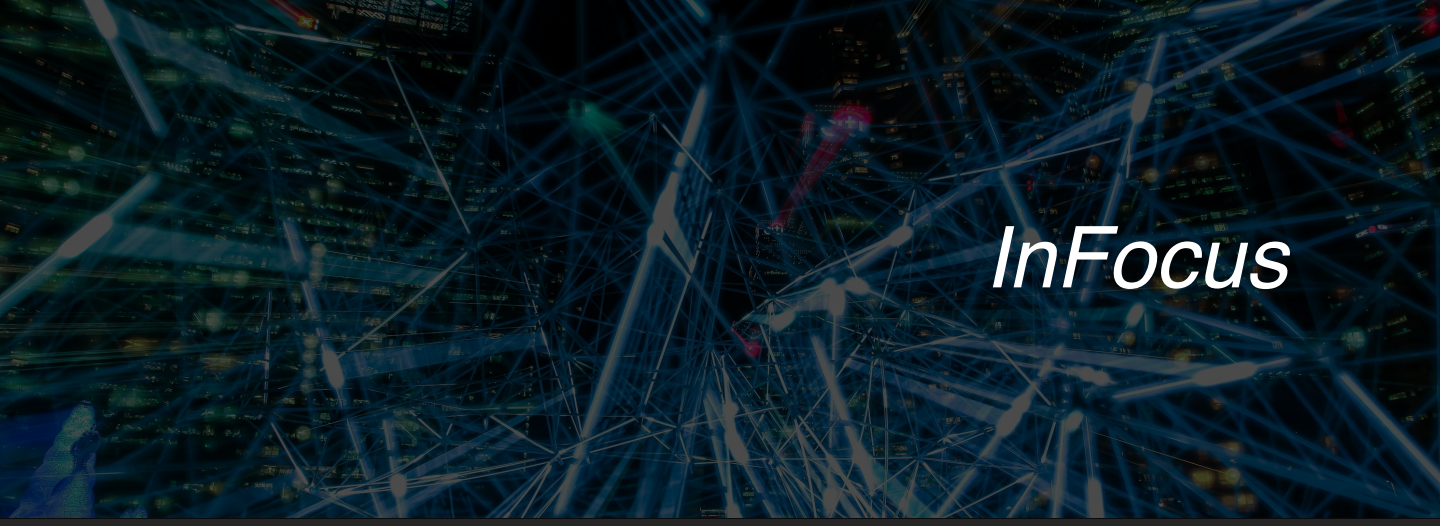

InFocus

Open Banking Module Summary

A summary of open banking regulations issued by the Central Bank of Bahrain

FinTech Consortium

Bahrain FinTech Bay

INTRODUCTION

During November 2018, the Central Bank of Bahrain (CBB) announced the launch of draft rules (25 pages) on open banking. The document is directed toward open banking operators that provide either of the following services:

- Providers of account information
- Providers of payment initiation

The common factor between both of these regulated services consist of gaining access to customer accounts from electronic wallets, conventional Islamic and retail banks through 'application program interfaces' (APIs).

TIMELINE OF OPEN BANKING DEVELOPMENTS IN BAHRAIN

- April 2018 - Tarabut Gateway joins the regulatory sandbox as first open banking applicant
- 11 November 2018 - CBB issues open banking draft rules
- 25 November 2018 - Deadline for feedback on open banking draft rules
- 11 December 2018 - Tarabut Gateway graduates from regulatory sandbox

DEFINITIONS

- Application Program Interfaces (API): API consists of a software intermediary that allows two applications to interact.

- Account Information Service Providers (AISPs): A CBB-licensed entity that provides online account information services.

- Payment Initiation Service Providers (PISPs): A CBB-licensed entity that provides online payment services.

Key themes

Legal Arrangements

AISPs and PISPs must establish a legal arrangement with customers. They must provide customers with information regarding the service, the provider, adopted safeguard and corrective measures, as well as any alterations to the legal arrangement including its termination. Such information must be provided prior to customers being bound by the legal arrangement for the services.

Standards for Authentication and Communication

AISPs and PISPs must have a secure customer authentication process and overall security approach for the following three primary elements:

- Knowledge: information that is only known to the customer of the platforms e.g. passwords
- Possession: something that only the customer possess e.g. algorithm specifications
- Inherence: focuses on devices or softwares that read an element of the customer e.g. biometric sensor

The security measures for each element must be independent to avoid compromise especially in cases when the same device (such as a mobile phone or tablet) is used for more than one operation.

Payment Transactions

Customers must consent to initiate payment transactions. The PISP may agree on payment transaction limits and stop the use of a payment instrument if it compromises the security of the payment instrument or there is suspected unauthorized or fraudulent use of the payment instrument. There is no specific amount mentioned as a limit therefore indicating it is a case-by-case situation. The AISPs and PISPs may implement fees and charges, which reasonably correspond to operational costs, but should be explicitly agreed on by both parties in the initial legal arrangements.

Security

Both AISPs and PISPs are obligated to hire a third-party cybersecurity specialist to perform vulnerability assessments and penetration testing every six months. Separately, external consultants need to also evaluate the operator's systems at least once every three years.

Technology requirements

AISPs and PISPs must adhere to the best practices of technical standards, including for application program interfaces (APIs), electronic identification, transmission of data and web security. Technology architecture that uses “screen scraping” method must not be used. AISPs and PISPs in conjunction with licensees maintaining customer accounts shall develop an open banking API standard based on a standard adopted in a leading financial center, which should be subject to independent tests, including testing in a test environment.

CONCLUSION

This summary highlights key requirements and recommendations by the CBB for open banking. The introduced regulation is directed toward open banking operators that are providers of account information and/or providers of payment initiation. Following the launch of regulations, the local ecosystem welcomed the first graduate of the regulatory sandbox; the first open banking service provider in Bahrain. With the graduate’s solution successfully integrated with over 11 local banks, open banking in the future will enable FinTechs to integrate and innovate more seamlessly with financial institutions.