Attachment

Abuse and Fraud Prevention in Private Banking and Wealth Management
Management Control and Oversight[1]

1. Board and senior management oversight

- Policies and procedures should be properly approved by the board / management to control business operation, with clear accountability established for the risk management and control functions.

- Regular meetings should be held to oversee the operation / business as well as compliance with corporate policies and procedures.

- Complete, accurate and timely MIS reports should be provided to the management for review of business activities, customer services, compliance and exceptions.

2. Policies and procedures

- Policies and procedures governing the PB and wealth management operations should cover, but not limited to, the following areas:

  - background and integrity checks on RMs
  - account and transaction monitoring
  - responsibilities of RMs
  - staff code of conduct
  - compliance
  - discretionary investment management (if this is provided)
  - customer transaction processing and order execution
  - hold mail service
  - inactive and dormant account handling
  - complaints handling
  - fraud detection and reporting.

- These policies and procedures should be reviewed and updated on a regular basis. There should also be established processes and procedures for ensuring staff's awareness of and compliance with these policies and procedures.

[1] This attachment puts forth some good practices in general on management control and oversight to minimise chances of staff abuses and frauds in PB operations. Many of them are also applicable to the higher end of retail wealth management. They are not however meant to be exhaustive. It remains the full responsibility of each AI to develop its own policies and procedures to prevent abuses and frauds suited to its needs and scale of operation.

3. Risk measurement, monitoring and management reporting system

- There should be procedures in place for reporting of operational losses and irregularities to the appropriate officers. Complete, accurate and timely MIS reports (e.g. performance by individual RMs, exceptions on operational losses and transaction irregularities, customer complaints, inactive and dormant accounts) should be prepared for review by the responsible officers or line managers.

4. Internal controls

Internal control environment

- Job responsibilities should be well-defined, with duties properly segregated among the front and back office staff, in particular:
  - there should be dual control on the approval of new customer relationships
  - new account documentation processing and account activation should be performed by departments independent from marketing
  - RMs should not single-handedly be responsible for the execution of customer instructions without involvement of other control units for checks and controls
  - customer complaints, customer statements, hold mail services, and inactive and dormant accounts should not be handled by RMs only.

Conduct of staff and compensation scheme

- There should be rules governing staff dealing activities and these activities should be subject to management approval / regular monitoring. Staff relatives' in-house accounts should also be subject to regular monitoring.

- Compensation schemes of staff should not be solely driven by financial performance without taking into account satisfactory audit / compliance review results and complaint investigation results.

- Block-leave policy should be imposed on staff and properly enforced.

Account monitoring

- Where feasible, consideration should be given to periodic rotation of RMs / introducing the immediate supervisor of the RM to the customer.

- Audit trails of communication with clients (e.g. call reports) should be maintained.

- Formal annual review of customer relationships should be conducted on a timely basis to ensure that customer information remains up-to-date.

Hold mail

- If hold mail service is maintained, there should be control measures in place to mitigate the risks, e.g. tighten the control on such applications, separate custody of the customer's mail from the RM, reconfirming with customers who have requested for this service.

- Procedures should be established to verify customer authorization for releasing hold mail. If RMs were allowed to release mail on hold to customers directly, there should be control measures, e.g. customers' signatures should be obtained to acknowledge receipt of the mail and the signatures should be verified by an independent unit.

Inactive and dormant accounts

- There should be a clear policy to classify an account as inactive / dormant. These accounts should be subject to monitoring by units independent of the RMs.

- Sufficient control procedures should be formulated for reactivating these accounts.

Customer account statements

- There should be proper segregation of duties in (i) generating and delivering customer statements, (ii) handling customer request for change of correspondence address and (iii) collecting and following up with returned mail / advice / statements.

Voice logging

- All the telephone lines of RMs/assistants should be tape-recorded. Procedures should be established to control the tape-recording system and the safe-keeping of tapes.

- Procedures should be in place for periodic tape listening on sufficient samples.

Whistle blowing

- A hotline or compatible reporting channels should be set up for staff to report irregular activities encountered at work to an independent unit such as Compliance.

5. Compliance

- Regular review should be performed on compliance with the established operational control policies and procedures. Vulnerable customers, e.g. users of hold mail service, residing outside Hong Kong, old-aged, should be subject to more frequent checking of account activities to ensure no irregularities.

6. Internal audit

- Regular internal audit should be conducted, with the implementation of the audit recommendations properly followed up by Internal Audit.

7. Reporting of suspicious cases

- Senior management of AIs must be made aware of any suspicious cases involving serious implications and/or possible criminal elements in a timely manner. To this end, AIs should have policies and procedures in place on when and how to escalate suspicious cases (which may arise from customer complaints, MIS reports, another staff's report, etc) to the senior management for attention. To ensure timeliness of the reporting, AIs should establish a designated unit on fraud detection and prevention which can report directly to the senior management.

- In addition, whenever there is a suspected case involving possible criminal elements, AIs are expected to report the incident to both the Police and the HKMA in a timely manner.

July 2009
Hong Kong Monetary Authority