Key Takeaways | Frankfurt, Germany

Roundtable on Payments and Technology

October 2023

Perspectives on Cross-Border Payments
Efforts to improve global cross-border payments continue to advance toward better outcomes for end users in a digitizing economy; however, we are at an inflection point with new hurdles emerging in the path ahead. Challenging targets have been set for cost, speed, and transparency by the public sector, while emerging threats to trust and security—driven by AI, tech, and geopolitical conflict—have merited ever-increasing industry attention and resources.

On October 17th, the IIF, in partnership with Visa, convened leaders from banks, payments networks, and technology firms to discuss these issues with global standard setters and central bankers. Two main themes were set for the dialogue, "Ecosystem Developments and Risk" and "Investing in Security and Innovation". The agenda was designed to share perspectives on pathways to advance customer-focused outcomes in a rapidly shifting external environment characterized by rising cases of AI-linked fraud and improvements in speed challenged by reporting requirements. The dialogue reflected key points in global efforts to improve payments.

The impact of data frameworks is significant but difficult to see. The requirement to ensure data security throughout the payment lifecycle is a significant factor limiting progress toward G20 targets. Institutions noted that data privacy rules in certain markets prevent them from sharing details of accounts they have identified as fraudulent. Solutions attempting to ameliorate these data sharing challenges can take the form of data repositories, such as in the Swiss example, where permissioned networks enable institutions and the public sector to access information on proven bad actors without fully identifying the accounts. Private sector participants also asked for pathways for two-way sharing to be developed – e.g. relevant authorities could share indicators of bad actor-linked accounts with the banks to mitigate banks' time wasted looking for the proverbial needle in the haystack. Such two-way sharing could complement (not replace) existing AML/CFT efforts to increase effectiveness and reduce associated costs. Presently, the system relies on private entities meeting increasingly complex compliance burdens due to evolving illicit networks, driving up costs.

Compliance costs are one of the two main drivers of cost to the end user, the other being foreign exchange costs. Of the two, the cost of compliance is the element continuing to increase. There may be an opportunity to alter the pricing dynamics by rethinking the bundling and processes necessary for compliance, but that will require official sector support. All in, meeting targets set by the FSB, among others, is a much more complex endeavor than reports reflect.

The current gold standard is zero-trust proofs; for this system to operate, data must be technologically verifiable end-to-end, necessitating that the payment and information about the payment move together. Accomplishing this movement requires greater technology investigation and richer data environments than currently implemented.

Foreign Exchange (FX) is currently viewed as a significant cost driver, but it could in fact be a place where firms are receiving revenue to cover other costs (such as the growing compliance costs noted above) driven by requirements in other areas; hence, the complexity of bundling.

Investment in the future of payment innovation and security requires the possibility of a return. There could be limited incentives to innovate or develop new payments solutions and security if policy pressures continue to constrain financial institutions' ability to charge customers for improved service. In other words, if there is no return on developing a better product and systems, because developers cannot charge a market price to use it, then investment in the next generation of payments will be curtailed.

Customer needs are diverse but global targets and KPIs lump together a broad array of payment types, diverse customer needs, and priorities. For instance, how fast is fast enough? Sometimes instant transfers are not necessary from the standpoint of customer needs and efforts could be better spent/resources could be better allocated to securing systems.

Big stakes for ISO 20022 and harmonization are driven by the same cost dynamic outlined above. ISO 20022 has been the single most expensive payments initiative for the financial industry, and it is still ongoing. Talk of upgrading data sharing further in common standards will come up against financial constraints and commercial abilities of banks. Finding the correct degree of harmonization in ISO 20022 will be important while API solutions could improve outcomes. While the benefits may take time to come to full fruition, the improvement derived from data made more consistent and accessible via ISO 20022, when implemented, will be very beneficial for the financial services industry.

New frontiers of fraud have emerged. GenAI and other new technologies are driving down the cost to commit fraud, while the cost to prevent fraud is simultaneously going up in this new technology era. The operating environment will feature these dynamics, potentially forever, which should prompt the industry to study the types of data it uses, the way it uses it, and to think creatively about managing these risks. Fighting fraud gets more complex every day, with growing vectors of attack with every additional technological innovation.

The road ahead toward more secure, more transparent, faster, and cheaper payments could use some fresh thinking. A useful exercise may be to work backwards from idealized standards and then figure out what achieving those targets would entail in terms of time, cost, and security. What would need to change to make a given pathway or corridor economically viable? Would a change in the volume of investment in or funds transiting an emerging market corridor change the viability of continuing to service it/lower the cost of doing so, for instance? If so, what can be done?