FIGI Working Groups

The FIGI Working Groups develop knowledge, technical tools, and policy recommendations on the following three areas: Security (including Cyber Security), Digital ID for Financial Services, and Electronic Payments Acceptance.

Security, Infrastructure and Trust (SIT) Working Group:

The Security, Infrastructure and Trust (SIT) Working Group, led by the International Telecommunications Union, aims to build confidence and trust in the use of digital financial services and develop tools to assess digital financial service provider security compliance, address digital fraud, protect the privacy of consumer data and investigate interoperable authentication technologies for security digital financial services. The SIT Working Group is broken into 4 workstreams: (i) Security (Application Security for DFS Applications; Telecommunications Infrastructure Security and Security Assurance Framework; Interoperable Authentication Technologies for DFS); (ii) Trust; (iii) Quality of Service (QoS); and (iv) Distributed ledger technologies (DLT). Recently, the SIT Working Group has released several new reports and guidance notes that are particularly relevant towards ensuring security and business continuity with telecommunications against the current landscape of Covid-19:

- The first new report, entitled '**SS7 Vulnerabilities and Mitigation Measures for Digital Financial Services Transactions**', provides an analysis of telecom vulnerabilities and their impact on digital financial services, both for end-users and service providers, with the overall aim to help providers of digital financial services understand telecom vulnerabilities and the mitigation strategies to safeguard their clients.
- The second report, entitled '**Unlicensed Digital Investment Schemes (UDIS)**', focuses on 3 countries (India, Kenya, and Nigeria) to analyze the legal and regulatory frameworks under which these unlicensed schemes thrive, and to provide an understanding of the impact of this fraud on both the consumers and the financial sector.
- The guidance note presents a '**Methodology for measurement of Quality of Service (QoS) Key Performance Indicators (KPIs) for Digital Financial Services**', which is geared towards helping policymakers and industry stakeholders to define processes for carrying out DFS QoS field tests, procedures to assure data quality and integrity of the KPI results, and to establish a data driven basis for both telecom regulators and DFS operators to define requirements in order to assure a good service quality for DFS.

This methodology has now become an international standard, **ITU-T Recommendation P.1502 Methodology for QoE testing for DFS**.

- The SIT working group also completed their compilation of **developer resources for strong authentication frameworks** in June 2019.

Cybersecurity for Financial Market Infrastructures Workstream (SIT Working Group):

The Cybersecurity for Financial Market Infrastructure Workstream, led by the WBG as part of the SIT Working Group, aims to explore compliance and best practices for cybersecurity specifically on financial infrastructures. A toolkit of resources and materials has been developed as a resource for awareness and education for policymakers and related stakeholders and has recently issued a newsletter to stay informed of new issues related to cyber security.

This workstream, together with the with the European Central Bank (ECB), published the '**Cyber Resilience for Financial Market Infrastructures**' report, which presents a methodology developed by the ECB to operationalize the Guidance on Cyber Resilience for FMIs provided by the Committee on Payments and Market Infrastructure (CPMI)—International Organization of Securities Commission (IOSCO). The methodology presented within this report can be used by FMIs and authorities to comply with and assess their FMIs against the **CPMI-IOSCO Guidance**, thereby enhancing the overall cyber resilience of financial market infrastructures critical for financial stability and financial inclusion.

Digital Identification for Financial Services Working Group:

The Digital ID (ID) Working Group, led by the WBG, aims to identify and accelerate the use of digital identification for expanding access to, and improving uptake of, financial services. This working group will work closely with the WBG's Identification for Development (ID4D) initiative to identify ways to leverage IDs for financial inclusion, including through digital platforms.

The Working group published a **blog post** on highlights from the **G20 Digital Identity Onboarding report**, with a particular emphasis on policy considerations relevant to digital ID for the financial sector. Many of the principles relevant to ID as a whole as have been outlined in the ID4D **Principles on Identification**. The FIGI Digital ID working group is working to translate these policy considerations into practical approaches that can be applied at the national level given different country contexts and regulatory frameworks that pertain to the financial sector. The working group is also developing an ID assessment

tool for the financial sector, which complements the **Identification for Development** (ID4D) Identity Management System Analysis (IMSA) **framework**.

Most recently, the FIGI Digital ID Working Group contributed to FATF's **Guidance on Digital ID**, which was initially circulated as a draft for **public consultation** in November, 2019. This highlights the benefits of trustworthy digital identity for improving the security, privacy and the convenience of identifying people remotely for both onboarding and conducting transactions while also mitigating ML/TF risks. As a response to COVID-19, the FATF have released a **statement** in April 2020 related to simplified CDD measures and the use of Digital ID and implications of digital/contactless payments and digital onboarding to reduce the risk of spreading the virus.

Electronic Payments Acceptance Working Group:

The Electronic Payments Acceptance (EPA) Working Group, led by the WBG, aims to foster effective practices for enabling and encouraging acceptance and use of electronic payments, with an emphasis on person-to-business (P2B) payments, both for proximity payments at the point of interaction and e-commerce, and on unserved and underserved groups. This working group works on advancing the understanding of effective practices for enabling merchant acceptance of electronic payments, in the interest of reducing dependencies on "cash out", and increasing the prevalence of cashless transactions with MSMEs, including through e-commerce. The working group also focuses on improving usage of electronic payments, including through policies and incentives.

The group recently released a new report entitled '**Electronic Payments Acceptance Incentives: Literature Review and Country Examples'**, which collates and summarizes existing literature covering electronic payments acceptance incentives, country examples and identifies emerging trends.