14 MARCH 2024 • *Brussels, Belgium*

CENTR Comment on Proposal for a Regulation on a framework for Financial Data Access

Summary of CENTR key recommendations

- Domain-level enforcement action, such as suspension or deletion of domain names, has far-reaching consequences on consumers and businesses and should only be used after a careful balancing act by competent authorities, in case of serious risks for safety and security of end-users, and where no other more effective means are available.
- 'Delete' action without the possibility for competent authorities to re-register the deleted domain name can create an opportunity for malicious actors to deceive consumers and obtain personal data and log-in credentials, exposing end-users to more security threats and grave data breaches.
- In absence of any justification why such drastic enforcement measures, such as domain-level action, are beneficial for the purposes of respecting obligations under the FiDA proposal, the enforcement measures at domain level should be excluded from the proposal.
- Considering the cross-border nature of open banking, the FiDA proposal and its enforcement measures need to be aligned with the well-established and effective consumer protection mechanisms under the CPC Regulation that will avoid further administrative burden and conflicting competencies on national level.

Introduction

CENTR is the association of European country code top-level domain registries (hereinafter ccTLDs). All EU Member State and EEA country ccTLDs (such as .nl and .no) are members of CENTR.

CENTR members are at the core of the public internet, safeguarding its stability and security. The majority of European ccTLDs are non-profit organisations or SMEs, providing an internet infrastructure service in the interest of and in close cooperation with their local internet communities (e.g. registrars, end-users, CSIRTs, law enforcement and other competent authorities).

ccTLDs are responsible for operating and maintaining the technical Domain Name System (DNS) infrastructure for their top-level domain (such as .de or .cz). The DNS is a well-established network protocol at the heart of the internet infrastructure – commonly thought of as the "phone book of the internet". It provides a navigation function to map user-friendly domain names to numeric IP addresses. ccTLDs only hold information enabling users to navigate the internet but do not store, transmit or enhance any content online.[1]

CENTR welcomes the European Commission's intentions behind the Proposal for a Regulation on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554 (hereinafter, 'FiDA proposal') for enabling consumers and businesses to better control access to their financial data and promoting a greater digital transformation of the financial sector.

Since domain names are included as part of enforcement measures available for competent authorities under the FiDA proposal, CENTR wishes to support **evidence-informed policymaking**, taking into account the intentions behind the FiDA proposal to increase trust of customers in EU financial service, in line with EU Better Regulation guidelines.[2]

CENTR wishes to raise the following concerns and offer additional clarifications to the legislative text.

Domain names as key internet infrastructure

Domain names are foundational pieces of internet infrastructure that encompass several crucial functions: 1) Domain names are essential as a technical sign-post to ensure that right resources are found and directed to when users browse and communicate online (e.g., website loads, email is sent, etc.); 2) Domain names are essential for establishing an online identity and starting an online business connected to the unique identifier online (e.g., brand and business identity). Before any associated service can be offered to the end-user (e.g., a website, application, platform), an individual and/or business user needs to register a domain name.

[1] For more information on the role of the DNS in accessing and delivering online content, see CENTR, "Domain name registries and online content" (2022).
[2] European Commission Staff Working Document, Better Regulation Guidelines, SWD(2021) 305 final.

A domain name and its management are distinct from any content or any other service associated with it. The infrastructure for connected services, such as website, email address, or an application are provided by other intermediaries (e.g., web hosting companies, mail service providers etc.).

The FiDA proposal includes the domain-level action as part of enforcement measures available for competent authorities. Article 18(1)(c) of the FiDA proposal includes a specific domain-related provision, stipulating that "in the absence of other available means to bring about the cessation or the prevention of any breach of this Regulation and in order to avoid the risk of serious harm to the interests of consumers, competent authorities shall be entitled to [...] to order domain registries or registrars to delete a fully qualified domain name and to allow the competent authority concerned to record such deletion".

There are a number of concerns with inclusion of domain-level action in the FiDA proposal which, despite its objective to increase consumer trust and respect for consumer rights, might inadvertently have unwanted consequences on both consumer protection, as well as the ability of the financial sector to continue its business online.

CENTR members would like to raise the following **concerns with Article 18(1)(c) and potential risk-scenarios involving domain-level enforcement action.**

Consumers lose access to financial service and all customer data

The deletion of a domain name removes the domain name from the TLD zone file and prevents it from resolving on the public internet. All subdomains (i.e., mail.ing.nl) and services related to it (i.e., email addresses, websites, applications) are no longer functional. It also disables users' ability to navigate lawful content on websites linked to the domain. A 'delete' action cannot be undone when this choice of action is erroneously implemented,[3] and as a result has a dramatic impact on consumers.

As a result of 'delete' action, all services related to a financial service under the scope of the FiDA proposal stop working. For the users of that financial service, this effectively means losing access to their accounts, associated financial and customer data, as well as the ability to contact the customer support or get in touch with the infringing service. This may have a counterproductive and adverse effect on unsuspecting users of the service, in light of the intentions behind the FiDA proposal.

Due to the fact that domain-level action is a drastic intervention at the internet infrastructure level, **it is often reserved for cases when the risk to collective interests of consumers is imminent and serious enough to mandate such intervention**, by effectively removing access to any associated service to prevent more consumers from getting harmed. For example, the Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 ('CPC Regulation') gives

[3] For more information on the differences of domain-level actions available for domain registries to address abuse, and their effects on the internet infrastructure, see Internet & Jurisdiction Policy Network, "Toolkit: DNS Level Action to Address Abuses" (2021).

consumer protection authorities a power to order deletion of domain names of infringing digital services, "where appropriate" and where no other effective means are available to avoid the risk of serious harm to **the collective interests of consumers**.

It is not clear from the proposal that the purpose of the FiDA regulation is to include enforcement measures that can justify such drastic intervention when it comes to ensuring consumer rights. The **purpose of the FiDA proposal seems to encourage the diversification of the financial services on the market, while putting consumers control over their financial data at the core of it. Domain name level enforcement action goes against that aim, as it puts consumers at disadvantage** by effectively removing their access to their data and financial services.

Financial services risk to lose their business or suffer irreparable financial losses due to their inability to comply with FiDA

The language of domain-level enforcement action in Article 18(1)(c), i.e., "delete a fully qualified domain name and to allow the competent authority concerned to record such deletion", suggests a technical action that releases domain name for re-registration to the general public. As a result of a deletion of domain name from the list of registered domain names, the domain name can be re-registered by a third-party on a "first-come, first-served" basis.

In addition to consumers losing their access to all services associated with the domain name, **the deletion (and subsequent re-registration) of the domain name has irreversible consequences on the owner of the financial service** that has relied on the domain name to offer their services to consumers. In case of the infringing service aligning its compliance efforts with the FiDA Regulation, the ownership change of the domain name that has previously been subject to the enforcement action under the FiDA can only be challenged in courts.

Coupled with effectively losing its business due to customers' inability to access their accounts and services as a result of the deletion of a domain name, as well as all potential legal challenges in appealing the authorities' decision to restore the ownership of a domain name that had served as a business identity and brand recognition online, the consequences of this enforcement decision on the financial service and its business continuity can be devastating.

According to the Impact Assessment accompanying the proposal, the initiative is expected to create pressure on firms to compete on innovation and costs to the benefit of consumers. As a result, "weak market offers would be pushed out of the market and competition would remain high[...]".[4] The purpose of the FiDA proposal seems to promote a healthy competition on the market, based on the innovative approach to services offered to consumers.

[4] European Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554, SWD(2023) 224 final.

It is not clear from the proposal, nor its preparatory documentation, that the purpose of the FiDA regulation is to allow drastic market intervention by authorities, followed by EU companies effectively losing their business altogether, or **invoking a significant financial and reputational loss on a financial service under the scope of the FiDA proposal**.

Alignment with existing EU consumer protection acquis

The aim of the FiDA proposal is to incentivise financial services to share customer data, inter alia through more effective enforcement.

Article 18 of the FiDA proposal seems to be inspired by the existing EU consumer protection law, namely the CPC Regulation, and follows the logic of minimum enforcement powers available to competent consumer protection authorities under its Article 9.

First, **it is not clear what the relationship between competent authorities under the FiDA proposal and the CPC Regulation is**, especially since both have a similar aim to protect consumers online and include largely overlapping enforcement measures.

The CPC Regulation has encouraged and strengthened cross-border cooperation mechanisms between national authorities within the CPC Network within a number of areas applicable to consumer rules, including unfair commercial practices and e-commerce.[5] Considering the cross-border nature of open banking, it might be **beneficial to simply align the FiDA proposal with the CPC Regulation** by referencing existing legislation in the area of consumer protection enforcement, **instead of creating a different authority and duplicating efforts that are aimed at achieving the same goal**, with potentially conflicting competences.

Naturally, this should be coupled with **extending the competencies of existing consumer protection authorities at national level to allow for effective and coordinated enforcement of obligations under the FiDA proposal**, especially within the global and borderless digital market.

The enforcement measures at domain name level are already part of the ammunition of consumer protection authorities under the CPC Regulation, albeit the technical action referenced in the CPC Regulation is fundamentally different from Article 18(1)(c) of the FiDA proposal.

Domain-level action for greater consumer protection

As mentioned earlier, the deletion of a domain name has an irreversible effect on the ownership of the domain name, as well as resulting in inaccessibility of all associated services. Due to this often disproportionate measure for the purposes of responding to unwanted content or sanctioning a non-compliant digital service, deletion must be reserved to cases of serious risks to safety and security of consumers, followed by an informed

[5] For more information on the CPC Network, see European Commission's informational page.

balancing test performed by competent administrative and judicial authorities. Third-party interests, such as availability of lawful content and services to end-users online, need to be taken into account and weighed against any potential short-lived gains of this enforcement action.

For these reasons, it is commendable that Article 18(1)(c) includes a number of procedural safeguards before any action at domain level can be mandated. This includes a reference to the risk of serious harm to consumers, and the absence of other available means to bring about the cessation or the prevention of any breach of this Regulation before action at domain level can be mandated by competent authorities. **CENTR welcomes the explicit reference to the principle of proportionality and compliance with procedural safeguards, as well as the principles of the Charter of Fundamental Rights of the European Union**.

However, it is unclear why the Commission decided to include a particular technical action available for competent authorities when issuing orders to registries that simply releases the domain for re-registration to the general public: "[...]delete a fully qualified domain name and to allow the competent authority concerned to record such deletion" in Article 18(1)(c).

In addition to consumers losing their access to the services offered, as well as the financial service losing their identity online, the re-registration of the same domain by a third-party **will inevitably result in more confusion for consumers** who will be returning to the domain name they are used to, without finding the previous service they became accustomed to. Additionally, it would be possible for malicious actors to re-register the domain name with the purpose of tricking consumers to share their personal data or log-in credentials, which exponentially increases the risk of further security and data breaches. Established and well-known domain names that have previously been used for providing a financial service can be especially attractive for malicious actors for conducting phishing and other fraudulent activities, exploiting the recognition of the domain name associated with the legitimate service.

Article 9(4)(g)(iii) of the CPC Regulation that stipulates domain-level action available for competent consumer protection authorities references a fundamentally different action: "delete a fully qualified domain name and ***to allow the competent authority concerned to register it***" (emphasis added). This effectively means that the domain name ownership of an infringing service is assumed by the competent authority. This action still makes uncertain whether the associated services continue being available for the end-users, as well as the subsequent fate of customer data. However, it does give power to competent authorities to proceed with other awareness or enforcement measures, such as redirection of users to an information page about any available remedy measures, once end-users attempt to reach the domain name previously associated with the infringing service.

If deemed necessary and proportionate by the co-legislators to include enforcement measures at domain level as part of the FiDA proposal, **it is strongly advisable to at least align the language with the existing EU consumer protection acquis**, and reference technical action that, whilst still having a grave consequence on consumers and the infringing service, allows more flexibility for competent authorities to avoid further consumer confusion.

Conclusion

The absence of any justification why such drastic enforcement measures, such as deletion of domain names of infringing financial service, are included in the FiDA proposal is not in line with the EU Better Regulation guidelines that mandate evidence-based policymaking and justification of proposed measures, especially when these have significant economic impact.

As a result of the lack of justification, as well as of a feasible scenario when non-compliance for FiDA might require such drastic intervention at the technical infrastructure level with disproportionate consequences for financial services and consumers, CENTR calls for deletion of domain-level action from the enforcement measures available for competent authorities under the FiDA proposal.

At minimum and in case of provided evidence that such enforcement measures are merited due to the risk of serious harm to consumers in case of non-compliance with the FiDA proposal, the enforcement measures referenced in Article 18(1)(c) should be aligned with the existing EU consumer protection law. Namely, by bringing the FiDA enforcement measures under the auspices of competent consumer protection authorities and their minimum enforcement powers under the CPC Regulation.

Lastly, the technical action referenced in Article 18(1)(c) with regard to domain-level enforcement powers available to competent authorities under the FiDA proposal needs to reflect the purpose of the enforcement measure to increase consumer trust, as opposed to undermining it. CENTR calls for aligning the language of Article 18(1)(c) as closely as possible to the existing enforcement measures available to consumer protection authorities under Article 9(4)(g)(iii) of the CPC Regulation.