FNALITY GLOBAL PAYMENTS

ADDRESSING SPILLOVER RISKS IN FNALITY GLOBAL PAYMENTS

THE FNALITY TEAM

JULY 2021

CONTENTS

INTRODUCTION

Fnality International, a consortium of major global financial institutions founded in 2019, is developing a number of independent wholesale payment systems called Fnality Payment Systems (FnPS). Initially, FnPSs for five key currencies are planned: CAD, EUR, GBP, JPY and USD. While each FnPS settles transactions in one currency, the FnPSs are also operationally linked with each other (the network of linked FnPSs is called Fnality Global Payments or FnGP). It will be the first time that real-time gross settlement payment systems in major currencies are linked directly with each other. Thanks to these linkages, the simultaneous settlement of both legs of cross-currency (or foreign exchange) transactions can be achieved easily (payment versus payment or PvP). This property greatly contributes to the reduction in systemic risk arising from cross currency or foreign exchange markets.

While these PvP linkages bring about several risk reducing benefits, they may also become the channels through which disruptions in one system are transmitted to the others. It is thus of key importance that such spillover risks are managed and controlled effectively. High level guidance on how risks from linkages among Financial Market Infrastructures (FMIs) should be managed is provided, for instance, by Principles 3, 12 and 20 of the CPMI-IOSCO Principles for FMI (PFMI).

As sound, state-of-the-art risk management is of paramount importance to Fnality, the company intends to monitor, assess and control risks at all levels of the organisation and across FnPSs. This paper provides an overview of two envisaged approaches and methodologies with a focus on spillover or inter-systems risks. First, we outline a proposed conceptual framework for identifying key inter-systems spillover risks within FnGP. We then show how such risks can be mitigated. The second part of the paper looks at spillover risks from a quantitative perspective. More concretely, we present some of the results of an extensive quantitative simulation exercise looking into various potential spillover scenarios. The analysis includes spillovers - measured by the changes in the liquidity needs - between the central bank operated interbank payment systems (Real-time Gross Settlement systems or RTGS systems) and the FnPSs as well as between the FnPSs themselves.

THE FNALITY ECOSYSTEM

Before delving deeper into the specifics of the Fnality Risk Management methodology, it is helpful to illustrate the Fnality Ecosystem (see Figure 1). At the centre, there are the planned independent Fnality Payment Systems (FnPSs), each processing payments in one currency (CAD, EUR, GBP, JPY and USD). Through their linkages, they form Fnality Global Payments (FnGP).

Each FnPS, operated by a local entity (Fn Local), is connected to the RTGS system of the central bank whose currency it processes.[1] For example, £FnPS will be connected to the CHAPS system and have an account at the Bank of England; $FnPS will be connected to the Fedwire system operated by the Federal Reserve, and €FnPS to the Target2 (or T2) system. Finally, there are the participants in FnGP, i.e., large financial institutions that are active in wholesale markets. They have accounts in one or more FnPSs as well as at least one central bank of the in-scope currencies. The FnPSs, the RTGS systems and the participants together form the Fnality Ecosystem.

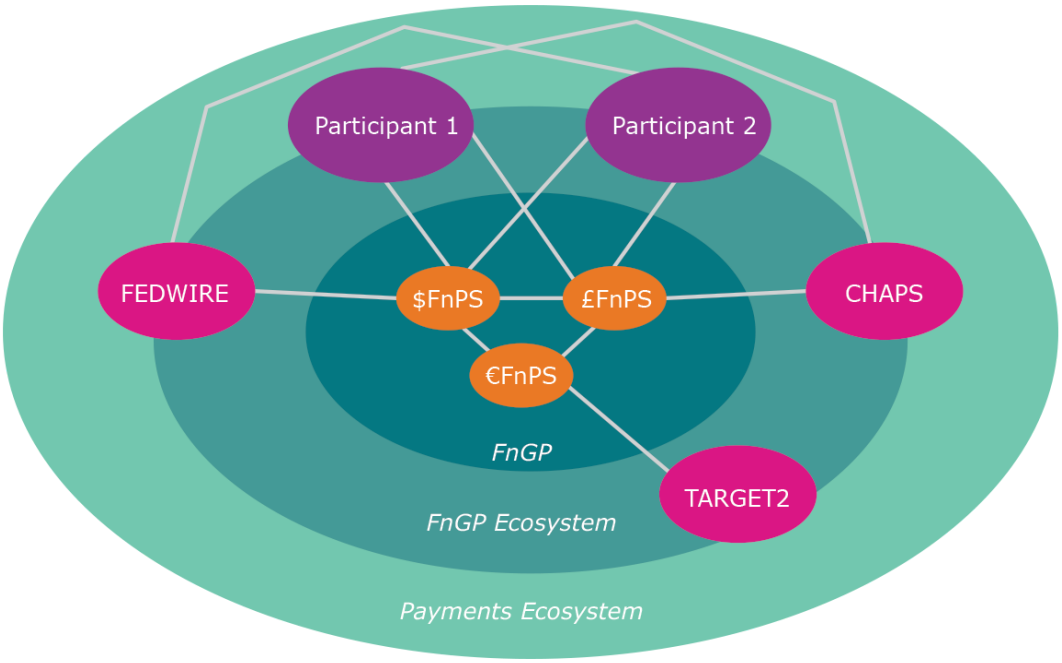


Figure 1: The Fnality Ecosystem

FNALITY'S RISK IDENTIFICATION METHOD

Fnality's Risk Management System (RMS) uses techniques based on the Management of Risk framework which itself is informed by ISO31000:2009 (the international standard for risk management). As per the framework, risks will be identified, triaged, and mitigated.

In concrete terms this is a five-step process:

1. Hazard Review
2. Risk Ideation
3. Transmission Linking
4. Impact Evaluation
5. Risk Mitigation

Hazard Review

The entire ecosystem is reviewed with the aim of identifying hazards. A hazard is a part of the ecosystem that is a source of risk, and identifying them is a useful way of focussing attention onto the riskier parts of that ecosystem. These can be processes, systems, data, groups of people or assets.

As an example, when settling a cross-currency transaction, funds in one FnPS are first earmarked (or reserved) and then funds are earmarked in the other FnPS. Settlement is achieved by the FnPSs exchanging the proofs of earmarking which guarantees atomicity. In this instance, "a funds balance" (the funds used by a Participant to settle transactions) is an asset as it is controlled by a Participant and presents an asset hazard as negative events could affect it. The "proof of earmarking" is a piece of data that flows around the ecosystem and presents a data hazard due to the negative events that can affect it – as we shall see in Risk Ideation.

Risk Ideation

The hazards are now reviewed to identify the adverse events that could potentially affect them. These are the risks and there may be several risks for each hazard. Using the "proof of earmarking" example above, the risks could be that "the proof is lost" or "the proof is communicated slowly".

Transmission Linking

Although risks can occur in isolation, there is usually a cause-and-effect relationship between them. In the above example, if one FnPS blockchain drops below a critical number of nodes (representing a node network hazard) then the probability of the risk of “the proof is communicated slowly” increases, thereby affecting the linked FnPS. These transmissions show how adverse events in one payment system (or indeed participant, supplier or regulator) may transmit to another ecosystem member.

Impact Evaluation

When evaluating the impact of a risk occurring in an ecosystem it depends on each affected organisation’s point of view. The impact of a risk occurring may be an inconvenience for one organisation but terminal for another. The high impact risks can be defined as ‘failure outcomes’ i.e., that cause a risk to financial stability across the ecosystem or to one or more local payment systems, and the objective of the Risk Management System is to ensure they never occur.

Risk Mitigation

The transmission links can be disrupted (and thus the failure outcomes made less likely) using mitigations. The combination of risks and mitigations forms the core of the risk response plan. Ideally mitigations should be as far “upstream” as possible. Mitigations usually take the form of processes or technology.

EXAMPLE RISKS

Table 1 below shows a non-exhaustive list of events that may happen and are outside the Fn Local's[2] control (external events).

A non-exhaustive list of actors who may be responsible for external events are Fnality protocol developers and partners, participants in an FnPS, Fnality staff, central banks, regulators, validator node operators (VNOs) and the SWIFT Bureau Provider.

Possible External Events			
Technology	FN Staff	Participants	Central Banks
Poor work authorising smart contracts	Execute processes poorly	Goes insolvent	Change to laws and regulations
Poor work designing interop protocol	Incorrect manual transfer to ledger	Poor liquidity planning	RTGS system unavailable
SWIFT messages are tampered	Fail to spot changes in participant status	Loss of private key	

Table 1: External Risks for an FnPS

The occurrence of one of these events increases the likelihood of other internal risks occurring which in turn may result in a failure outcome the Fn Local is trying to prevent.

Two of the main internal risks that lead to spillovers are where i) a Participant is unable to make a payment when it is obliged to, and ii) a Participant makes a payment when it should not be able to.

i) Inability to make a payment when a Participant is obliged to – Since both legs (currencies) of a cross-currency transaction need to be transferred simultaneously to avoid a one-sided exposure, the funds of one of the counterparties needs to be earmarked or blocked first on one FnPS ("lead ledger") until the other counterparty has submitted its payment instruction and has enough funds balance to settle the transaction on the other (linked) FnPS ("follow ledger"). If the latter is slow in submitting its payment instruction in the FnPS of the follow ledger, then earmarked funds on the lead ledger cannot be released and are effectively "locked up" for longer, leading to possible settlement delays (and liquidity risk) in the FnPS of the lead ledger. To work this through from the external risk, the steps are:

- Participant plans its liquidity for the day poorly (on the follow ledger)
- Participant does not have enough funds to execute the earmark on the follow ledger for a cross-currency transaction
- Settlement of the cross-currency transaction takes longer than usual
- Earmarked funds on the lead ledger are blocked for longer than usual
- Settlement delays in the FnPS of the lead ledgers (resulting in excessive liquidity risk)

ii) Making a payment when a Participant shouldn't be able to – When Participants can make payments when they shouldn't be able to, there is the chance that those payments will be unwound at a later date, which ultimately leads to excessive operational risk. For example, as part of a Participant's insolvency process, their ability to dispose of their funds balance should be frozen in accordance with the rules and procedures set out in the relevant FnPS Rulebook. Again, working this through from the external risk, the steps are:

- Fnality Staff fail to execute a process within the SLA (service level agreement). In this case the process is to de-permission a Participant's account based on an insolvency notification
- The insolvent Participant makes and receives payments when it shouldn't
- Some payments may then be unwound at a later date
- Excessive Operational Risk for all Participants who have payment obligations with the insolvent Participant, and for Fnality Local who will have to manage the subsequent reversal of payments.

EXAMPLE MITIGATIONS

In general any mitigations will either reduce the likelihood of a risk occurring, or the impact if it does. As risks have a knock-on effect, ideally any mitigations should be as far “upstream” as possible, i.e. if we mitigate the external risks then we reduce the probability and impact of internal risks occurring. Table 2 below shows the potential mitigations for the external risks described above.

Returning to the previous illustration of poor liquidity planning of one of the Participants, a proposed mitigant might be the provision of real-time settlement related data across the FnPSs. Using the historical settlement data in the FnPS in a feedback loop for the Participants should help them improve their intraday liquidity planning in the future. It is also envisaged that each FnPS Rulebook will stipulate clearly when funds are expected to be earmarked on the follow ledger.

For the second example in which a Participant makes and receives payments after it has been declared insolvent by its supervisor(s), a proposed mitigant might be regular testing of the default procedures, including communication between relevant supervisors and the Fnality Locals.

Mitigation Examples	
Technology	
Poor work authoring Smart Contracts	Independent review of smart contracts (EY)
Poor work defining interop protocol	Open source protocol for public s crutiny and enhancements
SWIFT messages are tampered	Supplier contract (including SLAs and liability allocation)
SWIFT Bureau is unavailable	Supplier contract (including SLAs and liability allocation); Manual message insertion (short term); Direct access to Fn Access (long term)
FN Staff	
Fail to execute a process within the SLA (service level agreement)	Culture, Training, Company policies, Management Control
Invalid manual transfer of funds from the System Account	Stric t "8 eyes" approach to manual transfers; Dual signatures
Fail to spot changes in status of participants	Rulebook obligation on Participants to proactively notify changes
Participants	
Goes insolvent	Insolvency plan and annual testing of plan
Plans its liquidity for the day poorly	Providing data to help Participants with Liquidity planning
Breaches Rulebook; Breaches usage limit; fails KYC	Rulebook obligations on Participants (incl. in their capacity as VNOs)
Lost private key	Rulebook obligation on Participant to maintain information security
Central Banks	
Changes applicable law, regulation or policy regarding settlement	Regulation scanning and proactive action
RTGS system unavailable	Highly resilient design of FnPS and FnGP
Changes rules regarding Interop	Regulation scanning and proactive action

Table 2: Mitigations for External Risks

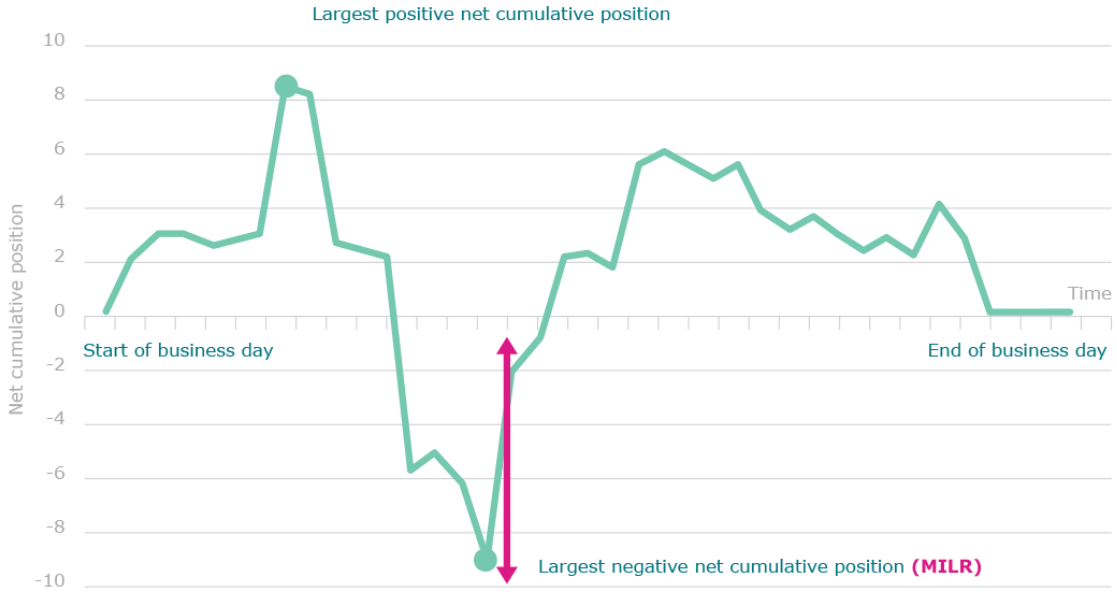
MODELLING A RISK THROUGH SIMULATIONS

Operators of payment systems need to assess, monitor and control risks in a comprehensive way, including risks arising from links with other systems (PFMI #3 and #20). To further this objective, Fnality has partnered with FNA – a deep technology company specialising in simulating and modelling payment systems and networks.

We acknowledge that links between FnPSs in multiple jurisdictions may lead to spillover risks. Extensive quantitative simulation capabilities from FNA lets us explore these risks and quantify their magnitude to display that any additional risk from FnPS utilization is minimal even with extreme FnPS volumes and values.

By way of an example, we specifically tested against the first risk - **Inability to make a payment when a participant is obliged to** - and concluded that it increases the liquidity needs of the other Participants and thus, the system as a whole. This excessive liquidity risk will be analysed against baseline calculations to determine significance.

We measure liquidity risk as the Maximum Intraday Liquidity Requirement (MILR) and its corresponding volatility. **MILR** is calculated as the largest negative net cumulative position of a Participant throughout the day.



We calculate system MILR for a specific payment system by summing the individual MILR for each Participant of said system.

1. Initial assumptions

An FnPS is modelled to interact with the corresponding RTGS system in each jurisdiction. We also simulate CHAPS (£), TARGET2 (EUR), Fedwire ($), BOJ-NET (JPY) and LVTS (CAD). The data used to simulate these systems is based on publicly available network statistics for each system. Liquidity savings mechanisms are integrated and utilised in each FnPS.

We simulate 50-days' worth of representative payments and then plug these payments into each scenario.

The payment distribution is modelled such that a minority of the RTGS and FnPS Participants are responsible for most of the volume/value sent through the system. A CLS participant has also been included to more accurately model each RTGS.

2. Testing and Results

The volumes and values of transactions in the initial stages of Fnality adoption are expected to be too small to present any spillover risk so long-term projections are selected for simulations. There are two levels that we vary to explore impact:

- Fnality utilization level: The number of wholesale payments routed through from FnPS Participants.
- PvP injection level: The number of cross-currency transactions routed through from FnPS participants.

We have three main settings to run through:

1. Standard operations – how does FnPS usage affect the RTGS at baseline?
2. Counterparty stress – how does FnPS usage affect the RTGS under the main liquidity risk scenario?
3. PvP impact – does the injection of PvP transactions affect the conclusions from the above settings?

3. Setting 1: Standard operations

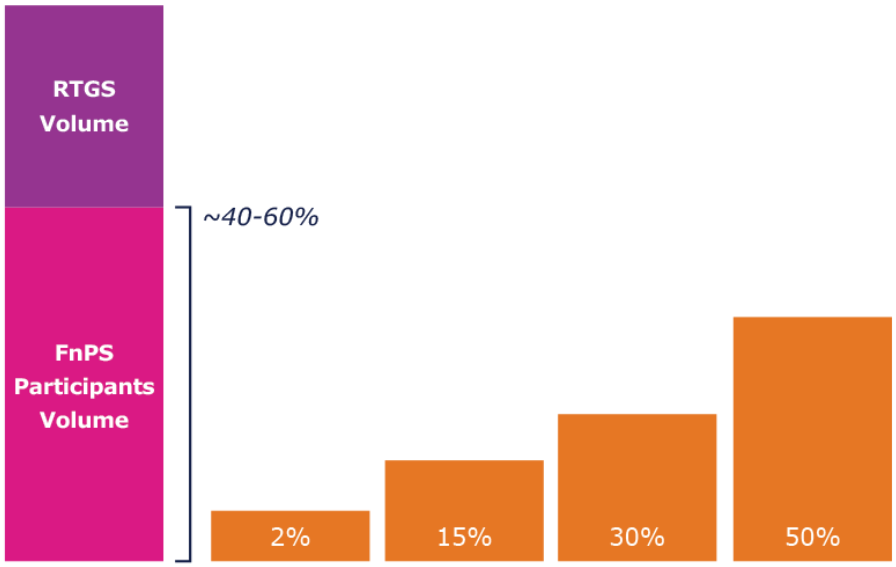
Each RTGS is modelled under standard operations. Some of their traffic is then routed through to the respective FnPS in a growing percentage – the Fnality utilization level.

Baseline calculations of the MILR for each RTGS is then calculated:

System	50-day average MILR
CHAPS	44.4 billion GBP
TARGET2	457 billion EUR
FEDWIRE	660.7 billion USD
BOJ-NET	25.4 trillion JPY
LVTS	39.4 billion CAD

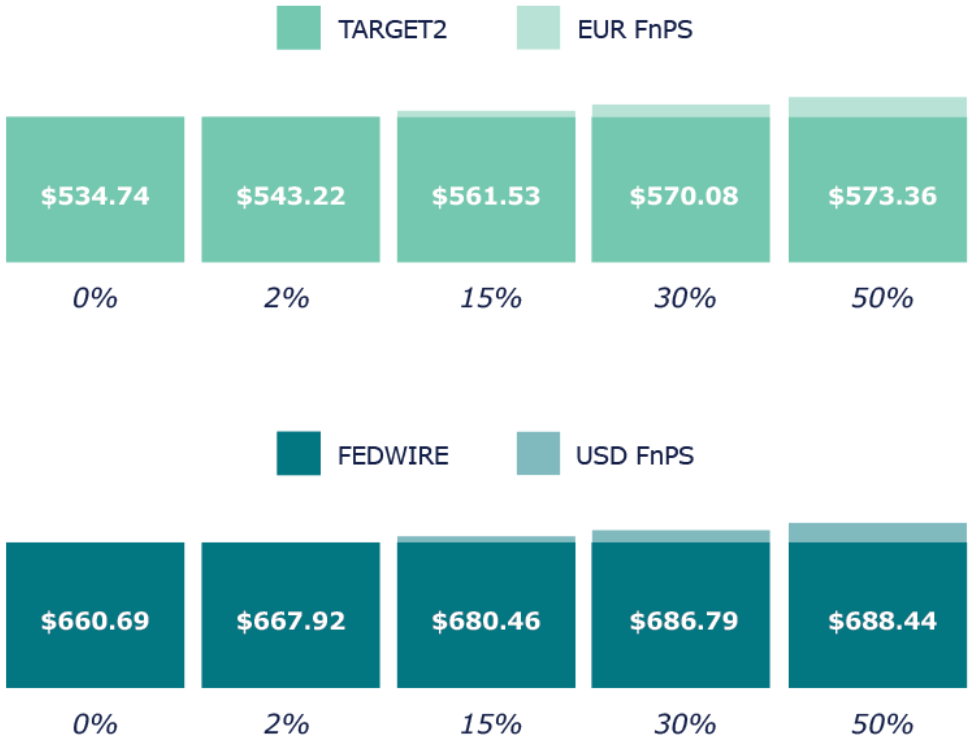
This means that, for example, on average in our 50-day simulations CHAPS requires GBP 44.4 billion to settle every payment made regardless of time. This data will be used as a benchmark and represents the current risk profile of each system.

To determine a reasonable volume of Fnality traffic, we select Participants of varying sizes to become FnPS Participants and then route an increasing percentage of RTGS payments into the FnPS.



To determine if Fnality utilization has elevated the risk levels we observe the overall MILR of both the FnPS and respective RTGS.

The figures on the graphs below denote the MILR for each utilization scenario for the two largest RTGS systems: FEDWIRE and TARGET2. Results are similar for the rest of the RTGS.



Firstly, as expected, there is an increase in the overall MILR due to the initial splitting of liquidity pools, however, we must determine whether this increase is statistically significant.

This can be quantified by looking at the volatility of MILR (measured by its standard deviation) in the RTGS at baseline and comparing this to the increase caused by Fnality utilization.

	50-day standard deviation of milr (billions)	50% Fnality utilization extra liquidity requirement (billions)	% comparison
CHAPS	£5.78	£4.72	82%
TARGET2	€20.21	€33.00	163%
FEDWIRE	$19.85	$27.75	140%
BOJ-NET	¥2389.31	¥2511.21	105%
LVTS	C$5.34	C$2.66	50%

The above table displays the increase of liquidity needs on both the RTGS system and the FnPS per currency in the (extreme) 50% Fnality utilization scenario against the 50 day sample standard deviation of the RTGS MILR baseline (I.e. no Fnality utilization). The extra liquidity falls within two standard deviations for all RTGS systems and one for some – the norm for determining statistical significance. We can thus state that the increase in extra liquidity is not statistically significant within this setting.

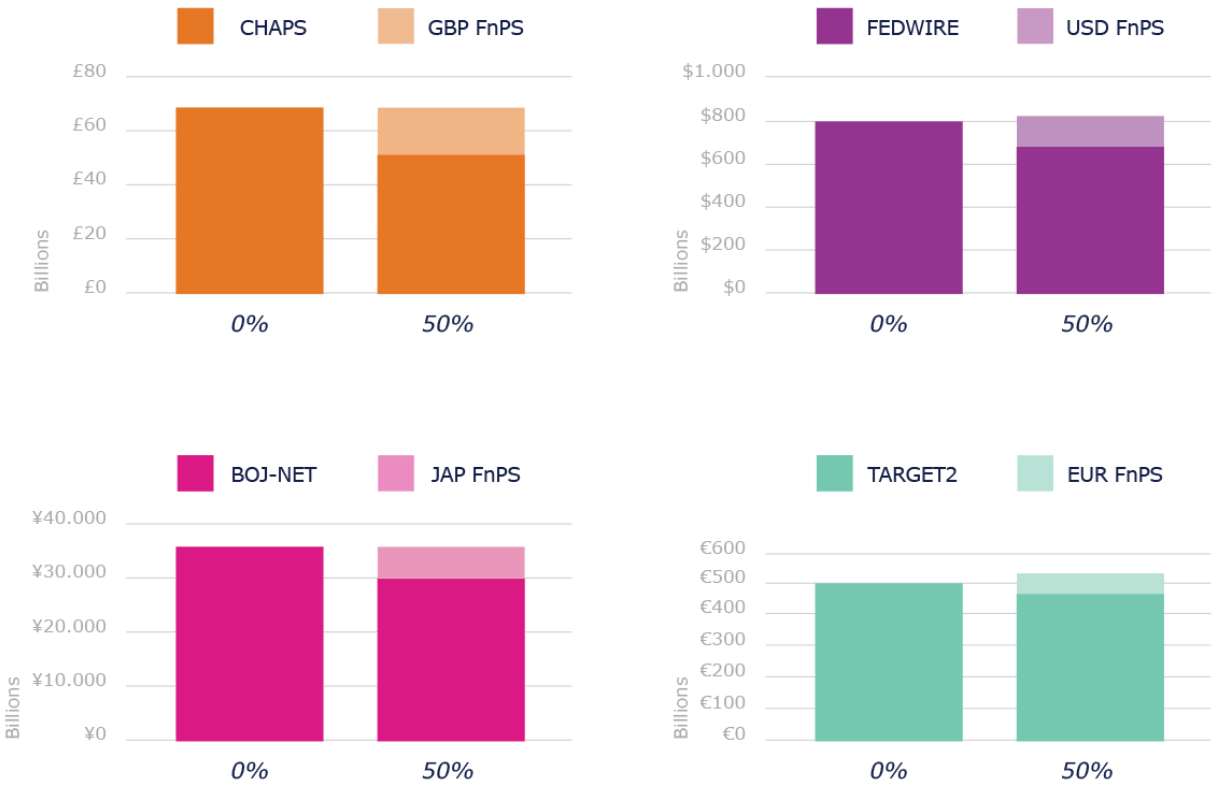
4. Setting 2: Counterparty stress

We test against the main risk of two Participants being unable to make a payment they are obliged to make. This is achieved by selecting the two greatest Participants by volume/value, who participate in both FnPS and RTGS system (of the same currency) and making them unable to make any outgoing payments for a given day.

The impact of these two Participants being offline for a day on the MILR is highly dependent on the assumptions made of the system, e.g., the value and volume of traffic on a “non-stress” day.

CHAPS, as a smaller system, is more disproportionately affected – it experiences an MILR rise of 53.7% on average over the five Fnality utilization scenarios. In comparison, as larger systems, Target2 and FEDWIRE experience an increase of 6.8% and 17.5% respectively. This can be attributed to the fact that CHAPS has fewer participants compared to Fedwire and Target2.

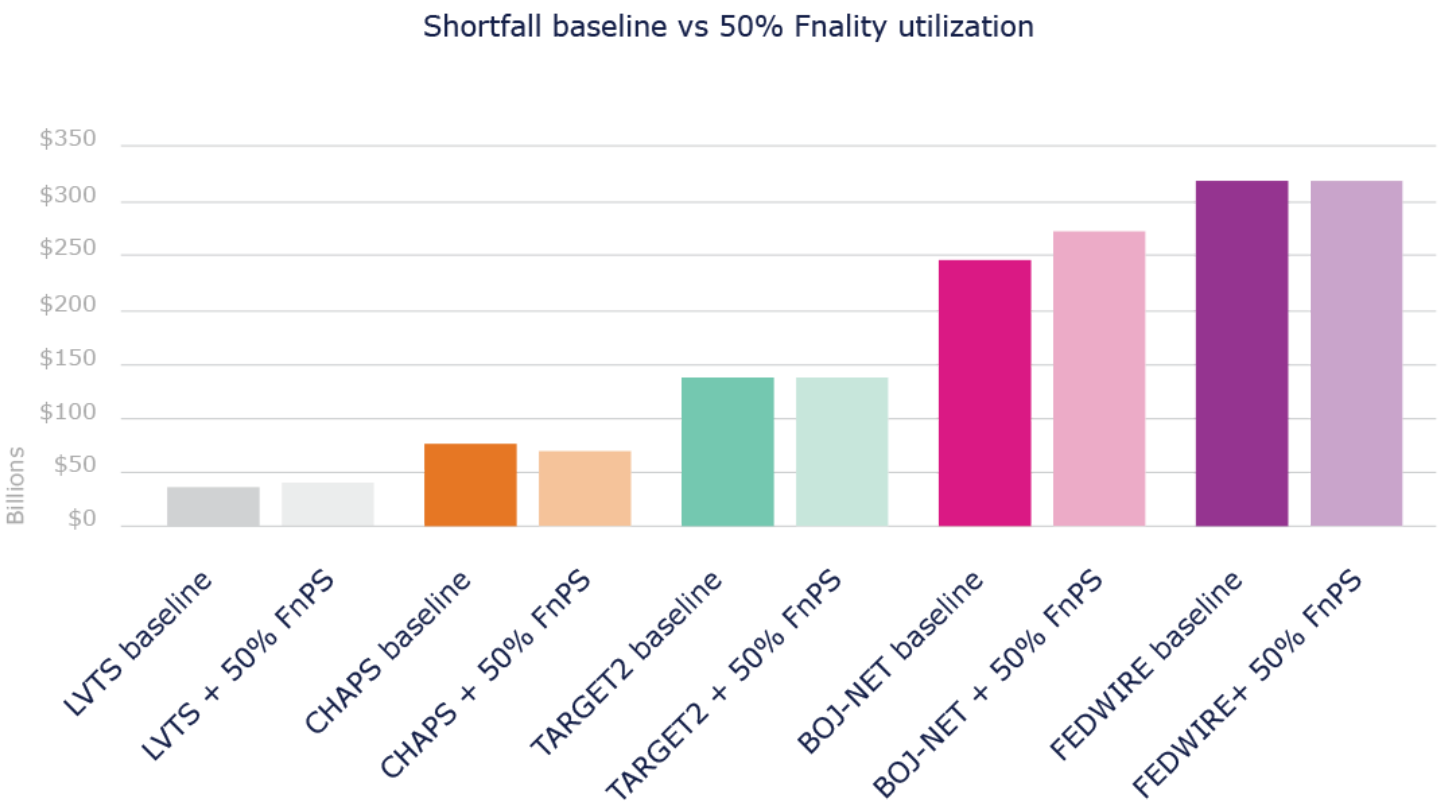
The counterparty stress scenario results in a clear increase in liquidity requirements versus standard operations. To understand the full impact, we look at the MILR for the underlying RTGS payment system and FnPS combined under each Fnality utilization scenario.



Each system reacts differently due to the underlying assumptions made when simulating (e.g. their size and integrated Liquidity Savings Mechanisms) but there is almost no change when comparing to the 0% baseline.

The next metric we use to measure the impact of counterparty stress is the value of payments that would have taken place on a given day but did not due to the missing obliged payments from the two restricted participants. We can see this as the liquidity shortfall for a given day.

Below, you can observe on the left the baseline shortfall, what happens when the stress scenario is imposed without Fnality utilization. The right will then display what happens with the highest level of Fnality utilization (50%).



Above you can observe that the effect of Fnality utilization is marginal to zero. This is to say that Fnality utilization does not increase the number of payments that cannot be made due to the missing liquidity from payments not made by the two offline Participants.

In conclusion, Fnality utilization here does not significantly elevate the MILR for any of the systems under stress and thus does not worsen an adverse event like the large participants not being able to submit payments.

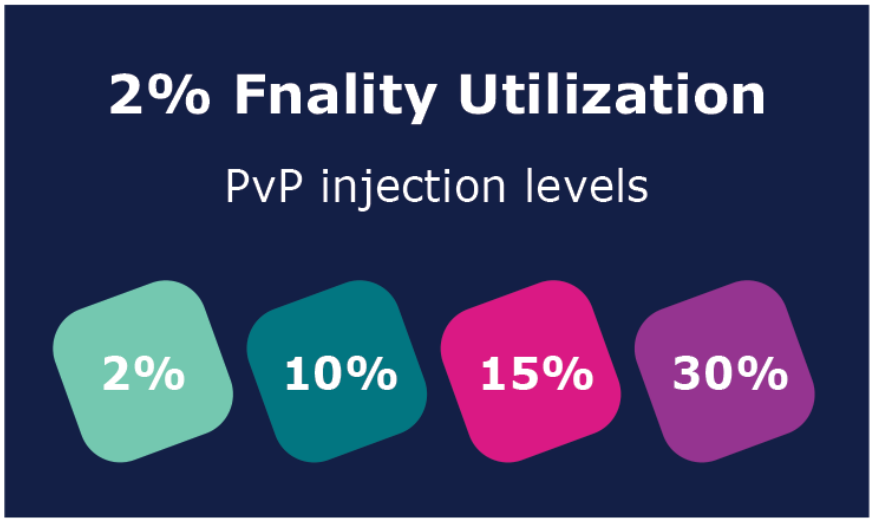
5. Setting 3: PvP impact

The settlement of cross-currency transactions on a PvP basis means that both legs of a trade need to settle concurrently. Generally, we would expect this mechanism to increase the MILR in both systems.

Utilizing publicly available data from CLS and volume predictions from our business plan, we create a representative transaction data which we route through to specific participants who have access to two FnPSs. We utilize the EUR/GBP and USD/GBP currency pairs and thus only route through the payments to participants who are either in both EUR/GBP FnPSs or USD/GBP FnPSs.

With extensive research and use of publicly available data we have determined a level of addressable PvP transactions for a selection of FnPS participants.

The PvP injection level refers to the percentage of the addressable PvP transactions that are routed through to the respective PvP participants in each FnPS. We generate 8 scenarios for each currency pair under the 2% and 15% Fnality utilization scenarios using this combination of wholesale payment and PvP injection levels.

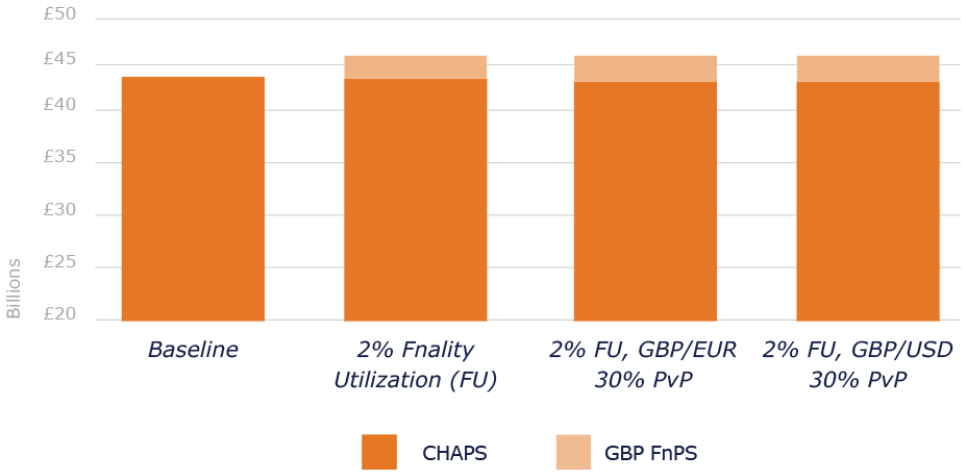


To gauge the effect on the Fnality Ecosystem of the predicted PvP transaction volumes, we take the baseline RTGS systems, increase Fnality utilization to 2% and then route through increasing PvP injection levels.

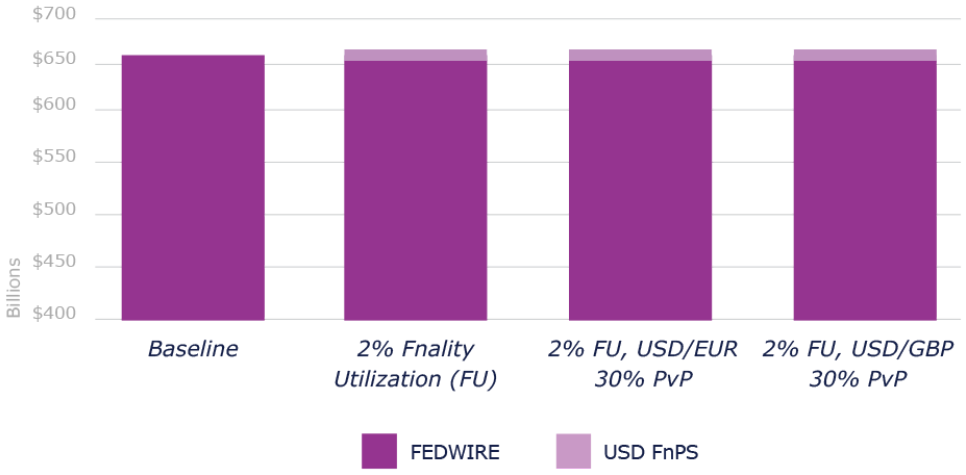
We also tested at a higher Fnality utilization level of 15% and found no significant difference in the conclusions made.

The effects are shown below for each system. In each graph we display the baseline measurement of liquidity required and then show what happens at 2% Fnality utilization, then finally the result when we increase the PvP injection level to 30% for each currency pair.

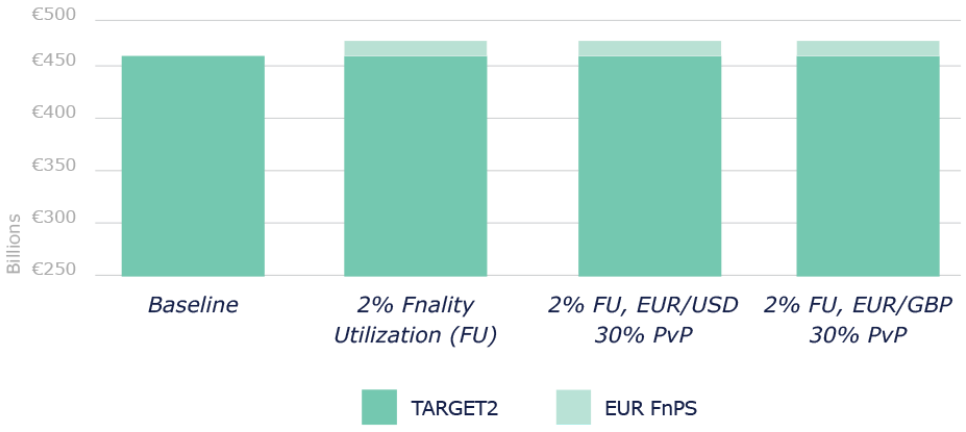
MILR for CHAPS & GBP FnPS in normal operations with PvP



MILR for FEDWIRE & USD FnPS in normal operations with PvP

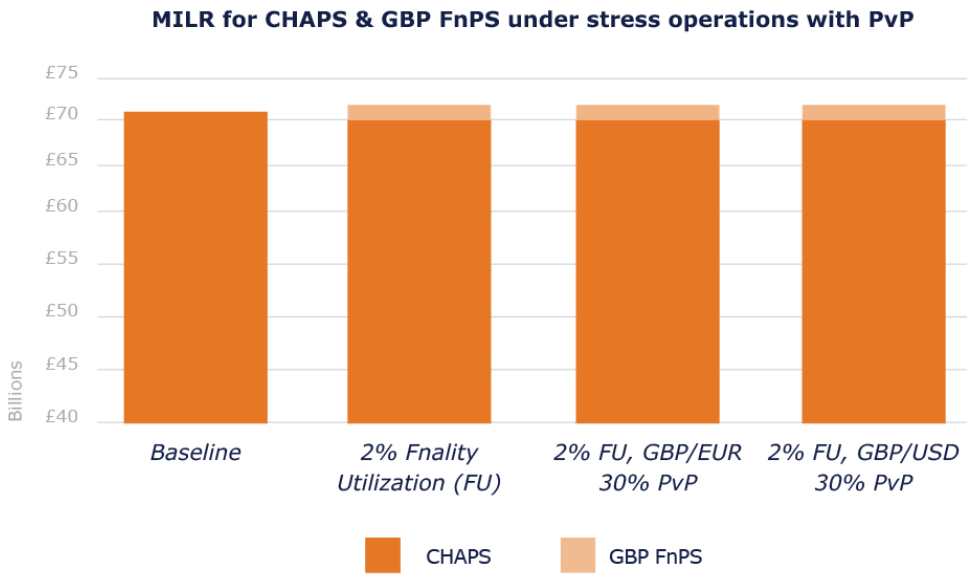


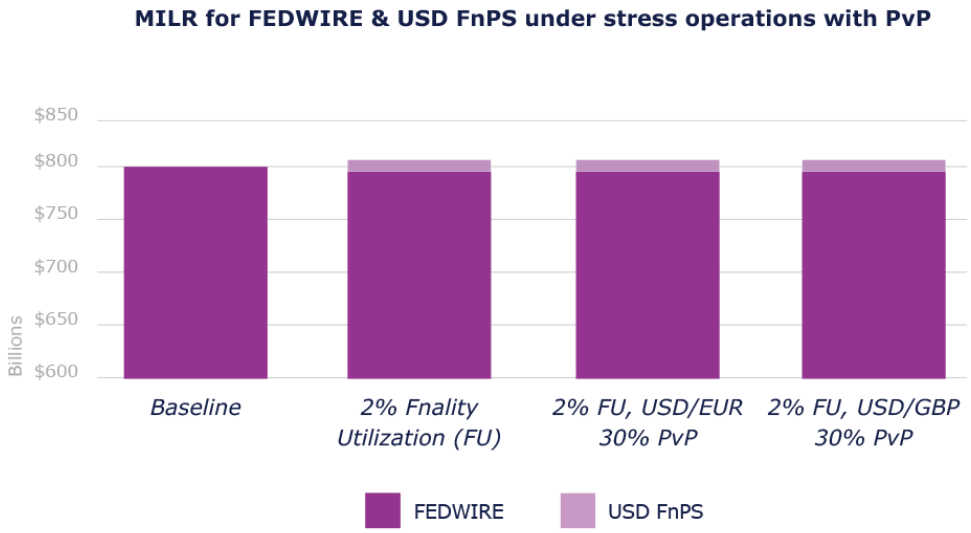
MILR for TARGET2 & EUR FnPS in normal operations with PvP

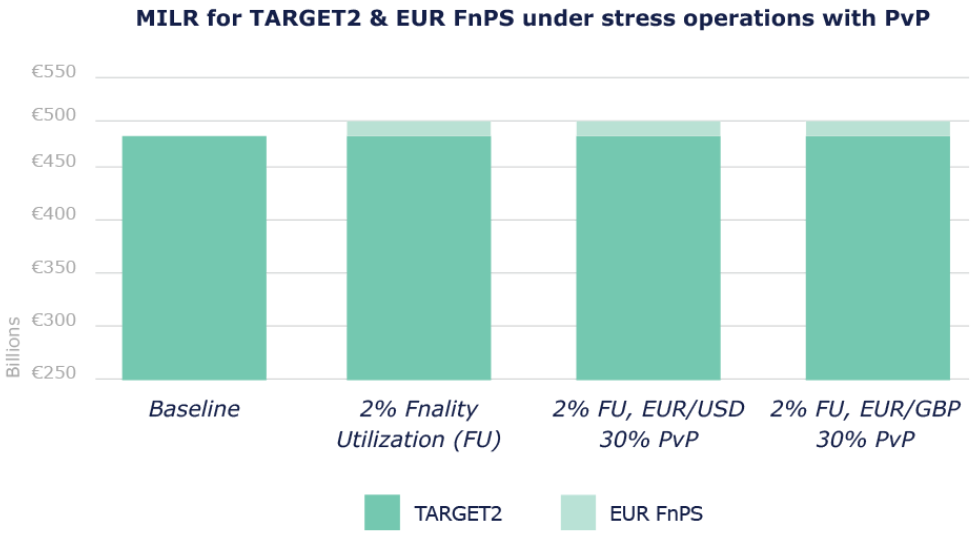


As can be observed from the graphs, even at the highest PvP injection levels the overall effect on the liquidity requirements of the Fnality Ecosystem is not significant. We can thus conclude that under our current modelling, the introduction of cross-currency transactions to the does not significantly elevate the risk profile of the Fnality Ecosystem during normal operations, even at the most optimistic volume projections.

The final point to determine is whether introducing PvP transactions significantly affects the risk profile under the same stress scenario previously defined (failure of the same two participants to submit payments).







The same conclusion can be reached on these graphs – PvP injection and Fnality utilization do not significantly affect the liquidity requirements under this extreme counterparty stress scenario.

Further, when we compare the shortfall, the average across all systems is 3.22% with again a maximum of 13.58% increase in the GBP FnPS in a 15% Fnality utilization scenario.

The conclusion from our modelling is that there is no significant effect on the risk profile of Fnality Ecosystem at baseline or under a counterparty stress scenario with Fnality utilization, even under our most optimistic expectations of wholesale or PvP transaction volumes.

CONCLUSION

Linkages among Financial Market Infrastructures (FMIs) rightly deserve a prominent place in operators' risk management frameworks. Fnality is using both quantitative and qualitative approaches to address these risks.

The results from our extensive simulation exercises show that the impact of liquidity spillover risks appears to be moderate. The introduction of FnPSs as additional payment systems to the central bank operated RTGS systems only moderately increase the liquidity needed for swift settlement. Also, in times of stress, modelled as the failure of two large participants being unable to make payments, the impact of liquidity spillovers between FnPSs appears to be moderate.

Obviously, even the best risk management framework cannot prevent adverse events from happening. Fnality's Risk Management Systems – following international best practice – is geared towards reducing the probability of adverse events from happening, while at the same time, putting in place adequate mitigants against a wide spectrum of such events.

We are confident that we can provide a comprehensive landscape covering all the relevant risks present that may arise.

FOOTNOTES

1 - RTGS systems are used by central banks to implement their monetary policies. They are also the gateway for settlement in other payment systems (sometimes referred to “ancillary systems”).

2 - A FnLocal is the legal entity operating an FnPS in a specific currency.