National Bank of Ukraine

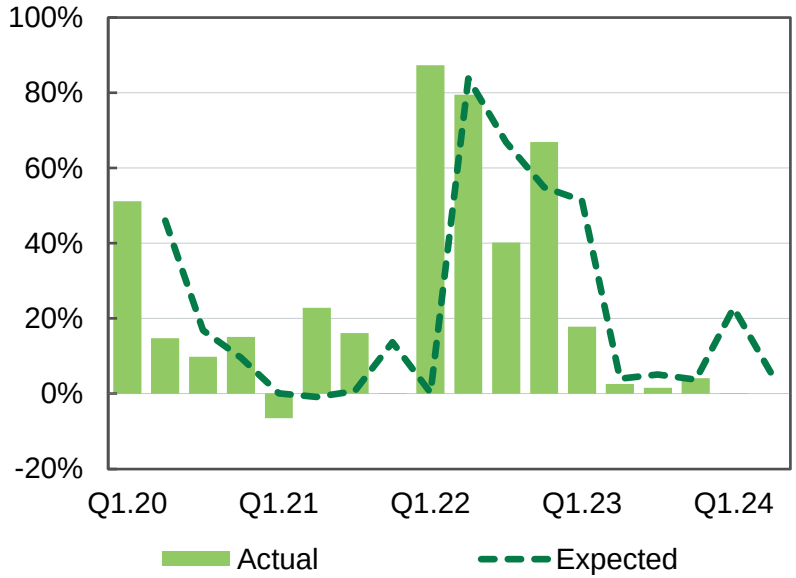
Tail risks for payment systems and implications for financial stability: Ukraine's experience during the war

Pervin Dadashova

5 June 2024

Operational risks materialized in full from the first day of invasion

Change in banks' operational risks over three-month period (balance of responses*)



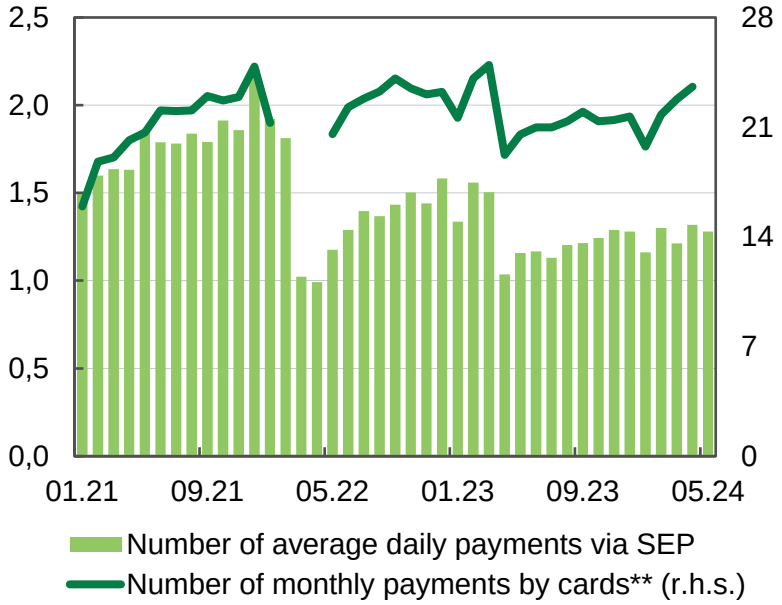
* A positive balance of responses indicates an increase in risks.

Source: NBU Lending Survey

- Banks had contingency plans for crisis events, but rarely assumed a full-scale war.
- These plans had to be updated immediately after the invasion.
- During the first days of invasion only one third of bank branches in endangered regions were functioning, regular cash supply channels were interrupted.
- The need for the use of electronic payment instruments, on-line money transfers and payments increased.
- All efforts of banks and the regulator had to be focused on sustaining key bank functions, i.e. making payments and keeping customer funds safe.
- Disruption of these functions could trigger larger-scale systemic problems.

Undisrupted access to payment services promotes trust to banks

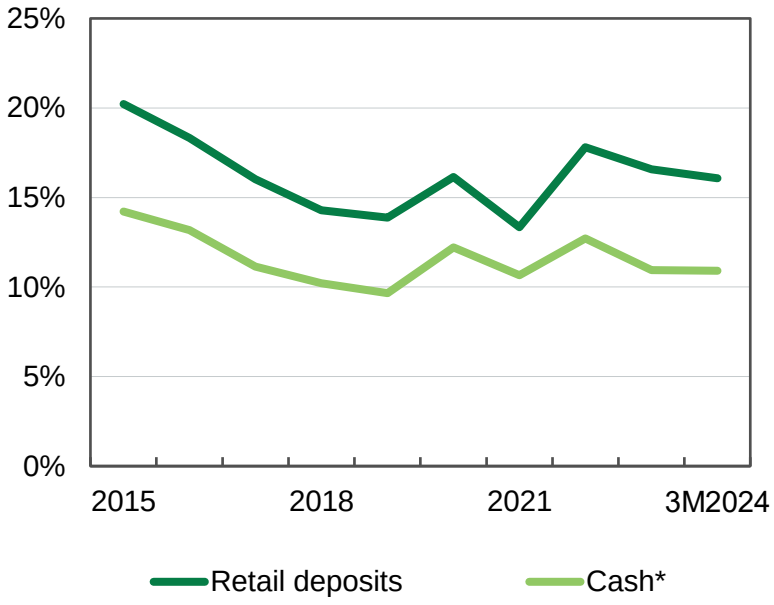
Number of payments through SEP* and by cards, millions of transactions



* SEP - System of Electronic Payments. ** Cards issued by Ukrainian banks and NovaPay. Submission of the statistics was suspended in Feb-Apr 2022.

Source: NBU.

Retail deposits and monetary base relative to GDP



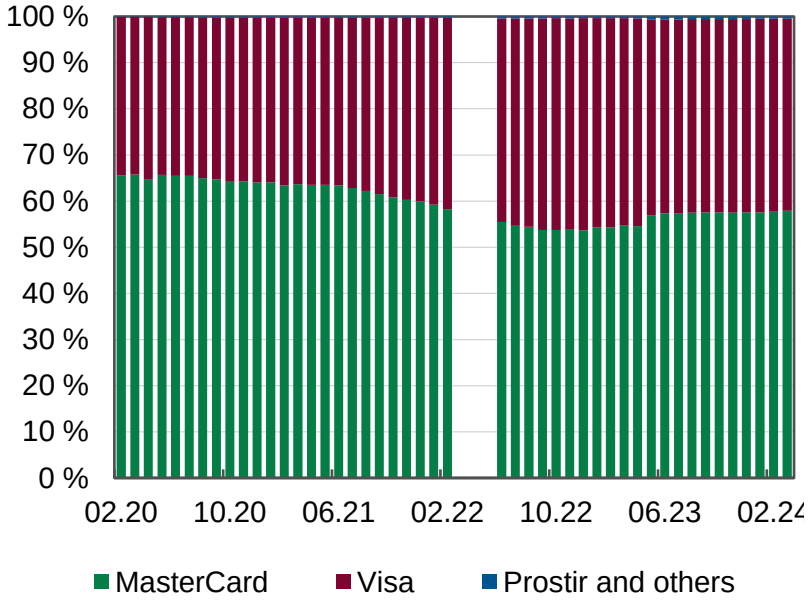
* M0 monetary aggregate.

Source: NBU.

- Despite the full-scale war, payments were continuous, which prevented high demand for cash and saved banks' liquidity.
- The system of interbank payments (SEP) maintained by the NBU supported regular transactions. Only in the first days of the invasion and during massive bombardments some payment orders took more time to get completed and were slightly postponed.
- That said, it took considerable efforts and resources of the NBU to support the system.

Retail payments are made through international payment systems

Proportions of retail cashless transactions by quantity, by payment system



* In February–April 2022, the statistics submission was suspended.

Source: NBU.

- International payment systems (MasterCard and Visa) make up over 99% of Ukrainian market.
- The international payment systems are immune to direct physical threats of war. However, they can still be vulnerable to cyber attacks and operational risks.
- For instance:
  - In 2018, Visa experienced a systemic failure throughout Europe.
  - In early March 2022, a failure in Visa card processing in Ukraine occurred because of disruption of main connection channel.
  - In Q2 2023, customers of two major Ukrainian retail banks had problems with MasterCard transactions due to technical issues on both sides.
- The NBU is the oversight body for international payment systems in Ukraine. However, efficient oversight requires more than national regulator's attention.

KyivStar case – third party risk that materialized

- In December 2023, one of the largest Ukrainian Telecom companies, KyivStar, faced one of the biggest cyber attacks on IT infrastructure in world history. Hackers obtained access to KyivStar's network through a compromised employee account.
- The attack lasted for three days. The attack erased 40% of company's virtual infrastructure. Many banks used KyivStar's network as part of their communication infrastructure.
- What this meant for banks:
  - Bank head offices stayed in touch with branches thanks to backup communication channels.
  - POS terminals and ATMs that relied on KyivStar-provided mobile Internet took the major hit.
  - Mobile- and Internet-banking users who used KyivStar faced difficulties with completing their transactions through mobile applications (authentication was not possible).
- After the dust settled, the NBU started to develop requirements concerning third party risks that covers key service providers for banks.
- Most subscribers, partners, vendors, large businesses, and influencers remained loyal to the provider, according to the company. "I chose this brand" indicator was only 2% down, which is minor for an accident of this scale.

Key takeaways from Ukraine's experience

- Operational risks including cyber-risk are usually much more serious than previously thought, and can potentially trigger other risks.
- Operational resilience of payments systems and third-party services providers mitigates systemic risks for banks, primarily liquidity risk, and enhances the trust in banks.
- According to public opinion polls, in Ukraine the trust to banks improved twice since the full-fledged war started in early 2021.
- Regulators and banks should be prepared not only to operational risks that materialize for individual banks but also to a simultaneous shock for a number of banks, payment systems and the central bank. Therefore, they should have contingency plans for such tail events.
- Threats for smooth functioning may come from different events, and the banks have to adjust quickly to preserve financial stability.

Follow for more details:

NBU Financial Stability Report, December 2023, Payment System Risk

NBU Financial Stability Report, December 2022, Payment Infrastructure Risk