Safety by Design Will Not Save Us: Why Financial Technologies Always Side with Economic Abuse Perpetrators

Belén Barros Pena
Centre for HCI Design
City St George's
University of London
UK
belen.barros-pena@citystgeorges.ac.uk

Clare Wiper
School of Humanities and Social Sciences
Northumbria University
Newcastle upon Tyne
UK
clare2.wiper@northumbria.ac.uk

"Safety by design" has become a familiar mantra within design, policy and information security circles. We take issue with this approach to design, an ahistorical and solutionist interpretation of technology-facilitated abuse that asks practitioners to anticipate how their systems might be misused, and to adjust their design to foreclose those possibilities. We argue that the features enabling technology-facilitated abuse are deeply embedded in the foundational principles under which digital technologies are conceived, and that addressing such harms instead requires systemic change. Taking fintech-facilitated economic abuse as our case study, we demonstrate that "safety by design" is powerless against the harmful potential of digital systems, and that promoting it is not merely ineffective but actively counterproductive.

Financial technologies, Fintech, Safety by design, Fintech-facilitated economic abuse

1. INTRODUCTION

This alt.article takes issue with something called "safety by design" (Online Safety Act Network, 2026; Fitzpatrick, 2019; PenzeyMoog, 2021; eSafety Commissioner, no date), the belief that, in order to "solve" technology-facilitated harms, it suffices that technology makers anticipate those harms and build their technologies in ways that make them impossible to perpetrate. We propose that safety by design is a distraction at best, and a dangerous idea at worst. First, because it intimates that the ability to prevent technology-facilitated harms resides exclusively with technology makers, removing power and agency from everyone else. Second, because it assumes that tweaking the surface of technical systems is enough to solve the insidious problem of technology-facilitated violence and abuse. Using financial technologies as an example, we demonstrate that safety by design is powerless against the harmful potential of digital systems, and that promoting it is not only ineffective but counterproductive.

2. FINTECH-FACILITATED ECONOMIC ABUSE

Digital technologies are actively being used to cause harm to others, and not just by professional criminals driven by personal profit, or by corporations and their business models. Digital technologies have become tools for perpetrating harm to close others as well, as in domestic violence and intimate partner violence. This is commonly referred to as technology-facilitated abuse (Koukopoulos, Janickyj and Tanczer, 2026). Systems often implicated in technology-facilitated abuse include tracking technologies, i.e. services whose main purpose is to monitor the activity and location of people and devices, location and mapping services, smart home devices and, interestingly, financial technologies, which are software applications and services related to digital forms of money.

Because financial technologies are frequently implicated in technology-facilitated abuse, we can identify a distinct sub-category: fintech-facilitated abuse (Nyman, Evertsson and Henrikson, 2023). Where this abuse targets a person's money and assets, it constitutes economic abuse: behaviour that controls a survivor's ability to acquire, use and maintain economic resources, including not only money but

© Barros Pena et al. Published by BCS Learning and Development Ltd.

the goods and services money provides access to (Sharp-Jeffs, 2022). We use the term ”fintech-facilitated economic abuse” throughout to denote this intersection.

Some technologies are indeed designed and developed with harmful intent, such as “stalkerware”. These are systems purposefully built to enable the surreptitious surveillance of individuals and to violate their right to privacy. But the vast majority of problematic technologies are not designed with malicious intent: the fact that they can be used for abusive purposes is an unintended consequence. The people who design and make these technologies don’t want to cause harm, but there is something in the functionality that these technologies provide, or in the way that functionality is structured, that enables perpetrators of violence and abuse. Financial technologies are a clear example of these unintentionally harmful technologies.

Financial technologies have many advantages. They enable fast payments without requiring access to physical cash; they allow us to transact at any time and from anywhere; they give us easy access to some of our financial data, such as balances and transactions; they help us build a credit history, which in turn allows us to borrow money from mainstream lenders; they assist us in comparing all kinds of products and services to find the one that suits our needs; and they deliver convenient safety features such as quickly freezing a lost or stolen bank card. But co-existing with all these advantages, we also have fintech-facilitated economic abuse. Why are financial technologies unintentionally abetting and helping perpetrators of this kind of abuse?

Some professionals in the software industry believe that financial technologies enable abuse perpetrators because those who make them do not think about personal safety when developing their products. From this perspective, the problem is that the unintended consequences of software in relation to personal safety are not actively or explicitly considered when designing software applications. These professionals advocate something they call ”safety by design” (Online Safety Act Network, 2026; Fitzpatrick, 2019; PenzeyMoog, 2021; eSafety Commissioner, no date), a set of methods, techniques and principles that help software teams actively and explicitly consider the unexpected safety implications of their technologies as they build them. The idea is that, if software professionals apply this ”safety by design” approach, the tendency of technologies to help economic abuse perpetrators will go away. This is a very appealing proposition because it suggests that technology makers are in control and can easily change things. Sadly, at least in the case of financial technologies, safety by design will not work. Safety by design is a well-intentioned framework; and the techniques, methods, and principles it proposes can be instructive. However, in the case of financial technologies, safety by design will not stop fintech-facilitated economic abuse.

3. WHY DO FINANCIAL TECHNOLOGIES ALWAYS SIDE WITH PERPETRATORS?

To understand why this is the case, we need to return to the “why” question: why are financial technologies unintentionally abetting and helping perpetrators of economic abuse? The answer is that the tendency to abet abusers is deeply embedded in the underbelly of these technologies. The link between fintech and abuse is ingrained in the fundamental principles and priorities that govern fintech design, and not in their functionality or interface. These principles are so foundational to our existing fintech ecosystem and to the way we conceive and understand these technologies that they are almost never mentioned or spoken about. In fact, most fintech designers and developers do not even know they exist, even if they enact and reproduce them in their technology-making work every day. These nefarious design principles, which are the water we swim in, are: *efficiency*, *visibility*, *rigidity*, *replacement* and *negative security*.

3.1. Efficiency

The main driver in the design of financial technology today is making transactions as fast and efficient as possible for all involved. The emphasis is on speed, seamlessness, anytime anywhere access, convenience and ease of use. The problem with this focus on efficiency and convenience is that it results in the removal of most friction, and that’s how we end up with ”tap-something” and ”one-click” payments; but also with credit applications that can be submitted is just a few clicks. For instance, the HSBC UK mobile banking app proudly boasts that you can apply for a credit card in 3 easy steps. Their online banking website allows you to apply for a mortgage almost as easily. We name HSBC UK because we bank with them and have easy access to their digital presence, but we believe the observation applies to most banks.

Lack of friction may appear great on the surface, but it is extremely problematic. It subjects people to constant temptation to spend, discourages deliberation over significant financial decisions, and ultimately enables one of the classic strategies of economic abuse: credit applications submitted in a victim’s name to damage their credit score and, with

it, their ability to borrow from mainstream lenders (Littwin, 2012). Because access to credit is often essential to regaining independence after abuse, this damage can be devastating.

3.2. Visibility

According to design academics, financial technologies are "dataful" (Ferreira and Perry, 2019). This means that they transform money into information, and they are built to collect and preserve the vast amounts of data generated by digital transactions. This in turn engenders transparency and visibility. That's how we can access information about our finances at any time and from anywhere; and also how we build financial histories, which become visible to service providers for credit rating and marketing purposes. But of course that same data, and that same history, are equally available to perpetrators of economic abuse. They can use them to impersonate victims in digital interactions with financial service providers, to intimidate and coerce, and to build cases against them in the family courts. Visibility is not neutral: it delivers to perpetrators an infrastructure of surveillance they would otherwise have to construct themselves.

3.3. Rigidity

Rigidity encapsulates the fact that digitising financial tasks and workflows involves turning them into linear, step-by-step processes (O'Neill, Dhareshwar and Muralidhar, 2017). This is unavoidable: in order to be expressed through software, human actions must be simplified, formalised and structured. Our rich, nuanced, and wonderfully complex human interactions are reduced to a sequential series of linearly concatenated events. That removes all flexibility from them and makes them unable to cope with the chaos and complexity of people's lives. By contrast, economic abuse and other forms of coercive control are the exact opposite: messy, unpredictable and infinitely adaptable (Stark, 2024).

Rigidity in financial systems manifests in all sorts of ways. Sometimes in relatively small things, like the fact that real-time transaction notifications in joint accounts always go to both account holders. An example of this is available on the Monzo forum: https://community.monzo.com/t/joint-account-notifications-only-for-my-own-card/45820. There is nothing these joint account holders can do about it: they are condemned to know every time their spouse makes a purchase of any kind, even if the payment is done with an individual card. At the time of writing, no UK bank appears to offer joint account holders the option of disabling notifications to the other party. This is not merely an oversight: it is an open invitation. A perpetrator who has coerced a victim into using a joint account for everyday payments - a dreadfully common situation (Wilson-Garwood, 2025) - acquires, at no cost and with no technical skill, a real-time surveillance tool that the bank maintains on their behalf.

The intrinsic rigidity of financial technologies also disempowers and discourages the few remaining humans in financial service provision from exercising discretion and applying flexibility in extraordinary circumstances. The digital process rules, and front-line staff in banks are either not allowed or become reluctant to contradict the standard automated procedures, since that entails taking risks that may impact their employment. "Computer says no" has become the standard mode of operation, and that also ends up helping perpetrators, because it is the survivors who most often require the understanding and the flexibility that is no longer available in financial service provision. A common example involves victims of abuse unable to remortgage their family home after separating from the perpetrator, because bank affordability checks determine they cannot repay a mortgage on their own (Cartwright, 2024).

3.4. Replacement

Our financial technologies are designed to replace all other forms of money, including cash. The end goal is to remove all other alternatives, so that citizens have no choice but to jump on the digital money bandwagon. This comes from the idea that digitising money brings "operational efficiencies", which essentially means that banks believe digital saves them money. Whether that is actually the case is not so clear. Digitasing finance involves substantial costs: from sourcing, paying and retaining competent technical expertise; to cloud infrastructure, security and incident response; and the usual expense of maintaining and updating software systems.

The idea that the digitisation of money is unavoidable and should be total is probably an impossible fantasy. No country has successfully fully replaced cash with digital money, between other things because of the dear consequences that would have for national security and the resilience of financial infrastructure (Birch and Grosclaude, 2025). Most worryingly, the idea of fully replacing cash with digital money excludes and ignores those who, for one reason or another, have no choice but to rely on cash (Access to Cash Review, 2019). That includes migrant communities refused access to the formal banking system. A recent report from a UK charity describes how digitising money impacts migrant survivors of abuse, and the terrible powers it confers on perpetrators (Royal, 2025). The rapid replacement of cash by digital payments

may also foreclose the more discreet transactions survivors have historically relied on to retain some independent access to economic resources.

3.5. Negative security

The last design principle of financial technologies is about the way they understand and implement security. They adopt a negative conception of it: security as the absence of, or freedom from, threat (Roe, 2008). Negative security focuses on protecting assets and information, rather than people (Coles-Kemp and Bjerg Jensen, 2019); and it assumes a strict one-to-one relationship between digital accounts and users. Negative security also implements binary, all-or-nothing security mechanisms, such as PINs and passwords. These are binary because if you know them, you get full access to everything. This security model holds users responsible for their own safekeeping (after all, they own the access credentials) and imagines the threat as a stranger motivated by financial gain (Bellini, 2023).

This negative security model is completely inadequate in an abusive context. This is what late professor of cybersecurity Ross Anderson wrote in his seminal textbook: *"The problems faced by a woman leaving an abusive and controlling husband are among the hardest in the universe of information security. All the usual advice is the wrong way around: your opponent knows not just your passwords but has such deep contextual knowledge that he can answer all your password recovery questions. (...) the abuser has access to your device and may install malware"* (Anderson, 2020).

So the existing security model of financial technologies simply does not work for economic abuse. We need to find a new approach to keeping survivors safe. This new model needs to account for the fact that abusers have access to all kinds of personal information and they often enjoy physical access to and control of survivors' devices.

4. SAFETY BY DESIGN WILL NOT SAVE US

This is why financial technologies always side with perpetrators: because they are guided by these 5 principles. Because they prioritise efficiency, visibility and replacement above all else; because they result in rigid systems that lack essential flexibility; and because their model of security is ineffective and inappropriate for abusive contexts. These principles are not interface patterns, and they are not specific features: they are the fundamental premises under which financial technologies are conceived. No safety by design technique tackles design at this level, the level at which design meets ideology and politics.

The 5 principles are not arbitrary design defaults either that just happen to be bad for survivors of economic abuse. They are all united by a single driving factor, a design principle to rule them all: the reckless pursuit of profitability at all costs. Efficiency translates into higher transaction volumes, increased credit uptake and therefore more interest; visibility follows extractive rather than transparency logics, treating data as a monetisable asset only partially available to citizens, who are the legitimate data owners; rigidity is the result of cheap automation, which provides the excuse for reduced investment on frontline workers, eliminating professional discretion and enforcing self-serving notions of risk; replacing cash disposes of the one payment form that generates no data, no fees and no customer lock-in; and protecting information and assets, rather than people, is easier and delivers the absolute minimum required to avoid legal liabilities. Safety by design will not save us because it does absolutely nothing to address the "profitability at all costs" ultimate mandate (Wiper and Glinski, 2025), acting as a distraction that diverts attention from it.

But safety by design is not just ineffective: it is also counterproductive. It is attractive to regulators and industry because it is voluntary, market-friendly, and deflects responsibility towards technology makers, rather than the financial industry, citizens and the state. It lets the financial sector self-regulate rather than face binding consumer-protection law, mandatory liability shifts, or structural interventions. In doing so, safety by design becomes more than a distraction: it functions as a legitimating discourse that makes continued de- and self-regulation look responsible and desirable (Harvey, 2005). Safety by design is what Nancy Fraser has called an "affirmative remedy": an intervention that tackles negative outcomes by leaving their systemic causes intact (Fraser, 1995). Affirmative remedies are like surface patches: because they do not touch the underlying structures, the negative outcomes constantly reemerge, needing continuous interventions that end up positioning their beneficiaries as *"inherently deficient and insatiable"*, the recipients *"of special treatment and undeserved largesse"* (Fraser, 1995 p.85). This means that safety by design may end up negatively distorting societal perceptions of abuse survivors, victimising them even further.

As we have argued, safety by design will not change financial technologies and their abusive tendencies. Changing financial technologies requires changing our financial system and its obsession with profit, a much harder thing to do than fiddling with

interfaces and tweaking features. If we want to stop financial technologies from helping economic abuse perpetrators, we need to go way beyond designing for safety. We need to radically change the priorities that drive the design of our financial technologies and, we argue, most other types of digital technologies as well. We have already started thinking about how that could be achieved (Royal, Wiper and Barros Pena, 2025; Barros Pena et al., 2021; Barros Pena, 2023). Without this fundamental twist, our digital systems will continue to side with perpetrators.

REFERENCES

Access to Cash Review (2019) *Final Report*. Available at: https://www.accesstocash.org.uk/media/1087/final-report-final-web.pdf (Accessed: 15 July 2026).

Anderson, R. (2020) *Security Engineering - A Guide to Building Dependable Distributed Systems*. Third edition. Wiley. Available at: https://www.cl.cam.ac.uk/archive/rja14/book.html (Accessed: 15 July 2026).

Barros Pena, B., Kursar, B., Clarke, R.E., Alpin, K., Holkar, M. and Vines, J. (2021) *Financial Technologies in the Cycle of Poor Mental Health and Financial Hardship: Towards Financial Citizenship*, CHI Conference on Human Factors in Computing Systems. CHI '21, ACM New York, NY, USA. https://doi.org/10.1145/3411764.3445251

Barros Pena, B. (2023) *Money as an Interface*, Interactions, 30(6), pp. 42–46. https://doi.org/10.1145/3627702

Bellini, R. (2023) *Paying the Price: When Intimate Partners Use Technology for Financial Harm*, Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: Association for Computing Machinery (CHI '23), pp. 1–17. https://doi.org/10.1145/3544548.3581101

Birch, D.G.W. and Grosclaude, L. (2025) *Why cash alone won't cut it: Practical strategies to increase resilience in European payment infrastructure.*, Journal of Payments Strategy & Systems, 19(3), pp. 234–246. https://doi.org/10.69554/azph8747

Cartwright, D. (2024) *'Locked into a mortgage, locked out of my home' How perpetrators use joint mortgages as a form of economic abuse and how to stop them*. Surviving Economic Abuse. Available at: https://survivingeconomicabuse.org/wp-content/uploads/2024/09/SEA-Joint-Mortgages-Report-2024.pdf

Coles-Kemp, L. and Bjerg Jensen, R. (2019) *Accessing a New Land: Designing for a Social Conceptualisation of Access*, Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. CHI '19, ACM New York, NY, USA. https://doi.org/10.1145/3290605.3300411

eSafety Commissioner (no date) *Safety by Design*. Available at: https://www.esafety.gov.au/industry/safety-by-design (Accessed: 16 July 2026).

Ferreira, J. and Perry, M. (2019) *From transactions to interactions: social considerations for digital money*, Disrupting Finance - FinTech and Strategy in the 21st Century. Theo Lynn, John G. Mooney, Pierangelo Rosati and Mark Cummins. Palgrave Pivot (Palgrave Studies in Digital Business & Enabling Technologies, 2662–1282), pp. 121–133. https://doi.org/10.1007/978-3-030-02330-0

Fitzpatrick, C. (2022) *Designed to disrupt: reimagining banking products to improve financial safety*. Available at: https://apo.org.au/node/320806 (Accessed: 15 July 2026).

Fraser, N. (1995) *From Redistribution to Recognition? Dilemmas of Justice in a "Post-Socialist" Age*, New Left Review, (I/212), pp. 68–93.

Harvey, D. (2005) *A Brief History of Neoliberalism*. Oxford University Press. https://doi.org/10.1093/oso/9780199283262.001.0001

Koukopoulos, N., Janickyj, M. and Tanczer, L.M. (2026) *Defining and Conceptualizing Technology-Facilitated Abuse ("Tech Abuse"): Findings of a Global Delphi Study*, Journal of Interpersonal Violence, 41(1–2), pp. 249–275. https://doi.org/10.1177/08862605241310465

Littwin, A. (2012) *Coerced Debt: The Role of Consumer Credit in Domestic Violence*, California Law Review, 100(4), pp. 951–1026.

Nyman, C., Evertsson, L. and Henrikson, A.-S. (2023) *Digitally facilitated economic abuse in the age of digital financial services – new risks for economic abuse in intimate partner violence*, Journal of Gender-Based Violence, 7(3), pp. 368–382. https://doi.org/10.1332/239868023X16909576356057

Online Safety Act Network (2026) *Safety by Design Code of Practice*. Available at: https://www.onlinesafetynetwork.uk/documents/1684/Safety_by_Design_-_Code_of_Practice.pdf

O'Neill, J., Dhareshwar, A. and Muralidhar, S.H. (2017) *Working Digital Money into a Cash Economy: The Collaborative Work of Loan Payment*, Computer Supported Cooperative Work (CSCW), 26, pp. 733–768. https://doi.org/10.1007/s10606-017-9289-6

PenzeyMoog, E. (2021) *Design for Safety*. A Book Apart. Available at: https://abookapart.com/products/design-for-safety.html (Accessed: 8 September 2025).

Roe, P. (2008) *The "value" of positive security*, Review of International Studies, 34(4), pp. 777–794. https://doi.org/10.1017/S0260210508008279

Royal, K. (2025) Survivors' Needs: How financial services firms can support customers experiencing economic abuse to regain financial control and rebuild their lives. Surviving Economic Abuse. Available at: https://survivingeconomicabuse.org/wp-content/uploads/2025/04/Survivors-Needs_SEA_2025.pdf

Royal, K., Wiper, C. and Barros Pena, B. (2025) *Designing Out Economic Abuse in the UK Banking Industry: A Call To Action*. Northumbria University. https://doi.org/10.25398/rd.northumbria.30499676.v1

Sharp-Jeffs, N. (2022) *Understanding and Responding to Economic Abuse*. Emerald Publishing Limited. https://doi.org/10.1108/9781801174183

Stark, E. (2024) *Coercive Control: How Men Entrap Women in Personal Life*. Oxford University Press. https://doi.org/10.1093/oso/9780197639986.001.0001

Wilson-Garwood, R. (2025) *Counting the Cost: The Scale and Impact of Economic Abuse in the UK*. Surviving Economic Abuse. Available at: https://survivingeconomicabuse.org/wp-content/uploads/2025/07/Counting-the-Cost-report-Surviving-Economic-Abuse-July-2025.pdf

Wiper, C. and Glinski, J. (2025) *The Role of Banks in Addressing and Preventing Coerced Debt in the Context of Intimate Partner Abuse*, The British Journal of Criminology, p. azaf078. https://doi.org/10.1093/bjc/azaf078