



Consumer Protection

Potential (or actual) privacy violations


This barrier refers to situations where customers' personal identifiable information is breached or exposed to third parties.

Why is this barrier important?

Evidence shows that while both men and women value data privacy, it is not a factor that inhibits adoption and/or use of DFS or other financial services. For women, this barrier mirrors the challenges and threats they encounter in their physical lives, which can lead to negative experiences when using DFS. While privacy violations are an increasing issue across quickly developing markets, many countries (policy-makers, regulators, and providers) are implementing data protection frameworks to limit this barrier's negative impact on customer and the financial sector.

Connected Barriers

- 

Information Availability & Capability
Digital literacy
- 

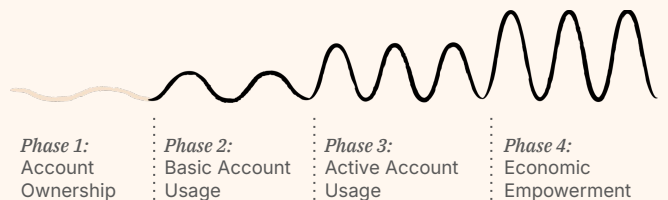
Product & Service Quality
Reliability and quality of in-person services
- 

Consumer Protection
Fraud and scams
Online/Phone/Social media harassment

Most Relevant Segments

- | | | | |
|---------------------------|-----------------------------|--------------------------|------------------------------|
| 1 | 2 | 3 | 4 |
| Excluded,
marginalized | Excluded,
high potential | Included,
underserved | Included,
Not underserved |

Customer Journey Relevance



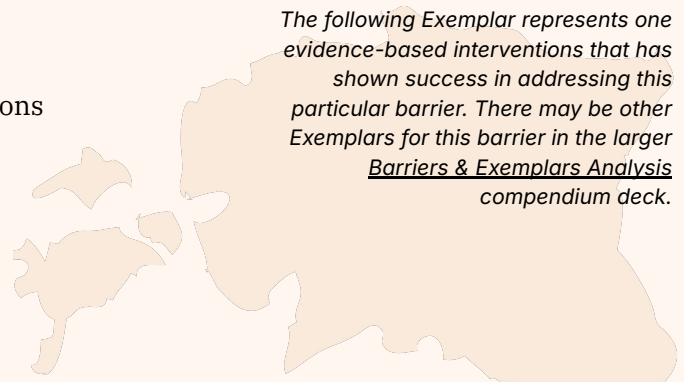


Key evidence relevant to this barrier

- Data protection is also becoming a key factor shaping DFS access and use, especially by women ([CGAP, 2018](#)), and recent studies show that in both higher and lower-income countries, consumers value protection of their personal data ([UNCDF, 2021](#)).
- A major deterrent for women from DFS is the fact that they have to divulge personal information (such as mobile numbers) to agents, who might, in turn, misuse it. This lack of trust and awareness of risk exposure are pertinent issues that must be addressed to allow uninhibited use of financial services by women ([AFI, 2020](#)).
- A study found that a majority of low-income customers in Kenya were willing to pay a premium for greater protection of their personal data in digital loan services ([CGAP, 2020](#)).
- Interviews with low and middle-income men and women suggest women see data use violations far differently than men do, and that DFS providers should take this into account. Women's concerns parallel the challenges and threats they encounter in their physical lives, such as location tracking and sexual harassment ([CFI, 2021](#)).
- Research in India revealed that concerns about their data and security can lead women to curtail their use of different services and self-censor their behavior. Women might also lack knowledge of how to safeguard their personal data and rely on male family members and more educated people for advice on how to protect their photos, social media messages, etc. ([Dalberg, 2017](#)).



The following Exemplar represents one evidence-based interventions that has shown success in addressing this particular barrier. There may be other Exemplars for this barrier in the larger [Barriers & Exemplars Analysis compendium deck](#).



Exemplar

Estonia's E-identity Program

"After gaining independence from the Soviet Union in 1991, Estonia, one of the smallest nations in Europe, was left with little public infrastructure and virtually no commercial activity. It needed to build high-functioning government services for its residents and fledgling private sector." (Braverman and Kuntz, 2012).

The Government of Estonia began building a robust digital ID ecosystem using citizen information from

the Population Register Act. "The Population Register Act issues a unique number to every Estonian resident, termed the Personal Identification Code ('PIC'). The PIC is issued to every individual at birth or any time after application to the processor of the Population Register ('PR'), but it does not function independently as a digital ID." (Digital ID, 2020). The government used this PIC as the input into a robust digital ID program.

Key activities

"In 2003, the government launched the first version of its e-government portal (www.eesti.ee), which offered secure online access to a handful of government services." (Braverman and Kuntz, 2012). "When a resident applies for the issue of a digital ID, the information they submit is checked against the Population Register, and they are issued a digital ID (or e-ID) that is made unique by the inclusion of the PIC." (Digital ID, 2020).

"The e-ID and the ecosystem around it are part of any citizen's daily transactions in the public and private sectors. People use their e-IDs to pay bills, vote online, sign contracts, shop, access their health information, and much more. Holders of a digital identity need not be Estonian residents anymore however. Since 2014, Estonia has also offered a program called e-Residency for anyone who wishes to become an e-resident of Estonia and access its diverse digital services regardless of citizenship or location." (Enterprise Estonia). "Private-sector entities, such as banks and telecommunications companies, also offer services through the state portal – and thus have an incentive to invest in maintaining the infrastructure backbone." (Braverman and Kuntz, 2012). The country also expanded the system to have a mobile ID service accessible via smartphones equipped with SIM cards.

Key uses of the e-ID:

Cited from Enterprise Estonia:

- A legal travel ID for Estonian citizens travelling within the EU
- A national health insurance card
- A proof of identification when logging into bank accounts
- Digital signatures
- Internet voting
- To check medical records, submit tax claims, etc.
- To use the e-Prescription service

Outcomes/results

"Today, Estonia's 1.3 million residents can use electronic ID cards to vote, pay taxes, and access more than 160 services online, from unemployment benefits to property registration... More than 99% of the country's people now have electronic ID cards, and every day approximately 10,000 users visit the portal." (Braverman and Kuntz, 2012). 70% of the population use an ID card regularly for public services. 94% of taxes are filed online through the portal.

"Estonia is, to date, the only nation where citizens can cast online ballots in every type of election from local to parliamentary. When Estonia held the world's first binding election using internet voting in 2005, a mere 2% of voters cast ballots online; in the 2011 parliamentary election, that number rose to nearly 25%." (Braverman and Kuntz, 2012).



Key enabling environment factors for the intervention

The government invested heavily in creating this electronic ID program (upfront investment of €50 million to €100 million). “To attract users, the government offered a 30% discount on public transportation to people who registered with the e-ID system. The number of e-ID card holders increased 213% in 12 months.” (Braverman and Kuntz, 2012). There are also legal frameworks in place governing the digital ID. First, the Population Register Act creates the input for the ID (a personal identification code), and the Identity Documents Act governs the issue of the digital ID, or the e-ID, incorporating this PIC.

Key design elements and principles that led to successful outcomes

- Open platform: Any institution can use the infrastructure and it works as open source.
- Transparency: Citizens have the right to see their personal information and how it is used by the government by checking log files. “Every Estonian can review the full history of inquiries about him or her, including police-, banking-, and health-related inquiries. If a user does not recognize or approve of an inquiry, they can file a complaint with Estonia’s Information Services Agency.” (Braverman and Kuntz, 2012).
- Efficient: Data is collected only once by an institution, which reduces bureaucracy and redundancy.
- Multiple use cases: Citizens can use the ID to vote, pay taxes, access unemployment benefits, register property etc.

Potential for scale/replicability

This program operates on a national scale and has greatly increased the number of services available on the e-portal. “A number of national governments—including those of Belgium, Germany, Italy, and the Netherlands, as well as a handful of Middle Eastern countries—have launched or are planning to launch e-ID card programs. None of them are as far along the path as Estonia. Other countries expanding their programs can take inspiration from how it overcame some foundational challenges.” (Braverman and Kuntz, 2012).

Challenges encountered during the program

Estonia experienced foundational challenges when launching this ambitious program but was able to overcome them. For example, when the platform first launched, the services provided were extremely limited, so demand was not initially high. To build a user base quickly, the government provided incentives through subsidized transportation, which helped attract the initial user base. The government then scaled up the amount of services available once it had built an established user base.

Recommendations from the research

Estonia’s program offers several lessons learned and recommendations for those wishing to build a digital ID ecosystem:

1. Build a user base quickly: Estonia succeeded in this by offering subsidized public transportation in exchange for registering in the system.
2. “Address privacy concerns: Estonia’s residents can opt out of making their data accessible.” (Braverman and Kuntz, 2012).
3. Scale up the amount of use cases of the e-ID.

Additional Exemplars

Aadhaar Project

Regulations Drive Success of Digital Finance in Côte d’Ivoire

The Role of Gender in Agent Banking

GRID Impact and SIA’s analysis revealed that this barrier along with 11 others require further research and examination as to how they affect the customer experience, other barriers and overall WEE-FI. More in-depth analysis can be found in the larger Barriers & Exemplars Analysis compendium deck.