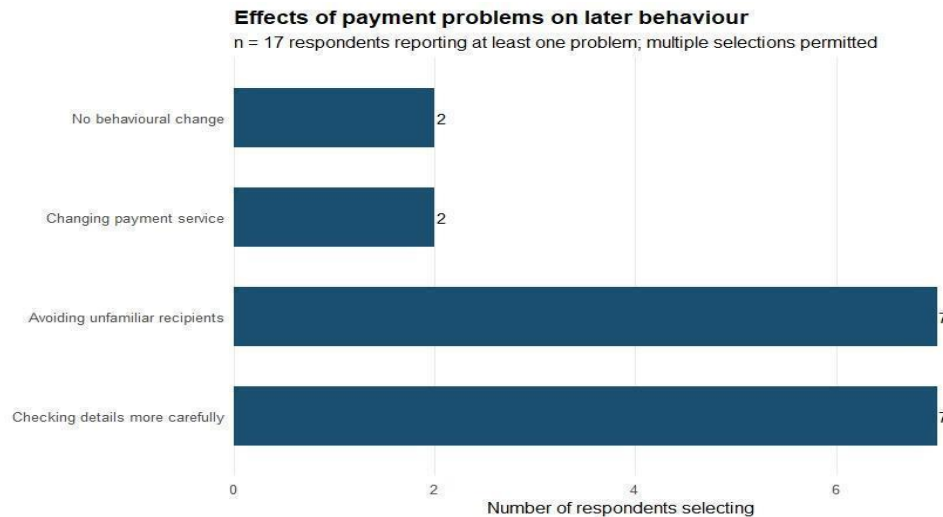


Figure 6: Effects of payment problems on later behaviour

The findings indicate that respondents used both interpersonal and institutional routes after payment problems. Direct recipient contact did not displace formal support, since platform procedures were used just as often as the first response. Reported problems were also associated with more cautious later practices, although the cross-sectional design does not establish that the problems caused those behavioural changes.

4.6 Platform Functions, Visibility and Information Privacy

Figure 7 presents respondents' use of eight functions on their primary payment service, distinguishing between non-use and feature unavailability. Transaction history was the most regularly used function, reported by 21 respondents (70.0%), followed by saved recipients or contact lists, used regularly by 20 (66.7%). Payment notes or references were used regularly by 14 respondents (46.7%), while payment requests were used regularly by 13 (43.3%).

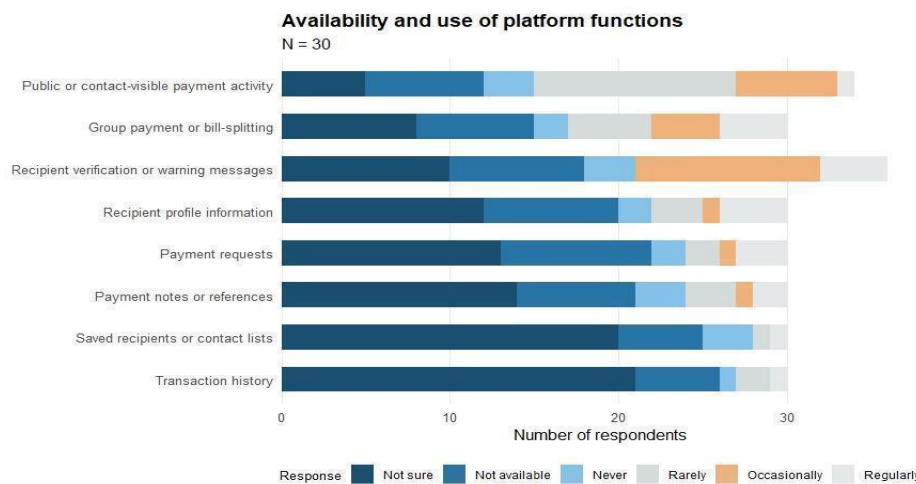


Figure 7: Availability and use of platform functions

Functions with a stronger social component received less use. Eight respondents (26.7%) regularly used group payment or bill-splitting functions. Public or contact-visible payment activity was used regularly by five respondents (16.7%), while 12 (40.0%) never used it and six (20.0%) reported that it was unavailable. Recipient verification or warning messages were used regularly by ten respondents (33.3%), although 11 (36.7%) reported that this function was unavailable. These results show that respondents used operational functions, particularly transaction histories and saved contacts, more often than socially visible features. The distinction between “never used” and “not available” also indicates that low use may reflect either individual choice or platform design.

Table 5: Responses to transaction visibility

Response	Number selecting	% of respondents
Changed or removed a payment description	7	23.3
Changed privacy settings	5	16.7
Felt uncomfortable about a payment	6	20
Avoided making a payment	2	6.7
Used another service	0	0
Asked another party to change visible information	0	0
No effect	16	53.3
Function unavailable	1	3.3
Unsure	1	3.3

Note: Respondents could select more than one option therefore percentages do not sum to 100 percent

Table 5 shows the reported effects of transaction visibility. Sixteen respondents (53.3%) reported no behavioural effect. Seven (23.3%) changed or removed a payment description, six (20.0%) felt uncomfortable and five (16.7%) changed privacy settings. None changed payment services. Visibility was therefore not central to most respondents' platform use. Where it did matter, it appeared mainly in payment descriptions, discomfort or privacy settings. The social character of P2P payments in this sample rested more on recipient relationships and payment context than on public-facing platform functions.

5. Conclusion

5.1 Response to the Research Question

Respondents assessed recipients mainly through personal familiarity, previous successful payments and matching identity information. External confirmation, shared contacts and expected social accountability carried less weight. Horizontal relational trust therefore rested primarily on direct relational knowledge rather than wider network endorsement. Respondents reported checking identifiers, contacting recipients through established channels, delaying transfers, using alternative payment methods, or refusing payment when uncertain. Some proceeded because the amount was small or because they felt socially obliged, showing that payment completion did not always indicate trust.

Following payment problems, respondents used both interpersonal and institutional information sources. Direct recipient contact and platform dispute procedures were the most common initial responses, followed by banks or card providers. Within this sample, relational information supported recipient assessment, while transaction records and formal procedures became more prominent during problem resolution. These findings describe reported practices and do not establish causal relationships or changes in trust over time.

5.2 Contribution and Study Boundaries

This study distinguishes trust in the payment provider from trust in the recipient while showing how the two may interact. Respondents combined platform-generated identity information and transaction records with familiarity, previous payments and external confirmation when assessing recipients. Recipient assessment can therefore be understood as an information practice shaped by the source, consistency and perceived sufficiency of available information. The assessment-action-resolution framework connects these reported information practices with protective actions and responses to payment problems. It classifies related practices rather than demonstrating that trust develops through a fixed sequence.

These contributions must be read within the study's boundaries. The small, non-probability sample does not represent the wider population of P2P payment users in Europe or North America. Each platform subgroup contained only seven or eight respondents. Cross-platform comparisons were therefore descriptive and cannot support reliable or generalisable conclusions about differences between Revolut, PayPal, Zelle and Wise. Reliance on self-reported practices also introduces possible recall error and social-desirability bias. Since the

cross-sectional design did not follow respondents or individual transactions over time, it cannot establish causality, temporal progression, or whether payment problems changed, weakened, or restored trust.

5.3 Closing Position and Future Research

Platform-mediated P2P payments involve recipient information, relationships and platform controls, with relational trust complementing technical and institutional assurance. Familiarity and past exchanges aid identification but can mislead or pressure. Future research should test how information design, privacy, warnings and dispute data shape decisions, using larger samples for regional and service comparisons and longitudinal work on post-problem trust, while accounting for regulatory and platform differences.

References

- Aasheim, C., & Wimmer, H. (2026). Social payments in a digital world: A study of P2P cash app use and acceptance. *Journal of Electronic Commerce Research*, 27(1).
- Aljaradat, A., & Shukla, S. K. (2025). Trust and cybersecurity in digital payment adoption: Socioeconomic evidence from India. *Journal of Business and Socio-economic Development*, 5(4), 372–386. <https://doi.org/10.1108/JBSED-04-2025-0119>.
- Blanco-Oliver, A., Lara-Rubio, J., Irimia-Diéguez, A., & Liébana-Cabanillas, F. (2025). Examining user behaviour with machine learning for effective mobile peer-to-peer payment adoption. *Financial Innovation*, 11. <https://doi.org/10.1186/s40854-024-00625-3>.
- Boston Consulting Group. (2025). Global payments report 2025: The future is anything but stable. <https://web-assets.bcg.com/25/91/2269153c468ca43684442f055cb0/2025-global-payments-report-sep-2025.pdf>.
- Center Forward. (2025). Paying the price of trust: Peer-to-peer payments. https://center-forward.org/wp-content/uploads/2025/03/FINAL_Peer-to-Peer-Payments.pdf.
- Federal Reserve Financial Services. (2026). 2026 Risk Officer Report: Key findings from the Financial Institution Risk Officer Survey. <https://www.frbfinancialservices.org/binaries/content/assets/crsocms/news/research/2026-risk-officer-survey.pdf>.
- Federal Trade Commission. (2026, June 15). FTC data show people reported losing \$3.5 billion to imposter scams in 2025. <https://www.ftc.gov/news-events/news/press-releases/2026/06/ftc-data-show-people-reported-losing-3-point-5-billion-imposter-scams-2025>.
- Ghosh, A., Mishra, R., & Mishra, A. (2025). Role of network externalities and trust facilitators in shaping mobile payment application continuance intentions: Variations across stages of adoption. *Marketing Intelligence & Planning*, 43(8), 1553–1575. <https://doi.org/10.1108/MIP-06-2024-0417>.
- Hammerslough, S., & Celik, N. (2026). Peer-to-peer payments: Beyond splitting the bill. *Financial Health Network*. https://finhealthnetwork.org/wp-content/uploads/2026/03/Peer-to-Peer-Payments_-_Beyond-Splitting-the-Bill.pdf.

- Kiernan, E. A., & Guzman, J. D. (2026). Paying in public: Peer effects, impression management and willingness to pay on digital payment platforms. PLOS ONE, 21(7), Article e0340550. <https://doi.org/10.1371/journal.pone.0340550>.
- Mombeuil, C., & Jean Pierre, S. (2026). Unravelling user switching dynamics in P2P mobile payments: Investigating satisfaction and trust in a duopoly market. FinTech, 5(1), Article 7. <https://doi.org/10.3390/fintech5010007>.
- The Payments Association. (2025). The payments trends report 2025. <https://thepaymentsassociation.org/article/the-payments-trends-report-2025/>.
- PayPal. (2026, July 6). PayPal privacy statement. https://www.paypal.com/de/legalhub/paypal/privacy-full?locale.x=en_DE.
- Revolut Group Holdings Ltd. (2026). Annual report 2025. <https://assets.revolut.com/pdf/annualreport2025.pdf>.
- Shao, Z., Zhang, L., Brown, S. A., & Benitez, J. (2025). Uncovering the structural assurance mechanisms in blockchain technology-enabled online healthcare mutual aid platforms. Journal of the Association for Information Systems, 26(1), 128–170. <https://doi.org/10.17705/1jais.00901>.
- Tan, K.-L., Leong, C.-M., & Richter, N. F. (2025). Navigating trust in mobile payments: Using necessary condition analysis to identify must-have factors for user acceptance. International Journal of Human–Computer Interaction, 41(5), 3325–3339. <https://doi.org/10.1080/10447318.2024.2338319>.
- Visa. (2025). Money travels: 2025 digital remittances adoption report. <https://corporate.visa.com/en/products/visa-direct/resources/money-travels-report.html>.
- Wisker, Z. L., & Alani, N. (2026). Banking on connections: How tie strengths, trust and perceived cybersecurity shape intention to use peer-to-peer P2P digital payment. Journal of Marketing Analytics. Advance online publication. <https://doi.org/10.1057/s41270-026-00530-x>.
- Zhang, Q., & Kim, H. (2025). From social to financial: Understanding trust in extended payment services on social networking platforms. Behavioral Sciences, 15(5), Article 659. <https://doi.org/10.3390/bs15050659>.



2026 by the Authors. This Article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>)