Baker McKenzie.

HONG KONG

Data Journey Map for Virtual Communications

Primer for Financial Institutions

COVID-19 is making physical meetings more difficult or undesirable, and all of us are regularly using virtual communications. However, in adopting virtual channels to deliver products and services financial institutions need to work through issues touching on financial regulation, data privacy and technology. This Data Journey Map developed by Baker McKenzie cross-disciplinary experts helps guide your organisation through these questions at a high level. In ten steps, it flags up considerations which should form part and parcel of your risk and compliance assessments with a view to mitigating the potential risks of supervisory intervention and litigation.

STEP 1 APPLICABLE LAWS AND SUPERVISING AUTHORITIES

Ask what laws apply to the bank / licensed corporation / insurance company / stored value facility operator / money services operator? Which regulator(s) supervise the entity? Has specific guidance on the use of virtual meeting technology been issued?

STEP 2 RESIDENCY REQUIREMENTS

Virtual meetings remain subject to local residency requirements regarding licensing.

Restrictions on **the offer and sale** of regulated products and services to Hong Kong persons still apply to offshore entities. What if HK-based financial services are offered to offshore clients?

STEP 3 VIRTUAL TECHNOLOGY SELECTION

All outsourced functions and technical solutions must be adequately assessed to meet the relevant outsourcing guidelines and legal and security requirements. These may include, as applicable, record keeping approvals, cybersecurity and data transfer requirements.

STEP 4 INTERNAL APPROVALS

Has the appropriate officer or oversight committee for the firm approved these forms of meetings and relevant processes and procedures? Has that approval been adequately documented along with the processes and procedures?

STEP 5 SUPERVISORY OBLIGATIONS

Does the virtual technology solution allow you to adequately supervise activities of any regulated persons? Can sessions be recorded and retained (i.e., like phone calls) to meet regulatory requirements? Where are the records maintained and has any necessary regulatory approval been obtained?

Update policies and procedures to reflect these requirements.

STEP 6 PRIVACY AND CYBERSECURITY

Prepare an appropriate Incident Response Plan to address any unusual situation occurring in a virtual session e.g., unauthorised persons join or intercept the call either inadvertently or for malicious reasons? Ensure that a trial run has been undertaken so people are familiar with the process and are ready to respond.

STEP 7 CUSTOMER NOTICES

Develop clear written explanations and checklists for employees on how virtual meetings will be conducted. What type of information should customers be expected to supply/provide during the meeting?

STEP 8 TRAINING

Develop mandatory training for employees addressing one-on-one conversations and when appropriate/inappropriate to present to groups (which could trigger additional regulatory or privacy requirements).

STEP 9 DEPLOY IN PHASES

Test the experience before a full deployment. Assess the challenges and risks against those anticipated before launch. Conduct post call audit processes to ensure that employees are conforming to firm requirements.

STEP 10 EDUCATE YOUR CUSTOMERS

Explain the limitations of virtual meetings. Some activities may still require e-mail or other steps. Provide the explanations in writing to customers so there is no question regarding receipt.

Contacts

DATA PRIVACY AND SECURITY

We advise multinational companies on all aspects of data privacy, security and information management. Our extensive experience includes helping financial institutions comply with global privacy and data security requirements, providing advice that is crucial for navigating the current "perfect privacy storm" environment of more data, more regulation and more enforcement at a global level.

FINANCIAL REGULATION AND ENFORCEMENT

We provide a full range of regulatory advice and enforcement counseling services. This integrated approach helps our clients to navigate the challenges presented by regulatory and reporting requirements while simultaneously considering how to assess and minimize potential enforcement exposure. Enforcement investigations and regulatory examinations are similarly addressed, not only with considerable enforcement experience, but also by fully leveraging the enormous value added by regulatory expertise.

TECHNOLOGY TRANSACTIONS

Baker McKenzie has extensive experience advising clients on complex, transformational technology transactions, including complex information technology, and application development and maintenance transactions, highly bespoke business process outsourcing transactions. Having closed tens of billions of dollars in contracts to source critical technologies, services and business functions, our lawyers possess a deep and sophisticated understanding of the unique features of technology agreements.

KAREN MAN
Partner, Hong Kong
karen.man
@bakermckenzie.com

PAOLO SBUTTONI
Partner, Hong Kong
paolo.sbuttoni
@bakermckenzie.com