Introduction and executive summary

This is the second edition of the Bank's Financial Market Infrastructures and Payment Services Report. It covers a wide range of financial market infrastructures (FMIs), custodians, payment service providers and critical service providers for which the Bank is responsible for prudential supervision or oversight, either as lead authority or in cooperation arrangements with other authorities. Although these systems and institutions may differ in scope and size – some of them have international systemic relevance – they all serve as the backbone for processing payments between individuals and/or financial institutions, securities transfers or messages on behalf of participants and/or clients. Therefore, their safe, sound and efficient functioning is one of the priorities of the Bank's supervisory and oversight activities.

The risk environment is evolving and becoming more complex. While physical security risk was a major concern after 9/11, and liquidity risks were one of the main focuses in the aftermath of the Lehman debacle, digital security (including data integrity) dominates risk management agendas today, not least because of a series of cyber heists in the last few years. The Bank is closely monitoring efforts made by the sector of FMIs and payment services to implement the CPMI-IOSCO cyber security guidance. The interconnectivity with other systems, institutions and participants, at wholesale or retail level, adds to the complexity of operational and cyber risks and to the potential impact. Also, the level of interconnectedness in the financial sector can evolve over time. On a longer term, new technologies like blockchain have the potential to lead to a certain degree of disintermediation. In other cases, regulatory initiatives such as the revised EU Payment Services Directive (PSD2) pave the way for the introduction of new stakeholders. With the aim of fostering competition, facilitating and regulating new core services for payment accounts, payment service providers (for the time being mainly banks) are required to open up access to their bank accounts to new categories of regulated institutions (if the bank account holder wishes to do so). This provides access for new, licensed suppliers providing new services using bank account data, which were until now in the remit of the traditional players (banks). Access to and storage of such sensitive (payments) data requires appropriate risk management.

As a rule, a chain of actors (connected systems, institutions and their participants or clients) is as strong as the weakest link between the nodes. Participants/clients, sometimes at the periphery of the network, are part of the so-called endpoints in the payment chain. The article on endpoint security strategies to mitigate payment fraud builds further on the CPMI report on wholesale payments security. It covers and compares strategies sponsored by different stakeholders in different areas of the sector of FMIs and payment services. As payment system operator, the central bank community itself should implement these endpoint security strategies, whereas in its role as supervisor or as catalyst, it should monitor and promote implementation in privately operated systems.

Like last year, the Report covers changes in the regulatory environment, as well as the Bank's oversight and prudential supervisory approaches, and its main priorities for 2018. In addition, the Report zooms in on specific themes such as developments in the sector of payment institutions and electronic money institutions, the role of cards as payment instrument in Belgium, while for other systems or institutions specific information is provided on their international dimension. As the Report is intended as a reference document, annexes on applicable rules/principles and statistics provide further insight for those interested.