防貪諮詢服務
Corruption Prevention Advisory Service

Banking Industry Integrity Focus #2
Bank Account Opening

March 2026

Introduction

A customer, either individual or corporate, opens an account with a bank for accessing any banking products, services or other financial facilities. Leveraging technological advancements, many banks have adopted electronic customer onboarding alongside traditional bank account opening at branches to enhance the service efficiency and streamline the bank account opening procedures. To undertake customer due diligence (CDD) and to understand the customer's background and purpose of account opening, the bank account opening process in general includes the following critical steps: (i) verification of customer identity; (ii) document check; (iii) vetting of eligibility; and (iv) approval of application. Considering that bank account opening procedures can be corruption-prone and vulnerable to illegal acts or other malpractices, and in view of strong demand for bank account opening from non-local customers and practical challenges in verifying the authenticity of application documents, this Integrity Focus aims to highlight the potential corruption risks associated with bank account opening procedures and recommend corresponding corruption preventive measures, among others.

Part A – Integrity Insights: Case Studies and Corruption Risks

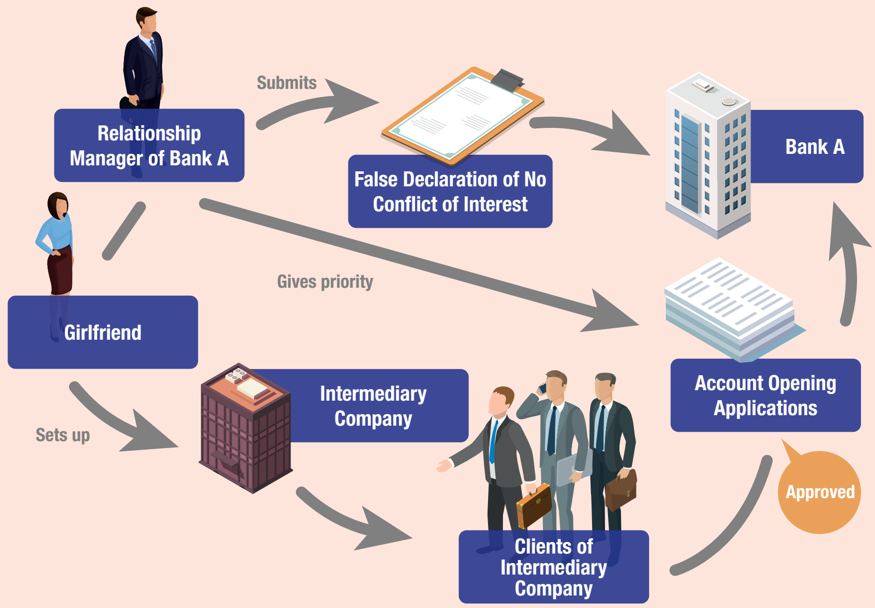
[Disclaimer: The following cases are based on certain corruption incidents and have been adapted to enhance clarity and ease of understanding.]

A.1 - Case Studies

Case Study 1

Acceptance of Advantages for Facilitating Bank Account Opening and Failure to Declare Conflict of Interest

1 A Relationship Manager (RM) posted to a branch of Bank A is responsible for opening bank accounts for customers. Knowing the strong demand from non-local customers to open bank accounts in Hong Kong, the RM and his girlfriend have established an intermediary company and actively promoted on social media platforms about its services in assisting non-locals to open bank accounts with a service fee.



2 While Bank A requires staff to serve customers in walk-in order or according to their advanced booking appointments, the RM gives priority to clients of the intermediary when handling their account opening applications at designated branch and guides them to complete the know-your-customer (KYC) process. For clients of the intermediary which are handled by his colleagues/supervisees, the RM induces/requests them to perform less stringent checks and provides coaching for clients via instant messaging application to fulfil the KYC requirements. With the RM's assistance, those clients' applications are approved by Bank A.

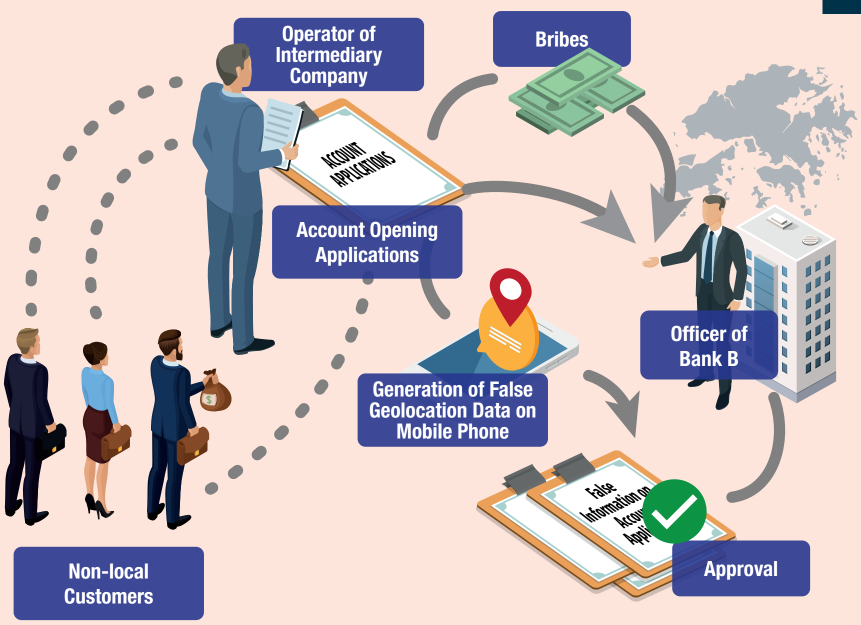
3 Bank A requires its staff to submit a declaration form annually of any actual or potential conflict of interest. However, the RM has never declared his financial interest with the intermediary and his relationship with his girlfriend on the declaration form submitted to Bank A.

Case Analysis

The RM is an agent of Bank A. He, together with his girlfriend, solicit and accept advantages (i.e. service fee) from non-local customers to facilitate bank account opening and assist in completing the KYC process, in relation to the bank's business and without the approval of his principal (i.e. Bank A), may respectively commit Section 9(1) of the Prevention of Bribery Ordinance (Cap. 201) (POBO). The RM, who conceals the conflict of interest dishonestly, with an intent to deceive his principal (i.e. Bank A), uses any receipt, account or other documents (e.g. declaration form of conflict of interest) which contain any statement which is misleading, false or defective in any material particular in respect of which the principal is interested, may contravene Section 9(3) of POBO or conspiracy to defraud of the common law.

Case Study 2

Conspiracy with Intermediaries to Submit False Information on Bank Account Opening Applications



1 Bank B requires non-local customers to attend a branch in Hong Kong in person to open an account. Upon arrival, a handling staff witnesses the attendance of the customer and requests the customer to generate a geolocation-based QR code via the bank's mobile application to confirm his presence in Hong Kong.

2 An operator of an intermediary company assists non-local customers in opening bank accounts in Hong Kong. Since some customers find it inconvenient to travel to Hong Kong in person, the operator offers several thousand dollars in cash to the bank officer at a branch of Bank B to facilitate the verification process. Knowing that Bank B solely relies on the handling staff to verify the customer's attendance, the operator visits the branch and uses his own mobile phone to generate a QR code via the bank's mobile application. The colluded bank officer then scans the QR code, purportedly that he has seen and checked the customer's identity at the branch. Subsequently, the operator inputs the customer information into the mobile application, resulting in the account opening application being approved.

Case Analysis

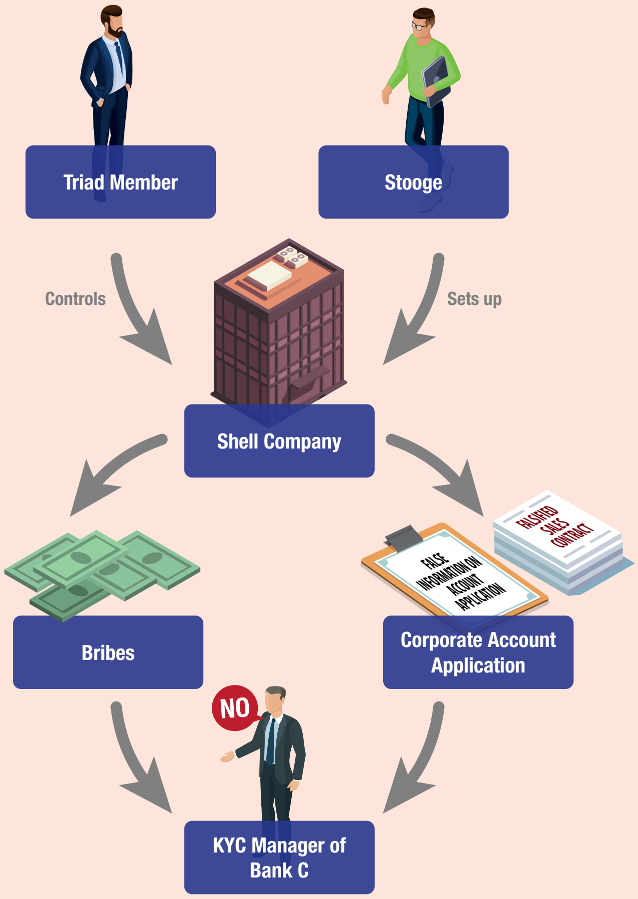
The bank officer is an agent of Bank B. The operator of the intermediary offers an advantage (i.e. cash) to the bank officer as a reward for deliberately concealing or conniving at the operator's provision of false information (i.e. the customer has arrived in Hong Kong for opening account) in the application process in relation to the bank's business. The bank officer may contravene Section 9(1) of POBO, if he accepts the advantage without the approval of his principal (i.e. Bank B). The operator of the intermediary who offers the advantage may contravene Section 9(2) of POBO. The duo may also commit conspiracy to defraud of the common law by submitting false information to Bank B.

Case Study 3

Offer of Advantages for Conniving at Money Laundering Activities

1 Bank C implements robust procedures for opening corporate accounts, including verification of company documents, background checks on authorised signatories and risk assessment of business activities.

2 A triad member recruits an individual to establish a shell company in Hong Kong and acts as its sole director. The duo submits an application to Bank C for opening a corporate account with the intent to launder crime proceeds derived from a fraud scam. To demonstrate that the company has a genuine business purpose, they present a falsified sales contract signed with an overseas buyer. During vetting, a Manager of the KYC Team of Bank C finds that the identity of the overseas buyer cannot be verified and suspects that the document may be falsified. When being enquired in a meeting, the triad member offers cash of $30,000 to the Manager, requesting him to turn a blind eye on the suspected falsified document.



3 The Manager refuses the offer and reports the incident immediately to his line supervisor who escalates to the Compliance Team. Upon receipt of the report, Bank C promptly refers the case to the ICAC with the duo arrested.

Case Analysis

The Manager is an agent of Bank C. The triad member, who offers an advantage (i.e. cash) to the Manager for conniving at his submission of falsified document (i.e. the sales contract) to open a corporate account for money laundering purpose, in relation to Bank C's business and which is prohibited by Bank C, may contravene Section 9(2) of POBO. The duo may also commit relevant deception offence(s) by conspiring together to submit false documents to Bank C. The Manager immediately reports the incident to Bank C, which then promptly refers the case to the ICAC for enforcement actions, thus upholding the bank's reputation.

A.2 - Major Corruption Risks and Red Flags

A.2.1 Corruption Risks

- Colluded bank staff solicit/accept advantages from customers/intermediaries for facilitating bank account opening (e.g. expediting the process, skipping certain checks, waiving fee).
- Compromised bank staff solicit/accept advantages from customers/intermediaries for conniving at the latter’s submitting false information / supporting documents (e.g. falsified documents such as business registration records, income proof, employment records, and false representation that the customer has arrived in Hong Kong for bank account opening) to the bank for opening bank accounts or assisting the latter in opening bank accounts for money laundering or other illicit activities.
- Dishonest bank staff deliberately fail to declare their conflict of interest with customers/intermediaries (e.g. close relatives, shareholders in the intermediary company) with a view to favouring the latter in bank account opening or obtaining personal gain.

A.2.2 Red Flags

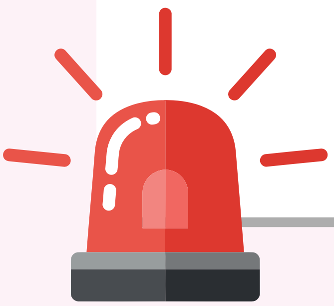
The following red flags are warning signs or suspicious indicators during bank account opening that signal the above corrupt practices and malpractices, and are crucial for banks to early detect/identify and prevent illicit activities.

Staff Related

- Exceptional increase in number of bank account opening cases handled by the same bank staff
- Abnormally high proportion of non-local customers handled by the same bank staff or branch when compared with others or mode of the bank’s operation and without justified reasons
- Exceptionally high exit rate of clients handled by the same bank staff
- Queue jumping in processing account opening applications
- Frequent overrides of automated risk flags

Customer / Account Activity Related

- “New customers” insist on requesting a specific staff member to handle their applications
- Suspicious supporting documents (e.g. edited or unclear records, records with discrepancies)
- Multiple unrelated businesses or individuals attempting to open accounts with the same IP address, device fingerprint or behavioural pattern (e.g. using tainted devices and known doubtful addresses), particularly where there is no apparent legitimate relationship (e.g. shared company secretarial service or group affiliation)
- Customers appear to be guided by unknown third part(ies) during KYC procedures (e.g. repeatedly glance at their phone for answers, give scripted/model responses, or cannot answer simple follow-up questions independently)
- Frequent, large or unexplained deposits or withdrawals shortly after bank account opening without adequate and appropriate justification, or other transactions which are incommensurate with the customer risk profile, or abnormal transactions



Part B
Corruption Prevention Safeguards among the Key Procedures in Handling Bank Account Opening

[Disclaimer: This Integrity Focus includes corruption prevention measures that are advisable to be adopted by banks. Individual banks may adopt these measures to suit their operational needs while adhering to the principles. The ICAC will provide tailor-made advice on request. Banks are strongly advised to make reference to the guidelines issued by the Hong Kong Monetary Authority (e.g. customer onboarding, due diligence, anti-money laundering / counter-financing of terrorism controls) in conducting the relevant banking operations.]

B.1 - Appointment Booking and Case Assignment

- Implement a transparent online booking system / appointment platform and an automated in-branch queuing system (such as real-time reservation status), which operates on a first-come, first-served basis to ensure fairness.
- Remind customers of the eligibility and documentation requirements prior to their visits to branches for bank account opening (e.g. issue SMS or inform verbally via phone after they have made such bookings).
- Monitor the demand for bank account openings and allocate sufficient resources (e.g. deploying additional staff, extending branch opening hours) to effectively manage periods of high demand.
- Allocate account opening applications on a rotational basis to bank staff for processing, with justifications properly documented for any cases out of turn, and dissuade customers from selecting or requesting specific handling staff.
- Require customers to declare on the application form and documents that all information and supporting documents submitted are true and accurate, and disclose whether they are referred by any intermediary or bank staff as well as any fee paid as appropriate, and draw their attention to a warning on possible consequences (e.g. criminal liabilities) of providing false information and submitting bogus documents.

B.2 - Verification and Checking

B.2.1 Customer Identity Verification

- Ensure proper checks and balances in customer identity verification (e.g. arrange two staff members to witness and check, and sign to confirm) and/or adopt electronic means (e.g. biometrics, liveness detection) to verify and authenticate customers' identity.

B.2.2 Customer Due Diligence and Know-Your-Customer

- Ensure CDD/KYC processes are adequate and not excessive.
- Require handling staff to verify the truthfulness of supporting documents submitted by customers by inspecting originals or certified copies, or by checking relevant records directly on the issuing platforms (e.g. bank statements in e-banking application and tax returns on the government e-tax platform).
- Utilise appropriate technologies (e.g. adopt AI-powered authenticity checks leveraging deep learning models and forgery detection algorithms) to detect the use of fraudulent documents.
- Conduct background checks and name screening on customers to detect suspicious indicators, red flags or association with suspicious parties for further enquiry (e.g. cross-check with internal database on previous dealings with customers).
- Verify the information against independent databases (e.g. records of the Companies Registry) and conduct physical inspection (e.g. for corporate customers) if necessary.

B.3 - Vetting and Approval of Bank Account Opening Applications

B.3.1 Vetting and Review of Applications

- Incorporate checklists into the bank account opening system to enable staff to systematically evaluate different types of customer accounts, and properly document the vetting results.
- Implement computer-aided programmes featuring configurable parameters and rule-based algorithms to automate risk assessment and vetting process and incorporate / build in red flags (***Cross-reference: A.2.2***) to facilitate compliance checks and detection of irregularities, and adopt security measures (e.g. maintain and review audit trails regularly) to prevent manipulation of the system rules and controls as far as practicable.

- Arrange an independent team (e.g. Compliance Department, AML Team) to conduct further review of applications on risk-basis, and mark and flag customers with issues identified during vetting process (e.g. customers with suspicious source of fund) in the bank's customer database for triggering additional scrutiny or escalated reviews in future interactions.

B.3.2 Approval of Applications

- Mandate maker-checker mechanism (e.g. require independent review of results and approval by another staff member, branch supervisor or independent team), and document justifications for approved/rejected cases as well as special cases (e.g. cases rejected on the electronic platform but are subsequently approved).

B.4 - Account Opening System Access Control

- Strengthen access controls (e.g. require two-factor authentication with password and access card, grant access rights strictly on a need-to-know basis, prohibit the use of shared accounts or sharing login credentials with colleagues, review access logs regularly) for branch-based account opening system and internal account processing system, and implement security safeguards (e.g. encrypt sensitive customer data, prohibit photo-taking/downloading/printing of confidential information) to protect customer information from tampering or leakage.

B.5 - Management Oversight and Supervision

- Require line supervisors to conduct checks on completed bank account opening cases and stay alert to staff with irregular behaviour (***Cross-reference: A.2.2***).
- Implement advanced data analytics tools (e.g. rule-based algorithms and machine learning models) to detect anomalies in bank account opening, and generate real-time alerts to Compliance Department for carrying out prompt investigation of suspicious activities.
- Conduct independent sample checks/reviews (e.g. by Compliance Department, AML Team) on account opening applications, especially high-risk cases, to verify compliance with relevant banking policies, internal procedural control requirements, and conduct surprise checks (e.g. mystery shopper) if necessary.

[1] *Banks are advised to make reference to the circulars/guidelines issued by the Hong Kong Monetary Authority in conducting electronic/remote boarding.*

Part C
Corporate Governance and Integrity Building

C.1 - Bank Policies

C.1.1 Policies and Guidelines

- Lay down clear and comprehensive policies and procedures (e.g. customer identity verification, collection of information and documents for due diligence, vetting, review and approval of applications, maintenance of proper documentation) for handling different types of customers / bank accounts (e.g. personal, corporate) and onboarding methods (e.g. face-to-face, online), and update the policies and procedures to address emerging risks and regulatory requirements regularly.
- Publicise bank account opening methods (e.g. in-person, online), eligibility requirements and necessary supporting documents through appropriate channels (e.g. bank's website, social media platforms).
- Require all relevant staff handling an account opening application to record their names and sign on the application form and/or account opening system and document whether clients are referred by any third parties (e.g. intermediary).
- Prohibit bank staff from communicating with clients through unofficial/private channels (e.g. personal mobile phones or social media platforms).
- Set reasonable performance targets for branches / bank staff based on a diverse range of metrics to avoid relying solely on the volume of new customers onboarded or new accounts opened, and reward staff for non-financial performance (e.g. diligence, honesty, ethics) to motivate integrity behaviour.
- Implement periodic duty/staff rotation (e.g. across branches and internal units), and adopt the block leave policy under which all relevant staff involved in the bank account opening process are required to take consecutive leave for a specified minimum number of days (e.g. one to two weeks), during which they must completely disconnect from all work and records with system access suspended and work responsibilities temporarily reassigned to other staff members, to facilitate the identification of irregularities or misconduct.
- Strengthen employee exit protocols by reminding departing staff of non-solicitation and confidentiality requirements to prevent misuse of client data and insider knowledge, and regularly remind serving staff of potential conflict of interest and consequences of colluding with former colleagues operating as intermediaries.

C.1.2 Management of Intermediaries

- Educate customers to dispel misunderstanding and misrepresentation made by third parties claiming to be intermediaries that customers have to engage intermediaries in order to open bank accounts successfully, remind them of the risks associated with engaging intermediaries, and encourage them to approach the bank directly for bank account opening without such engagement.
- Conduct continuous surveillance of online and social media platforms covering the promotional activities undertaken by intermediaries (which are not engaged by banks) to detect any misleading messages (e.g. guarantee on exceptional short time for approving account opening applications) and gather feedback from applicants to detect any irregular activities of intermediaries.

C.2 - Integrity Capacity and Culture Building

- Specify in the bank's Integrity Policy and Code of Conduct essential probity requirements and standards (e.g. prohibition of bribery and corrupt practices when handling bank account opening applications), and specify the consequences for breaches (e.g. termination of employment).
- Provide regular training to bank staff to ensure compliance with the established bank account opening procedures and internal controls (e.g. conduct checks to detect fraudulent documents) while reminding them of relevant anti-corruption requirements and knowledge (e.g. POBO provisions regarding the acceptance of advantages, declaration and management of conflict of interest, corruption risks and preventive safeguards related to bank account opening and management of the relationship with intermediaries).
- Provide guidance (e.g. issue reminders) to bank staff on how to handle bribery attempts by external parties during bank account opening or delivery of bank services. ***(Cross-reference: C.4)***

C.3 - Integrity Risk Management

- Regularly review the integrity risks associated with bank account opening procedures (e.g. through regular review of ICAC press releases of corruption cases) and update relevant control measures to address any new vulnerabilities and gaps identified.

C.4 - Corruption Detection and Reporting Mechanism

- Establish a whistleblowing policy/mechanism, which are approved and reviewed periodically by the senior management or board of directors, to enable staff members, clients or relevant parties to report irregularities, misconduct and corruption in the bank's business activities (including bank account opening process) through designated channels in confidence and without fear of retaliation.
- Arrange staff with necessary authority, competence and expertise to handle whistleblowing reports promptly and in strict confidence and prevent acts (e.g. tipping off the subject person) which may jeopardise subsequent criminal investigations by the law enforcement agencies (LEAs) (e.g. ICAC).
- For any suspected bribery attempt or other illegal activities (e.g. fraudulent application/supporting documents, money laundering), report to LEAs (e.g. ICAC) promptly for investigation / follow-up actions as appropriate.

Additional Tips
Handling Bribery Attempts Targeting Frontline Staff

- Clarify the purpose of suspected corrupt payment with customer/agent/intermediary and try to obtain their contact and personal information.
- Arrange the subject person to stay at the branch under safe circumstance.
- Report the incident to line/branch manager without delay.
- Escalate to the Compliance Department for assessment and promptly refer suspected cases to the ICAC.

C.5 - Independent Audits:

- Conduct regular internal audits or arrange external service providers to conduct independent compliance reviews to ensure compliance with established policies and identify potential vulnerabilities in the bank account opening process.

Enforcement Alarm

Early and prompt reporting of suspected corruption to the ICAC not only facilitates timely investigation and prevention efforts but also reinforces the bank's commitment to integrity management and accountability. Conversely, **delays in making a report** can **severely hinder investigation and apprehension of offenders.** To jointly combat corruption through public-private partnership, the ICAC's **Banking Industry Integrity Charter** requires participating banks to promptly report any allegations or suspicions of bribery, corruption, fraud, deception, or other illegal activities to the ICAC or appropriate LEAs. If your bank detects any suspected corruption or related malpractices in banking operations, please report immediately to the ICAC (Reporting means: https://www.icac.org.hk/en/rc/channel/index.html) without delay.

Corruption Prevention Advisory Service

The above are by no means exhaustive. For further controls on the overall corporate governance, banks may refer to the publication **"Corruption Prevention Guide for Banks"** developed by the **Corruption Prevention Advisory Service (CPAS)** of the Corruption Prevention Department of ICAC.

ENG

繁

簡

ICAC

CPAS 防貪諮詢服務 Corruption Prevention Advisory Service

CPAS provides free, confidential and professional corruption prevention advice and services (e.g. review of Code of Conduct, provision of anti-corruption training) to private companies and organisations, including banks.

Please subscribe to our **e-news** and visit our **webpage** for the latest training resources, news and activities.

Hotline	: 2526 6363 (Mon-Fri: 9am-6pm) (except public holidays)
Email	: cpas@cpd.icac.org.hk
E-form	: https://eform.cefs.gov.hk/form/ica004/en/
Website	: https://cpas.icac.hk/EN/

J8112/25