DOI: 10.26354/bb.12.2.103.2026

Tatiana Einbacher*

ORCID: 0009-0001-5539-9528
tatiana-einbacher@wp.pl

Forced Intermediation in Digital Banking: Financial Security and the Autonomy of Older Bank Customers

ABSTRACT

The article aims to explain the mechanism of forced intermediation in digital banking and its significance for the security and autonomy of older customers. It draws on a critical analysis of the literature, payment-services and accessibility legislation, and institutional documents. The article introduces the original analytical category of forced intermediation, five criteria for identifying it and a four-level classification of third-party involvement. It distinguishes technical authentication, consent to a transaction and the customer's actual agency. Actual agency is assessed in terms of the customer's understanding of the transaction's essential parameters, freedom of decision-making and ability to verify the outcome. On this basis, the article develops a conceptual framework for supported use of banking services and outlines a possible two-stage implementation in Poland: a sectoral standard defining a separate role and profile for the assistant, followed, where necessary, by statutory clarification of access to information, liability and activity-recording requirements. The model distinguishes technical assistance from a power of attorney and leaves the decision and final approval of the transaction with the customer.

Keywords: older people, digital banking, financial autonomy, financial security, digital exclusion, third-party assistance

JEL Codes: G21, G28, J14

* Tatiana Einbacher – independent researcher.

<< BACK TO THE CONTENTS

INTRODUCTION

For social and ethical reasons, particular attention should be paid to situations in which an older customer is unable to perform a specific banking activity independently and the bank does not provide a genuinely accessible, secure and equivalent alternative to the digital channel. Reductions in branch networks, fees for some transactions performed at a service desk, automated telephone helplines and the transfer of an increasing number of processes to applications may mean that formally holding an account is not equivalent to being able to exercise independent control over one's money (Latulipe, Dsouza and Cumbers, 2022, pp. 1–13).

Practices that restrict traditional access to banking services in favour of electronic channels may be described as forced intermediation in banking. The term does not refer to financial intermediation provided by a professional entity, but to the necessary involvement of an informal or formal assistant in relations and transactions between an older customer and a bank. The constraint need not be formalised. It may arise from the design of the technology used to deliver the service, such that, without assistance, an older person is effectively unable to use banking services, particularly their own account, or faces disproportionate difficulty in doing so.

The aim of this article is to identify and analyse forced intermediation arising from the spread of electronic distribution channels for banking services and to determine its consequences for the financial security and autonomy of older bank customers. The analysis also distinguishes voluntary support from third-party involvement made necessary by the absence of an accessible alternative. Finally, it proposes solutions capable of reducing older customers' dependence without depriving them of the benefits of modern banking channels.

The article is conceptual and presents an original conceptual framework. It draws on a critical analysis of literature on digital and financial exclusion, older people's use of electronic banking, informal assistance in account management and the financial exploitation of older people. It also considers accessibility and payment-services regulation, institutional reports and secondary data. The study does not present original quantitative or qualitative research and is not a systematic review. Its purpose is to reconstruct the mechanism, organise the relevant concepts and formulate a conceptual framework requiring further operationalisation and empirical verification.

1. DIGITAL AND FINANCIAL EXCLUSION IN BANKING

The literature treats digital inequality as a multi-level phenomenon: inequalities in access, knowledge and skills, modes of use, and the outcomes achieved through technology. For bank customers, relevant factors also include device complexity, connection stability, the sensory and cognitive accessibility of the interface, the ability to understand financial language, a sense

<< BACK TO THE CONTENTS

of security, and the possibility of obtaining help without disclosing confidential data. A person with internet access may therefore still be functionally excluded (van Deursen and van Dijk, 2019, pp. 356–360; World Bank, 2022, pp. 127–145).

Financial exclusion means restricted access to necessary financial services or an inability to use them appropriately, safely and in a manner suited to one's needs. As electronic communication channels and digitalisation become widespread, digital exclusion may form part of financial exclusion, although the two concepts are not identical. A customer may hold a bank account and payment card and have formal access to electronic banking, yet still lack a genuine opportunity to perform a particular action independently. Formal access therefore does not guarantee functional access.

Research on older users of banking technologies shows that involving other people, especially people close to them, in financial activities is not unusual. Assistance includes using a device together, explaining messages, carrying out transactions such as transfers, cash withdrawals or opening term deposits, and monitoring an account. Such assistance may be a precondition for using certain services and may strengthen a sense of security. At the same time, banking solutions are generally designed around a single, fully independent user, leaving actual practices of assistance outside the formal architecture of permissions (Latulipe, Dsouza and Cumbers, 2022, pp. 1–13).

From the perspective of financial autonomy, what matters is not only whether a transaction was completed, but also whether it was understood by the decision-maker, who made the decision, who technically carried it out and who could verify the outcome. In this context, autonomy does not mean complete independence or acting without third-party assistance. Financial autonomy may be understood as a continuum extending away from complete independence and encompassing varying degrees of support from one or more persons. Without analysing extreme cases, it means retaining the right to make decisions and control their implementation while receiving support proportionate to one's needs. Assistance strengthens autonomy when it leaves the customer with an informed choice, including the right to refuse or discontinue an action. Autonomy is weakened, and may in fact be lost, when the assistant effectively assumes the role of decision-maker in a financial operation, such as withdrawing funds from an ATM, making a transfer or closing a term deposit.

2. SERVICE ORGANISATION AND THE GENUINE-ALTERNATIVE TEST

The development of digital channels changes the structure of financial-service use and increases the importance of mobile banking. From the perspective of equal access, a problem arises when digitalisation is accompanied by reduced functional access to traditional, physical service alternatives. Statistics on active application users therefore fail to reflect customers who use their bank account only with third-party assistance or who cannot carry out certain activities (European Banking Authority, 2025, pp. 14–23).

<< BACK TO THE CONTENTS

Analyses by Narodowy Bank Polski of fees for bank accounts show that the manner in which a transaction is performed is reflected in bank tariff schedules. Differences in fees are not necessarily unjustified or impermissible. For the present analysis, however, the relevant question is whether a particular fee supports a voluntary choice of channel or imposes a higher cost on a person for whom the digital channel is inaccessible and who cannot use an equivalent solution (Narodowy Bank Polski, 2025).

The provisions of the Act of 26 April 2024 implementing the European Accessibility Act have applied in Poland since 28 June 2025. They cover, among other matters, payment services, payment accounts, consumer and mortgage credit, and selected services provided as part of brokerage activity. The Financial Ombudsman supervises compliance with accessibility requirements for retail banking services. The regulation reinforces the move away from treating accessibility as a voluntary convenience (Directive (EU) 2019/882, Annex I, Section III; Act of 26 April 2024, Article 3(1)(30) and Articles 33–35).

For the purposes of the analysis, nominal accessibility is distinguished from functional accessibility. A channel is nominally accessible when the bank formally offers it. Functional accessibility means that a particular customer can use it independently, safely and within a reasonable time to obtain the required service. This distinction prevents the mere existence of a telephone service or branch from being treated as resolving exclusion.

An alternative that is genuinely accessible, rather than merely nominally available, should satisfy at least five conditions. First, it must enable the same or a functionally equivalent action. Second, it should be accessible in terms of location and time. Third, it must not entail disproportionate cost. Fourth, it must provide a comparable level of confidentiality and security. Fifth, it should allow the customer to retain decision-making power and control without disclosing data to an unauthorised person.

3. FORCED INTERMEDIATION AS AN ANALYTICAL CATEGORY

It is insufficient to contrast independence with dependence. A person may act autonomously while receiving support from others. What matters is not cooperation itself, but the allocation of knowledge, decision-making and control. Assistance supports autonomy when it increases the customer's ability to act in accordance with their own will. It restricts autonomy when it replaces that will, cuts the customer off from information or becomes the only route to their funds (Havens and Latulipe, 2024, pp. 1–14; Latulipe, Dsouza and Cumbers, 2022, pp. 1–13).

Forced intermediation in digital banking is a situation in which, because a digital banking service is inaccessible or unsuitable and no genuinely accessible and safe alternative channel exists, a customer must rely on informal third-party assistance to obtain information, confirm identity, make decisions or perform actions concerning their own funds. Intermediation is

forced when forgoing assistance would make the service effectively impossible to use or disproportionately difficult.

The definition of forced intermediation comprises four elements that should occur jointly. The first is a barrier within the process or the manner in which it is made available. The barrier may be digital, sensory, cognitive, communicative, economic or organisational and need not be permanent. Forced intermediation may also arise temporarily, for example after replacing a phone, updating an application, having access blocked or during a deterioration in health.

The second element is the absence of a genuine alternative. If the customer can perform the same action at a branch, by telephone or through another accessible channel without excessive cost, the involvement of someone close to the customer remains, in principle, a matter of choice. If the alternative exists only formally and does not lead to a comparable outcome, it does not qualify as a genuine alternative. The accessibility of an alternative may be assessed by applying an appropriate test that takes account of the criteria discussed in Section 2.

The third element is the necessity of third-party involvement. This does not mean coercion by the assistant. The necessity may arise from the complexity of the service relative to the customer's financial competence. In particular, without another person the customer may be unable to obtain necessary information, complete authentication, execute an instruction or regain access. "Forced" refers primarily to the absence of functional choice, rather than psychological or physical coercion.

The fourth element is the assistant's access to information, de facto decision-making power, or ability to perform a financial action. Transport to a branch or the mere provision of a device does not yet amount to intermediation in the sense adopted here. The phenomenon arises when a third party obtains information and data concerning the bank account, participates in identifying the customer, interprets the customer's decision, operates the application, authorises an action using the customer's instruments or controls the outcome.

Identifying forced intermediation requires analysis of the specific course of action. Five criteria may be applied: the availability of an alternative, freedom of choice, the scope of the assistant's involvement, the customer's retention of control, and the reversibility of dependence. These criteria are not assessed on a simple points scale. A set of questions is needed to determine whether support still enables independent action or has become a condition of access to the service.

3.1. Four levels of third-party involvement

Level one – informational support. The assistant explains concepts, reads a message aloud or indicates the next step, but does not learn authentication credentials or perform the action for the customer. The customer operates the device, makes the decision and approves the transaction. As a rule, this level strengthens autonomy, provided that messages are not interpreted in a way that replaces the customer's will.

<< BACK TO THE CONTENTS

Level two – technical support. A third party helps configure a device, locate a function, enlarge the font or navigate the interface. Access to data may be limited, but the assistant is already closer to the banking process itself. Security depends on whether the customer continues to see and understand the actions and retains control over authorisation.

Level three – substitute performance. The assistant enters data, initiates a transfer, operates the application or contacts the bank using the customer's device or data despite lacking formal authority. The account holder may identify the purpose of the transaction, but its technical execution remains in another person's hands. A discrepancy then arises between the actual operator and the person recognised by the system.

Level four – de facto assumption of control by a third party who continuously holds the device, data and information, independently monitors the account, makes payments or decides the order of expenditure. The customer receives only selected information or merely the outcome of that person's actions. Such an arrangement may accord with the customer's wishes, but without necessary formalisation, transparency and control it creates a high risk of abuse.

3.2. ASSISTANCE, POWER OF ATTORNEY AND ASSUMPTION OF CONTROL

A formal power of attorney for banking matters creates a specific relationship between the customer and the assistant. The bank knows the identity of the person acting on behalf of the account holder, can define the scope of that person's authority, and attributes transactions to a formal mechanism of representation. A power of attorney does not guarantee the absence of abuse and does not always meet a need for short-term support, but it reduces the discrepancy between the actual and recorded course of action. Forced intermediation generally occurs outside such an arrangement (Financial Conduct Authority, 2021, paras 4.53–4.60).

The boundary between support and assumption of control is not determined solely by access to a login and password or approval of a transaction. The entire decision-making process – the chain of agency – must be considered: who possesses the information, who formulates the decision, who performs the action, who authorises it and who can verify the outcome. If all these elements fall within the assistant's activity, the customer's presence does not restore effective control.

The proposed category of assumption of control requires answers to three questions: was assistance necessary, was it organised safely, and did the customer retain autonomy? An affirmative answer to the first does not remove the need to answer the other two. Accessible banking should enable necessary support while minimising disclosure of data, recording participants' roles and leaving the decision with the account holder.

Forced intermediation is not equivalent to economic abuse or an unauthorised transaction. It is a mechanism that increases exposure to those risks. The next section examines how a discrepancy between formal authorisation and actual performance affects confidentiality, security, liability and the ability to challenge a transaction effectively.

<< BACK TO THE CONTENTS

4. FINANCIAL SECURITY AND THE CUSTOMER'S ACTUAL AGENCY

Forced intermediation reveals the difference between technical and functional security. The former asks whether the appropriate safeguards were applied and whether the system received the required data. The latter concerns the conditions of actual action: who operated the device, who knew the content of the instruction, who made the decision, and whether the owner of the funds could verify the outcome. A transaction may pass every technical check while leaving the customer without effective control.

PSD2 provides that a transaction is authorised only if the payer has consented to its execution. Article 40 of the Polish Payment Services Act adopts the same rule. Use of the correct password, SMS code, biometric identifier or in-application approval is therefore evidence concerning authentication and the technical course of the transaction, but should not automatically be equated with proof of informed consent to that specific transaction (Directive 2015/2366, Articles 64 and 72; Payment Services Act, Articles 40 and 45).

When acting independently, three elements generally coincide: the customer makes the decision, performs the action and uses their own credentials. Forced intermediation distributes these elements between at least two people. The customer may express a general wish to pay a bill while the assistant selects the recipient and amount. The customer may also approve a message that they have not read or whose parameters were entered by someone else. The formal record then fails to reflect the entire chain of agency.

For the purposes of this analysis, three dimensions must therefore be separated. Authentication, defined in Article 2(33b) of the Payment Services Act, asks whether the provider verified the user's identity or the validity of the use of a particular payment instrument, including the use of personalised security credentials. Authorisation in the legal sense concerns the payer's consent to a specific transaction. Actual agency concerns whether the customer knew its essential parameters, shaped the decision themselves, could refuse and could verify the outcome. These dimensions may diverge: the system may correctly authenticate the customer even though the assistant entered the data and the customer approved the transaction without sufficient knowledge of the recipient, amount or consequences. Successful authentication therefore does not establish who actually entered the data or whether the customer independently formed and knowingly confirmed the instruction. Assessing actual agency requires reconstruction of the entire course of action, not merely examination of the technical authorisation trail; this corresponds to Article 45(2) of the Act, under which recorded use of a payment instrument alone is insufficient to prove authorisation.

A payment-instrument user should use it in accordance with the agreement and take the necessary measures to protect personalised security credentials. Keeping passwords, PINs and codes confidential is rational because it impedes third-party access to the account and preserves accountability. Forced intermediation nevertheless creates a paradox. A customer may be unable to complete the procedure independently while the only available means of

assistance requires allowing an assistant, especially someone close to the customer, access to the device, screen or authorisation message (Payment Services Act, Article 42).

Fraud-prevention systems use, among other measures, real-time transaction monitoring based on AI/ML and behavioural biometrics (European Central Bank, 2025, p. 7). Behavioural analysis may consider the manner of interaction with the device and the course of the session. Unusual operation of the account by an assistant may therefore be treated as an anomaly, triggering additional verification or interruption of the transaction. This follows from the operation of anti-fraud tools and the separation between the customer's formal identity and the actual operator. Although the ECB document cited above does not directly address family assistance in banking, this does not justify circumventing safeguards or sharing passwords. On the contrary, it strengthens the case for a transparent and recorded assistant role.

The confidentiality paradox does not justify unrestricted disclosure of data. It demonstrates, however, that merely informing the customer of their obligations may be insufficient if the organisation of the service offers no safe means of obtaining assistance. Information should be combined with solutions that keep the customer's participation visible, limit the assistant's role and record the participation of a trusted person.

When a transaction is disputed, the provider must demonstrate that it was authenticated, accurately recorded and entered in the accounts and that it was not affected by a technical breakdown or other deficiency. Both PSD2 and Article 45 of the Payment Services Act state that recorded use of a payment instrument alone is insufficient to prove that the payer authorised the transaction or intentionally, or through gross negligence, breached their obligations (Directive (EU) 2015/2366, Article 72(1)–(2); Payment Services Act, Article 45(1)–(2)).

Forced intermediation may weaken the customer's position even before a dispute arises. A person who does not operate the account independently may detect an irregularity after a delay, be unaware of the transaction date or lack access to the account history. They may also depend on the same assistant when filing a complaint, changing a password or securing the account. If the assistant is the potential perpetrator, that dependence hinders both detection and reporting (Payment Services Act, Article 46(1)–(4)).

For security assessment, the article proposes analysing a chain of agency comprising five successive elements: access to information, formulation of the decision, technical preparation of the transaction, expression of consent and control of the outcome. In the independent model, all elements remain with the customer. In a supported model, the technical component may be entrusted to an assistant, but the decision, consent and ability to verify should remain with the owner of the funds.

The highest risk arises when the assistant possesses the information, formulates the decision, performs and approves the transaction, and is then the only person controlling the account history. The banking system may nevertheless attribute all activity to the customer. The fundamental importance of forced intermediation for financial security emerges precisely in this gap between the technical record and the actual allocation of roles.

<< BACK TO THE CONTENTS

5. AUTONOMY AND THE RISK OF FINANCIAL EXPLOITATION

Third-party assistance with banking transactions is not the opposite of autonomy. It may strengthen autonomy when it removes a technical barrier, leaves the decision with the customer and enables the customer to understand and verify the action. This is consistent with supported decision-making: support should serve the person's will and preferences rather than replace them with the assistant's assessment of the customer's best interests (Convention on the Rights of Persons with Disabilities, Article 12; Committee on the Rights of Persons with Disabilities, 2014, paras 17–29).

Where the absence of an assistant effectively cuts the customer off from the service, the dependence is infrastructural. It may arise in various circumstances in which the customer cannot act personally, for example because they cannot physically contact the bank or cannot reach an assistant or authorised representative. If only one person is familiar with the assistance procedure – for example, knows how to log in, keeps the device, receives correspondence and controls the account history – the owner's continuing ability to use the account depends on that person's availability and, importantly, goodwill. The risk of losing access then results from concentrating functions in one person, even in the absence of abuse.

The World Health Organization defines abuse of older people as a single or repeated act, or failure to act, occurring within a relationship in which there is an expectation of trust and causing harm or distress; the concept includes financial and material abuse. Financial exploitation is the illegal or improper use of an older person's money, property or assets. The essence is therefore not another person's involvement as such, but conduct contrary to the owner's will or interests, abuse of trust, benefit to the perpetrator or the infliction of harm (World Health Organization, 2024).

Forced intermediation is not itself a form of abuse, but it increases exposure to risk: both because of dependence on the assistant and because the assistant may abuse the dependent person's trust. The situation may become more serious when the dependent person is reluctant to disclose abuse or fears the consequences of doing so, such as losing the only available support, family conflict or scandal, loneliness, or revealing their lack of competence or frailty (Phelan, O'Donnell and McCarthy, 2023, pp. 2135–2156).

An ageist assumption that an unusual or disadvantageous decision by an older customer proves third-party exploitation must also be avoided. Autonomy includes the right to take risks, make gifts and make choices that others disapprove of or do not endorse. Protective intervention should be based on signs of pressure, absence of informed consent, concealment of information, a conflict of interest or harm, rather than solely on age or an assessment of the decision's rationality (Wood and Lichtenberg, 2017, pp. 3–13).

Informal involvement by an assistant may also have consequences that emerge only after the account holder's death. If one person prepared or executed transfers without a separate

<< BACK TO THE CONTENTS

profile or a formal record of the scope of assistance, heirs may be unable to determine which transactions implemented the older person's instructions, which were gifts and which lacked a basis in the owner's will. This creates a risk of disputes over accounting for funds that were transferred or otherwise used, bringing gifts into account when determining an heir's share or calculating the reserved share (zachowek), and obligations to return funds or provide an account of the actions performed. The risk arises not from family assistance itself but from the failure to separate identities, roles and the decision trail. A recorded assistant role would therefore protect not only the customer's current security but also subsequent civil accountability (Civil Code, Articles 6, 405, 740, 922, 993 and 1039; Financial Ombudsman, 2021, pp. 7–10).

Conversely, complete neutrality towards visible signs of pressure is also inappropriate. A proportionate protection standard should begin with a conversation with the customer in the absence of the third party, provision of information in an accessible form, verification that the specific action is understood, and an offer of a safe channel for further contact. Only the level and credibility of the risk may justify additional safeguards provided by law and contract.

The analysis identifies six conditions for a safe assistance relationship: voluntary choice of assistant, minimal access, separation of support from decision-making, transparency of every action, independent verification of the outcome, and easy revocation of permission or reversal of dependence. These conditions develop the earlier criteria for forced intermediation and apply them directly to the protection of autonomy.

6. A STANDARD FOR SAFE AND ACCESSIBLE BANKING

Directive (EU) 2019/882 and the Polish Act of 26 April 2024 implementing it cover retail banking services and require information and interfaces to be perceivable, operable, understandable and compatible with assistive technologies. These obligations, applicable since 28 June 2025, are an important starting point. They do not, however, exhaust the problem of forced intermediation, because compliance of an individual interface does not determine the actual accessibility of a branch, telephone service, complaints procedure or recovery of access to an account (Directive (EU) 2019/882; Act of 26 April 2024).

The proposed standard rests on four equal values: accessibility of the entire process, preservation of the customer's agency, minimisation of third-party access and accountability for every action. A bank should not require a choice between independence and security. A customer who needs support should be able to use it transparently and under control, without compromising the confidentiality of their data and without the fiction that they personally performed every technical action.

The first element of the standard is at least one genuinely accessible alternative channel. This does not require identical procedures in every channel, but it does require the customer to be able to achieve the same material outcome without disproportionate cost, effort or delay.

<< BACK TO THE CONTENTS

A branch dozens of kilometres away, a telephone service based solely on an extensive voice menu, or a charge for an operation that is free in the application may formally exist without constituting an equivalent alternative.

An accessible interface should offer clear language, enlargement of content, appropriate contrast, compatibility with assistive technologies, sufficient response time and error messages explaining how to correct the problem. For older customers, reducing time pressure, maintaining a stable layout, clearly naming the effect of an operation and enabling safe return to the previous step are particularly important.

Digital banking needs an intermediate solution between entirely independent access and a conventional power of attorney authorising another person to operate the account. A safe assistant role should be established with the customer's informed consent, limited in scope and time and capable of immediate revocation. The assistant could, for example, explain messages, prepare a draft transfer or help assemble documents, but should not automatically acquire the right to give final approval. A reference point for formally recording the limited role of a trusted person is the trusted-contact solution described by the US Consumer Financial Protection Bureau (CFPB). It is narrower, however: designation of a contact person does not itself grant access to the account or authority to conduct transactions without separate authorisation (Consumer Financial Protection Bureau, 2021, pp. 1–4).

It is desirable for the system to recognise the separate identities of the customer and the assistant. Each participant would use their own authentication credentials, and the history would identify who prepared, modified and approved the action. This would reduce password sharing, align the technical record with the actual allocation of roles and facilitate complaint handling. Research on proxy accounts indicates that existing tools often fail to accommodate flexible, everyday forms of support for older people (Havens and Latulipe, 2024, pp. 1–14).

Technical support is consistent with autonomy only when the customer retains the decision, understands the essential parameters and can independently approve or reject the transaction. Before authorisation, the bank should present, in an accessible form, at least the recipient, amount, fee, timing and irreversible consequences. Confirmation cannot be merely an automatic gesture performed at the assistant's direction.

A bank should have a procedure for identifying signs of possible financial exploitation, but its activation cannot depend on age alone. Relevant circumstances include a sudden change in transaction patterns, restriction of the customer's ability to speak freely, lack of knowledge of the balance, the assistant's conflict of interest, loss of the customer's own device or contradictory information about an instruction (Consumer Financial Protection Bureau, 2016, pp. 17–29).

<< BACK TO THE CONTENTS

6.1. Practical implementation of the model in Poland

The proposed conceptual framework may be implemented at two complementary levels. At sectoral level, a standard adopted by the Polish Bank Association or a code of good practice could define a voluntary assistant role distinct from a power of attorney, with a dedicated assistant profile, a defined scope of permissible actions, an activity record and a procedure for withdrawing consent. At statutory level, clarification might be needed principally in relation to liability, the legal significance of an action prepared by the assistant, access to information covered by banking secrecy and the use of the activity record in complaint proceedings. The aim would not be to create a new form of legal capacity or representation, but to regulate technical assistance in which the customer retains the decision and final approval of the transaction.

At the first stage, the bank could define in the account agreement and terms and conditions a voluntary assistant role that would confer no right to dispose of funds independently. Once identified by the bank, the assistant could explain messages, enter data or prepare a draft instruction. Establishing the role should include identification of both persons, the customer's consent in an accessible form, definition of the scope and duration of support, separate authentication credentials for the assistant, a record of the assistant's actions and an independent notification to the customer. The customer should be able to suspend or withdraw consent immediately through any channel. If the customer wished to grant a third party the right to submit legally effective instructions, a power of attorney would remain the appropriate solution.

The technical layer of the framework could separate preparation from approval of an instruction. Using their own profile and credentials, the assistant would prepare a draft operation within the granted authority. On their own device, the customer would receive an accessible and clear summary including at least the recipient, amount, fee, timing and effect, and would then independently approve or reject the instruction. The system would record separately the actions of the assistant and the customer. This solution would not require disclosure of the customer's passwords, codes or other personalised security credentials and would therefore not depend on creating an exception to the obligations under Article 42 of the Payment Services Act.

The assistant's access to banking information should be granular and correspond to the scope of support. Article 104(3) of the Banking Law already permits information covered by banking secrecy to be disclosed to a third party on the basis of authorisation granted by the person to whom the information relates, including authorisation given electronically and recorded by the bank. The proposed model should develop this possibility by defining the visible data, duration and revocation of access, liability for an action prepared by the assistant, the evidential significance of the activity record and complaint rules. If the assistant's role were to extend beyond preparation to independent initiation of transactions or submission of legally effective instructions, an appropriate contractual or statutory basis would be necessary. The solution could first be standardised through a sectoral standard and, following evaluation in practice, incorporated into payment-services or banking legislation.

<< BACK TO THE CONTENTS

7. RESPONSIBILITY OF BANKS AND SUPERVISORY AUTHORITIES

Responsibility for limiting forced intermediation should not be confined to compliance or digital accessibility. It should also encompass product design, security, complaints, the branch network and customer protection. Every material change to a process – especially moving an activity to an application, limiting branch service or introducing an additional fee – should be preceded by an assessment of whether a customer with particular needs can still deal with the matter independently or use transparent and safe support. The risk of informal intermediation should be treated as a design and operational risk, not merely as the customer's and family's private problem.

Assessing the effects of digitalisation also requires measures other than the number of active application users. Useful data include abandoned processes, repeated blocks and access recovery, waiting times in alternative channels, complaints submitted with third-party involvement, and matters that cannot be completed without moving to the application. These indicators should be analysed in aggregate and with respect for privacy, without automatically labelling a particular customer as dependent. Their purpose is to detect barriers in service organisation, not to profile older users on the basis of age.

Supervisory and consumer-protection authorities should assess the accessibility of the entire service journey, not merely formal interface compliance. Comparable indicators of channel accessibility, complaint analyses and mystery-shopping studies involving people with diverse needs would be justified. A minimum standard for safe assistance should define how the assistant role is established and revoked, its powers, separate authentication credentials, the record of activities and independent notification to the account holder. The EBA report indicates that digitalisation and reductions in branch networks may impede access to financial services for vulnerable groups, including older people (European Banking Authority, 2025, pp. 14–23).

The target model may be described as a transition from informal substitution of the customer to supported use of services. The customer retains direct access to information, the decision and final confirmation; the assistant acts in a separate, limited role; and the bank records the actual allocation of actions while providing an alternative channel and independent verification of the outcome. Every element of support is voluntary, proportionate and revocable.

CONCLUSION

The analysis answers the principal research question: the organisation of digital banking services makes an older customer's reliance on informal third-party assistance necessary when a barrier in the digital channel coincides with the absence of a genuinely accessible, safe and functionally equivalent alternative. Neither age alone nor the absence of a particular skill determines the phenomenon. What is decisive is the relationship between the particular customer's capabilities, the design of the banking process and the scope of the assistant's involvement.

<< BACK TO THE CONTENTS

The original result of the study is the identification of forced intermediation as an analytical category situated between voluntary assistance and formal substitution. It occurs when four elements coincide: a barrier to using the service, no genuine alternative, the necessary involvement of an informal third party, and that person's entry into the sphere of information, decision-making or performance of a financial action. Five diagnostic criteria – the availability of an alternative, freedom of choice, scope of the assistant's involvement, retention of control and reversibility of dependence – avoid both trivialising the problem and mistakenly treating every form of family assistance as a violation of autonomy.

Forced intermediation is not in itself economic abuse or evidence of disloyalty by the assistant. It may nevertheless create conditions conducive to exploitation, particularly when one person gains continuing access to the device, data, account history and capacity to approve transactions while the customer loses independent insight into the outcome. Protection against this risk should strengthen the older person's decision-making agency, not replace it with paternalistic control based solely on age.

The proposed conceptual framework has limitations. Above all, it does not diagnose the scale of forced intermediation in Poland or the frequency of the different levels of third-party involvement. The diagnostic criteria are not yet a validated measurement tool, and the proposed solutions require legal, technical and empirical evaluation. The diversity of older people, banking models and relationships with people close to them calls for caution in generalising the conclusions.

Ultimately, the measure of inclusive digital banking is not the number of services available in an application, but the customer's ability to remain informed about their financial position, make decisions about the use of their funds and retain control over their own money. Digitalisation strengthens autonomy when it expands choice. When the only route to a bank account becomes informal access through another person, it may create a new and hidden dependence. Identifying forced intermediation makes it possible to name, assess and limit that dependence without abandoning the benefits of technology or diminishing the importance of voluntary assistance from people close to the customer.

REFERENCES

Committee on the Rights of Persons with Disabilities (2014). General comment No. 1 (2014), Article 12: Equal recognition before the law, CRPD/C/GC/1, United Nations, https://www.ohchr.org [accessed: 7.08.2026].

Consumer Financial Protection Bureau (2016). Recommendations and report for financial institutions on preventing and responding to elder financial exploitation, https://www.consumerfinance.gov [accessed: 7.08.2026].

Consumer Financial Protection Bureau (2021). Financial institutions can help prevent elder financial exploitation with alerts to trusted contacts, https://www.consumerfinance.gov [accessed: 7.08.2026].

<< BACK TO THE CONTENTS

European Banking Authority (2025). Consumer Trends Report 2024/25, EBA/REP/2025/08, https://www.eba.europa.eu [accessed: 7.08.2026].

European Central Bank (2025). National Payment Committees' Actions on Fraud Prevention: Outcome of 2025 Stock-take on National Payment Committees and National Payment Strategies, https://www.ecb.europa.eu [accessed: 7.08.2026].

Financial Conduct Authority (2021). FG21/1: Guidance for Firms on the Fair Treatment of Vulnerable Customers, https://www.fca.org.uk [accessed: 7.08.2026].

Havens, Z., & Latulipe, C. (2024). Proxy Accounts and Behavioural Nudges: Investigating Support for Older Adults and Their Financial Delegates, in: Proceedings of the 50th Graphics Interface Conference, Article 4, pp. 1–14, https://doi.org/10.1145/3670947.3670962

Latulipe C., Dsouza, R., & Cumbers, M. (2022). Unofficial Proxies: How Close Others Help Older Adults with Banking, in: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, Article 601, pp. 1–13, https://doi.org/10.1145/3491102.3501845

Narodowy Bank Polski [National Bank of Poland] (2025). Analiza opłat i prowizji związanych z korzystaniem z rachunku płatniczego w Polsce (według danych na dzień 31.12.2024 r.) [Analysis of fees and commissions related to the use of a payment account in Poland (data as at 31 December 2024)], https://nbp.pl/system-platniczy/dane-i-analizy/analizy-i-opracowania/analiza-oplat-i-prowizji/ [accessed: 16.09.2026].

Phelan, A., O'Donnell, D., & McCarthy, S. (2023). Financial Abuse of Older People by Third Parties in Banking Institutions: A Qualitative Exploration, Ageing & Society, vol. 43, no. 9, pp. 2135–2156, https://doi.org/10.1017/S0144686X21001574

Rzecznik Finansowy [Financial Ombudsman] (2021). Poradnik spadkowy – jak uporządkować sprawy finansowe na wypadek śmierci [Inheritance guide: how to arrange financial affairs in the event of death], https://www.rf.gov.pl [accessed: 7.08.2026].

van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2019). The First-Level Digital Divide Shifts from Inequalities in Physical Access to Inequalities in Material Access, New Media & Society, vol. 21, no. 2, pp. 354–375, https://doi.org/10.1177/1461444818797082

Wood, S., & Lichtenberg, P. A. (2017). Financial Capacity and Financial Exploitation of Older Adults: Research Findings, Policy Recommendations and Clinical Implications, Clinical Gerontologist, vol. 40, no. 1, pp. 3–13, https://doi.org/10.1080/07317115.2016.1203382

World Bank (2022). The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19, https://doi.org/10.1596/978-1-4648-1897-4

World Health Organization (2024). Abuse of Older People: Fact Sheet, https://www.who.int [accessed: 7.08.2026].

Legislation

Convention on the Rights of Persons with Disabilities, adopted in New York on 13 December 2006 (Journal of Laws 2012, item 1169).

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (OJ L 337, 23 December 2015, pp. 35–127).

<< BACK TO THE CONTENTS

Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7 June 2019, pp. 70–115).

Act of 23 April 1964 – Civil Code (consolidated text: Journal of Laws 2025, item 1071, as amended).

Act of 19 August 2011 on payment services (consolidated text: Journal of Laws 2026, item 623, as amended).

Act of 26 April 2024 on ensuring that economic operators meet the accessibility requirements for certain products and services (Journal of Laws 2024, item 731).

<< BACK TO THE CONTENTS