Open banking: Ukraine enters new stage of payments market digital transformation

On 1 August 2025, the National Bank of Ukraine (NBU) enacted a series of regulations that establish an open banking system in Ukraine and significantly improve the regulatory environment for modern fintech services. The move also marks another significant step towards harmonizing Ukrainian laws with the European Payment Services Directive PSD2 (EU Directive 2015/2366).

NBU's regulatory acts on open banking

- Regulation on Open Banking (Resolution No. 80, dated July 25, 2025)
- Regulation on Authorization Procedures for Non-Financial Payment Services Providers (Resolution No. 81, dated July 25, 2025)
- Regulation on the Use of Electronic Trust Services When Payment Services Providers Access User Accounts (Resolution No. 82, dated July 25, 2025)

Together with the provisions of the Law of Ukraine "On Payment Services," the above acts establish a unified legal foundation for open banking in Ukraine. The new regulatory framework is designed to enshrine a transparent and technologically standardized model concerning account access, reinforced by strict requirements for authorization, authentication, liability, and technical compatibility.

In practice, the new regulation will have a number of impacts for banks, fintech companies, and consumers. Let us examine the main components of the open banking model initiated by the NBU, its implementation stages, and the requirements for participants.

01 What is open banking?

Open banking is a regulated interaction model that ensures the secure and controlled exchange of information between banks and other payment service providers (**PSPs**) through standardized interfaces (**APIs**), **based on user consent.**

At the heart of open banking is a fundamental principle: mandatory APIs for all banks, which gives fintech companies access to customers' bank accounts. This greatly simplifies PSP cooperation with banks and allows for the launch of new services.

02 Who participates in open banking?

Account servicing PSPs

Banks or non-banking payment institutions

Third-party PSPs (*i.e., fintech companies*)

Payment initiation service providers ("**PISPs**") and account information service providers ("**AISPs**")

Users

Individuals or legal entities who provide consent to access their accounts

Technology Operators

Companies that technically support interactions within the open banking ecosystem

03 What services are offered within the framework of open banking?

Payment initiation service

Transmission of a payment instruction from the user (payer) to the bank or other account-servicing PSP.

- Provided only after receiving the user's consent
- Initiates a one-time payment from the user's account
- Payment instruction is **transmitted via specialized interfaces** established under the open banking framework

Account information services

Access by a PSP to account data such as balance, transaction history, and other details defined by the user's consent.

- Provided strictly on the basis of **express user consent** (valid up to 180 days)
- Real-time access to account information

04 Client consent as the core condition for open banking

Open banking services can only be provided with the user's prior consent.

Method

Consent is provided directly to the Account-servicing PSP for the term not exceeding 180 days.

Content

User consent must clearly specify:

- The specific Third-party PSP being granted access;
- The specific account being accessed;
- The type of service being provided;
- The scope of information shared;
- The validity period of the consent (if unspecified, valid until revoked).

Form

Consent is provided electronically using enhanced customer authentication.
Consent logging is performed within the bank's information system and must include:

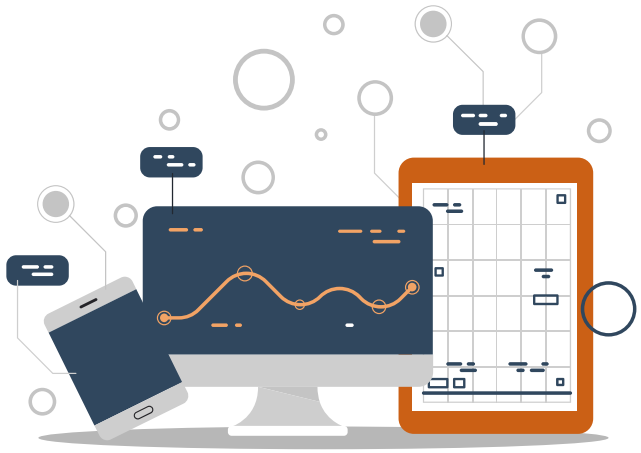
- The date and time of receipt;
- User identifiers;
- Authentication methods;
- Third-party PSP identifiers.

Revocation

The user is entitled to revoke consent at any time:

- Through the Account-servicing PSP; or
- Through the Third-party PSP.

Upon revocation, the Third-party PSP access is immediately blocked.



05 Registration and authorization of open banking participants

Requirements for Third-party PSPs

1. Authorization by the NBU and inclusion in the Payment Infrastructure Register
2. Availability of IT systems capable of interacting via APIs
3. Valid qualified open banking certificate
4. Liability insurance (for non-bank institutions)

06 Functions and responsibilities of open banking participants

Functions and responsibilities of open banking participants		
Banks and other Account servicing PSPs	**Responsibilities**	**Prohibited actions**
	▪ Ensure continuous access to accounts via basic interfaces; ▪ Include third-party access terms in the agreement with users; ▪ Verify Third-party PSP authorization via certificates and the Register; ▪ Obtain express user consent and permission for disclosure of confidential information; ▪ Ensure secure data exchange via specialized interfaces; ▪ Maintain logs, monitor activity, respond to unauthorized actions; ▪ Retain all user consents for a minimum of 5 years.	▪ Sharing information unrelated to the requested services with Third-party PSPs; ▪ Providing access without authorization or user consent; ▪ Modifying payment instruction details from Third-party PSPs.
Third-party PSPs	**Responsibilities**	**Prohibited actions**
	▪ Identification during each request to a bank; ▪ Provide non-financial payment services only with valid access; ▪ Retain user consents and data for at least 5 years.	▪ Receiving funds from the user in connection with payment transactions; ▪ Storing sensitive user payment data; ▪ Altering the amount or other parameters of a payment instruction; ▪ Requesting information unrelated to the provided service.

07 Liability of the payment service providers

Bank or other Account-Servicing PSPs are liable for:

- Granting access without valid user consent;
- Disclosing banking/commercial/payment secrets without permission or beyond the agreed scope;
- Failure to execute or improper execution of a payment operation initiated via a Third-party PSP.

Third-party PSP are liable for:

- Providing services without proper authorization;
- Violating the terms of agreement with the user;
- Causing damage due to non-performance or the improper execution of a payment operation.

08 Open banking implementation timeline

1 August 2025 — The NBU's open banking regulations enter into force

By 1 January 2026 — Banks and other PSPs must align their operations with the new regulations, particularly by ensuring API access

By 1 August 2026 — The transition period ends; during this time, **penalties** for some technical non-compliance are not enforced

How will the changes affect banks and fintech companies?

The introduction of open banking is expected to unlock new opportunities for **innovative financial products**, **increase competition** in the payments market, and expand the range of user-friendly services.

For more information regarding the terms and requirements for open banking in Ukraine, please contact:

Illya Muchnyk

Partner, Head of Banking and Finance Practice at Kinstellar Kyiv office and Firmwide Head of FinTech at Kinstellar

+380 44 490 9575

illya.muchnyk@kinstellar.com

Oleksandra Poliakova

Managing Associate

+380 44 490 9575

oleksandra.poliakova@kinstellar.com

Zakhar Oprysko

Junior Associate

+380 44 490 9563

zakhar.oprysko@kinstellar.com