



Workshop on environmental readiness for e-commerce: economic, legal and institutional factors

Session 3 : E-payment infrastructure for e-commerce and cross-border e-commerce

Shanghai, China
6-7 December 2018

Boon-Hiong Chan
GTB Market Advocacy

For more information
on Market Advocacy



What we understand



1. Overview of electronic payment infrastructure (method)
2. Interoperability among various payment solutions
3. E-payment for cross-border e-commerce transactions
4. Legal and regulatory environment



Overview. Some electronic payment methods

1. Credit card model
2. Telecom model
3. Fintech – Third Party Payment (in App)
4. Fintech – Third Party Payment (e-wallet)
5. “Virtual currency”
6. Bank – Debit Card, QR Code
7. Bank – Instant Payment
8. Bank – High Value Cross-Border, GPI
9. Future – Machine-to-machine supermicro payment

Some banking
infrastructure
involvement

Domestic and/or
cross-border
payments

Same payment
method,
“interoperability”
across border

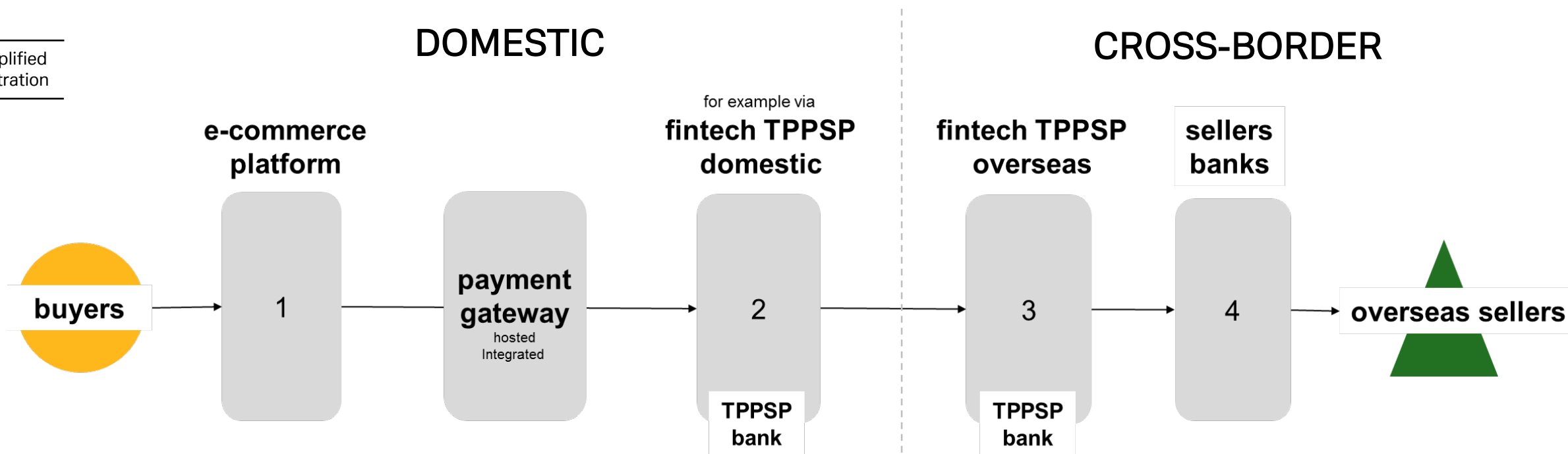
Different payment
“interoperability”
via software
payment gateway

Market behavior /
adoption is
important

Bank and Fintech (and Telco) collaboration for cross-border e-payments



Simplified
illustration



- Buyer transfer funds to e-commerce bank account
- E-commerce transfers funds to TPPSP bank account
- TPPSP, via its local bank, pays local seller in local currency
- TPPSP executes FX with its local bank and bulk remits to overseas TPPSP bank account to pay overseas sellers

- TPPSP foreign bank account receives funds
- TPPSP overseas receives beneficiary sellers' details
- TPPSP's bank(s) pays overseas sellers via local transfers

TPPSP – Third Party Payment Service Provider

NB: Flows can be different for different cross-border payment methods e.g. QR code, Telco wallets, etc.



Legal and regulatory considerations

REGULATE BY ENTITY

E.g. Payment systems.

TRANSACTION VISIBILITY

E.g. Fintech payment clearing.

ACCOUNT AT CENTRAL BANK

E.g. Restricted currency accounts, reports.

REGULATE BY ACTIVITY; DEFINITIONS

E.g. E-money, E-wallet, Stored Value, Virtual Currency, Private Money, etc.

DATA GOVERNANCE

E.g. Privacy, confidentiality, discriminative, manipulative, etc.

FUTURE DIGITAL CURRENCY

E.g. Central Bank Digital Currency and digital legal tender as digital cashless shifts trust from central bank-backed bills to technology and credit risks.

AML/CFT

E.g. criminal liabilities.

DATA LOCALISATION

E.g. What is a minimal set of data. Is data mirroring allowed to facilitate transaction monitoring? Is there any spill over effect to payment systems hardware?

E-COMMERCE TAX

E.g. Who is responsible to calculate, to collect, etc?

CROSS-BORDER DATA ACCESS

E.g. For enforcement purposes.



Market practice considerations

TRANSACTION MESSAGE FORMAT

E.g. Does the transaction message format contain complete information for sanctions, AML/CFT screening?

SHARED RESPONSIBILITY MODEL

E.g. what is the shared responsibilities between Banks, Fintech and Cloud computing service providers?

CONTROLS

E.g. What are the transaction controls as a result of instant payments, high-volume low value transactions?

VIRTUAL CURRENCIES

E.g. What is the expectations for KYC, fraud monitoring, AML/CFT standards on banks and non-bank participants?

FAIRNESS, EQUITABILITY & PROPORTIONALITY

E.g. What is the responsibility standard for the same data handled by a bank and fintech? Is the standard for KYC/AML/CFT and cybersecurity similar too?



Other environmental readiness considerations

ROLE OF TELCO

E.g. in Telco-led e-wallets?

PHYSICAL CONNECTIVITY

E.G. Latency, network speed and the implications on e-payment transaction cybersecurity?

DIGITAL EVIDENCE FOR ENFORCEMENT

E.g. What is a minimum set of digital evidence and storage duration?
Is this standard the same for cross-industry participants?

DIGITAL ANTI-COMPETITIVE PRACTICES

E.g. Data and other new indicators of barriers to competition in e-payments.
Is it anti-competitive practice or the results of faster innovation, greater adoption, network effects and efficiency benefits?

DIGITAL IDENTITY

E.g. Is it complete and reliable for KYC purposes?
Can it flow cross-border to facilitate KYC/AML/CFT monitoring?

CONSUMER PROTECTION

CYBERSECURITY, DATA INSURANCE

E.g. Is there availability of cybersecurity and data insurance?
What do they cover in an environment of interdependencies?

TOOLS & EXPERTISE

E.g. Are there appropriate product and policy/regulatory sandboxes, expertise availability and training?

Disclaimer



Copyright © December 2018 Deutsche Bank AG. All rights reserved.

This document is intended for discussion purposes only. It does not create any legally binding obligations on the part of Deutsche Bank AG and/or its affiliates (“DB”). The information contained in this document is based on material we believe to be reliable; however, we do not represent that it is accurate, current, complete, or error free. Any opinions expressed herein may differ from the opinions expressed by other DB departments. Without limitation, this document does not constitute a DB’s view, an offer, an invitation to offer or a recommendation to enter into any transaction. DB is not acting as your financial advisor or in any other fiduciary capacity with respect to this document. The transaction(s) or product(s) mentioned herein may not be appropriate for all users and before entering into any transaction you should take steps to ensure that you fully understand the transaction and have made an independent assessment of the appropriateness of the transaction in the light of your own objectives and circumstances, including the possible risks and benefits of entering into such transaction. You should also consider seeking advice from your own advisers in making this assessment. If you decide to enter into a transaction with DB, you do so in reliance on your own judgment. DB may engage in transactions in a manner inconsistent with the views discussed herein. DB trades or may trade as principal in the instruments (or related derivatives) discussed herein. The distribution of this document and availability of these products and services in certain jurisdictions may be restricted by law. You may not distribute this document, in whole or in part, without our express written permission. DB SPECIFICALLY DISCLAIMS ALL LIABILITY FOR ANY DIRECT INDIRECT, CONSEQUENTIAL OR OTHER LOSSES OR DAMAGES INCLUDING LOSS OF PROFITS INCURRED BY YOU OR ANY THIRD PARTY THAT MAY ARISE FROM ANY RELIANCE ON THIS DOCUMENT FOR THE RELIABILITY, ACCURACY, COMPLETENESS OR TIMELINESS THEREFORE. Deutsche Bank AG, including its subsidiaries and affiliates, does not provide legal, tax or accounting advice. The recipient of this communication should seek advice from an independent tax advisor regarding any tax matters addressed herein based on its particular circumstances. Deutsche Bank AG is authorised under German Banking Law (competent authorities: European Central Bank and German Federal Financial Supervisory Authority (BaFin) and, in the United Kingdom, by the Prudential Regulation Authority. It is subject to supervision by the European Central Bank and the BaFin, and to limited supervision in the United Kingdom by the Prudential Regulation Authority and the Financial Conduct Authority. Details about the extent of our authorisation and supervision by these authorities are available on request.