Bank Fraud in Asia

by Jee Meng Chen

A sampling of frauds experienced in Asia shows that many "new" frauds are actually old schemes with a new twist. Thus, good old-fashioned due diligence, combined with new technology-based solutions, is called for. Three caveats discussed here are management left unchecked, outdated audit techniques, and packaged deals.

Frauds have been referred to as "unmanaged risks." The term "unmanaged" connotes the practical difficulties associated with managing fraud risk effectively and dynamically. In recent years, while the number of publicized frauds—unauthorized usage of credit and ATM cards, checking account fraud, Nigerian scams, etc.—increased, these cases merely constituted the tip of the iceberg. Estimates are that just 20% of frauds are exposed and made public. The remaining frauds are either undetected or discovered but not made public because of reputation risk.

Past causes of Asian bank crises include lack of depositor confidence due to perceived deterioration in loan quality, unsound lending practices and lax credit controls, uncontrolled diversification into new business segments, overtrading, and liability mismanagement. The framework and technology for bank risk management have improved over time, mitigating these risks.

The risk of fraud—another crisis that can bring down a bank—remains more difficult to predict and manage. The inherent vulnerabilities of the banking and finance system provide a conduit for fraudulent activities. Coupled with an accelerated pace of financial development and an emphasis on realizing short-term returns, bank frauds are likely to increase in Asia, as they may in the rest of the world.

The greater concern, however, is the growing sophistication and complexity of frauds. Banks should contemplate two interrelated issues.

1. Is the risk architecture capable of protecting the institution against fraud attacks? That is, are there preventive controls designed to identify potential fraudulent activities either prior to or at the time of executing a transaction or contract? These controls are the foundation of the bank's overall business processes.
2. In 2003, Asia witnessed a spectrum of frauds. What happened and what are Asia's banks doing to combat frauds? And what should bank and risk practitioners look for in managing fraud risk?

 Jee Meng Chen is a Singapore-based auditor who specializes in examination of trade financing operations and structured trade finance credit. He is a freelance writer on general banking topics and lectures on international export management at a local polytechnic institute. The views expressed herein are the author's own, unless explicitly specified or apparent from the context. His organization assumes no responsibility for the accuracy of the information.

Table 1

Factors	Explanation
Circumstances	The fraud perpetrator may be a willing party either acting individually or colluding with third parties defrauding the bank for personal gains. The fraudster could, however, be subject to duress or financial distress and hence be perpetrating the fraud unwillingly.
Human Psychology	While greed is the primary driving factor, fraud perpetuators may deliberately circumvent controls to demonstrate their "intellectual superiority" and may not necessarily be after monetary gains.
Opportunities	Fraud thrives when conditions are right. A "fraud-friendly environment" is characterized by lax corporate culture on the enforcement of internal controls; deficient and/or absence of requisite risk controls, staff apathy, overconfidence, etc.

A Review of Fraud Cases

The first step in managing fraud risk is to understand why it occurs. Fraud can be expressed as a function of *circumstances* x *human behavior* x *opportunities* (see Table 1).

Bankers may ask, "What's so special about Asian fraud cases?" Old ways of stealing are being accomplished using new skills. According to well-known fraud expert Courtenay Thompson, being educated on past frauds is a stepping stone to combating current ones, as many "new" frauds are simply old schemes that have returned, sometimes with a twist.

Information theft. While information theft historically has been deemed "low level" fraud, it is generally less complex and therefore easier to perpetuate. Consider this: Pan Asia Bank (PAB) was under investigation for information leaks. Credit histories of nearly 1,000 people were reportedly leaked through PAB's consumer banking service center. Six staff members suspected of involvement in the case had been called in for investigation. Criminals used the names of two people to apply for loans totaling NT450,000 from the Union Bank of Taiwan (Union Bank) and Chinese Bank. Union Bank reported that one of its depositors was a victim of identity theft, in which the customer's name was allegedly used to borrow NT190,000.[1] (*NT* stands for New Taiwanese Dollar, commonly abbreviated as NT.)

- Shipping-related frauds.
- Fraudulent trade deals. Southeast Asia's log industry was reportedly hit by a wave of fraudulent documents. Banks asked the International Maritime Bureau (IMB) to verify the authenticity of documents presented under various letters of credit (LCs) associated with log consignments in Southeast Asia. In most cases, the documents were fraudulent.[2]
- Financing fictitious LCs. Bank Negara Indonesia (BNI) faced huge losses in connection with the alleged issuance of fictitious LCs worth U.S. $200 million between December 2002 and July 2003. A BNI branch disbursed monies to finance commodity exports to Congo and Kenya, but the exports never materialized. Requests for export credit facilities were supported with LCs from little-known banks in Kenya, Switzerland, and the Cook Islands that were not on BNI's list of approved correspondent banks. A total of 105 transactions purportedly were processed without formal assessments.[3]

Maritime or shipping fraud—in particular, documentary credit fraud—is nothing new. Yet although knowledge of trade frauds had grown considerably over time, such cases never seemed to cease. Why? In the first case, greed had lured the defrauded buyers into the trap. Responding to unsolicited offers of "cheap" cargo, buyers readily conceded to making payments without checking the validity of documents and/or background of the sellers. As it turned out, the shipments were nonexistent. The second case probably involved insiders who facilitated circumvention of stipulated controls, without which it would be difficult to explain how 105 transactions could have been approved over time when they were

clearly in violation of the bank's guidelines.

Technical frauds. With the advent of technology-based banking, it likely will not be long before technical frauds involving high-value payments overtake documentary fraud. Technology has been said to be the "fraudster's best friend." A string of bank frauds in Hong Kong, ranging from "spoofed" Web sites to fake ATM cards, were reported by the Hong Kong Monetary Authority (HKMA).[4] The Hong Kong branches of Bank of China, international HSBC Holdings, and U.K.-based Schroders reported having encountered similar frauds in December 2003. And in Taiwan, a series of ATM card frauds cost Taiwanese banks over NT$30 million in mid-October 2003.

Anti-fraud Measures

A deliberate and proactive approach in fraud risk management is commonly found only in large, sophisticated Asian banks, where it's not unusual to see anti-fraud units. These units could be part of the credit department, a unit related to corporate security, a unit of information technology, or a cross-functional team of professionals with an explicit mandate to ensure the fraud controls have been established and are effective. Understandably, large financial institutions are invariably more susceptible to fraudulent activities, given the diversity of their banking operations. The more sophisticated banks now are using several fraud risk management techniques, many of which are familiar to Western institutions.

Internal controls. While there is not yet any rigorous and holistic methodology for addressing all aspects of fraud risks, the concept of internal control remains central to fraud risk management. An analysis of financial frauds revealed that the root cause generally involved a breakdown in the control environment. Thus, it was no surprise that the *Turnbull Report* recommended that companies should "maintain a sound system of internal control." Also, companies subject to the Sarbanes-Oxley Act must implement anti-fraud programs and controls. Of late, continuing education and self-assessment exercises have gained importance in inculcating control awareness, and financial institutions are reinforcing such control fundamentals as segregation of duties and periodic rotation.

Are there better solutions to fraud prevention and deterrence? Probably not, but that said, internal controls do not provide 100% insurance against frauds because staff who are sufficiently motivated will invariably find some ways to circumvent existing controls. Moreover, controls invariably fail when staff members responsible for those controls do not understand the risks they should be worried about. This is not surprising, as awareness of internal controls usually comes from audit criticisms and/or monetary losses, which occur too late in the end-to-

Table 2

	Functional Area *	Nature of Fraud Risks	Current Controls
1	**Treasury Operations** —Exotic instruments	—Valuation fraud	—Independent valuation source(s)
2	**Commercial Lending** —Commodity financing	—Unauthorized disposal of collateral —Collusion with third parties	—Approved warehouse —Periodic independent checks
3	**Trade Financing** —Invoice discounting	—Fraudulent invoices	—Approved suppliers —Related companies' sales strictly prohibited
4	**Investments**	—Churning —Forged client's instructions	—Periodic; independent review of clients' transactions —Safekeeping clients' authorized signatures and mandate

* Another classification method is to determine the type of fraud: 1) manipulation of accounts, 2) theft of information and assets, 3) computer fraud, etc.

end business process. Thus, anti-fraud measures must include educating employees, particularly those who work directly with customers, on the type of technical controls they should implement or maintain.

Fraud risk assessments. In addressing fraud-related concerns, some banks have attempted to develop a "fraud risk map" by estimating and identifying key risk areas. A simplified fraud risk map is shown in Table 2.

Fraud risk assessments not only examine current controls (column 3), but also focus on controls relating to the prevention and detection of fraud. Such assessments facilitate investigation on the robustness of controls, that is, whether they can be circumvented or overridden. Fraud assessments could be further enhanced by a focus on fraudulent schemes and/or scenarios. To keep track of risk-prone areas as well as emerging businesses, regular reassessments are required.

An alternative is to ensure that each business has three lines of defense—the front office, a secondary control (operations, finance, risk, or a combination thereof), and internal audit.

Bankers should know, however, that fraud assessment is not an unassailable technique because potential fraud risk-points are inexhaustible. Implicitly, an institution cannot control risks it never identified. Besides, fraud risks that are passed off as immaterial might go unnoticed.

Technology-based solutions. Technology is integral to fraud control. It enables banks to proactively analyze 100% of transactions, homing in on fraud indicators. Fraud-detection technology, for instance, is commonly applied in the credit card industry. Primarily rules-driven, the "intelligent system" analyzes buying patterns of credit card consumers and filters deviations from the established norm on a real-time basis. Apart from front-office applications, auditors are known to have employed computer-assisted audit tools to pore through voluminous data for indications of unusual activity that might suggest fraudulent activity.

None of these "solutions" is the complete solution, and it would be wrong to attempt to manage and control fraud using a one-size-fits-all approach. At the end of the day, anti-fraud measures are mere techniques only, given their limitations. Ultimately, the best defense against fraud remains *people*!

The Role of Regulators

Amid heightened concerns over money laundering, terrorist financing, and technology-based frauds, Asian regulators responded proactively by endorsing the "40 Recommendations" of the Financial Action Task Force (FATF) on money laundering and on revising/promulgating legislations against frauds. However, the primary responsibility to prevent and detect fraud belongs to bank management, not the supervisors. Generally, supervisors do not adopt a prescriptive approach—that is, prescribing anti-fraud controls—other than for exceptional circumstances. For example, in February 2004, the HKMA suggested that Internet banking services—particularly those used for high-risk transactions—should be subject to stronger customer authentication. In June 2004, however, the HKMA mandated that, as a minimum standard, banks offer the option of two-factor authentication for high-risk transactions to their retail Internet banking customers in view of increased Internet banking fraud. In Taiwan, the Ministry of Finance required individual current account depositors to take digital snapshots from 2005 on as a means of countering fraudulent use.

Watch Out For These

Despite the abundance of fraud-related literature, the following pointers deserve mention.

Management left unchecked. This pointer is self-explanatory. Frauds perpetuated by insiders, particularly in the case of an insular senior management, remain a tricky area. Such managerial decisions as control overrides are seldom subject to open scrutiny for fear of reprisals. The following case may illustrate the significance of insider fraud and collusion. In a certain bank, the head of Operations, who oversees account-opening documentation, personally handled those accounts referred by the head of Corporate Banking. Apart from the head of Operations, no other staff had access to the account-opening documents. During an annual audit, the head of Operations would respond to the auditors' queries, prohibiting unnecessary contact with the staff. Subsequently, as a result of restructuring, the heads of Corporate Banking and Operations were respectively

moved to other areas. Approximately eight months after the restructuring, there was an unannounced audit of the branch's credit operations, which uncovered unexplainable anomalies in those loan accounts handled by the head of Corporate Banking. In an attempt to better understand the customers' profiles, the auditors requested the associated account-opening documents. However, the requested documents were missing!

Challenges for risk and audit practitioners. A typical large commercial bank faces a seemingly limitless array of fraud risks. Bearing in mind that frauds manifest in myriad ways, developing a comprehensive database of potential fraudulent schemes and scenarios is a mammoth task. In addition, the design of effective anti-fraud preventive and detective controls requires fraud-risk practitioners to understand, in reasonable depth, the mechanics and technicalities of various fraudulent schemes, given that each scheme poses idiosyncratic risks and implications for the organization.

Audit practitioners face two challenges:

1. Supplementing standard audit procedures with forensic investigation techniques. This requires both anti-fraud training and out-of-the-box thinking.
2. Identifying and assessing fraud risks. Practically speaking, this would be difficult for auditors who may never have seen a live fraud case in the course of their careers. At best, auditors identify the environmental weaknesses that can make an institution vulnerable to fraud.

Packaged deals. While fraudulent activities masquerading as legitimate commercial-lending or trade-financing transactions will continue to ensnare the unsuspecting or unvigilant banker, the modus operandi of such frauds is becoming more complex. Commercial-lending and trade-financing activities are very much alive in Asia. In recent years, some innovative structures have surfaced in the market and of these, *packaged deals* warrant special mention.

Proper credit structuring is instrumental in lending risk management.[5] A carefully structured lending proposition addresses key risks and safeguards the bank's interests. But what would the risk implications be if the bank is not required to structure the credit? This happens in packaged deals (special-purpose deals—for example, tax optimizations or transactions structured as synthetic lending), where the transaction flow and financing mechanics are predetermined by the client or structurer. Normally, the bank's involvement is relegated to that of a financing intermediary. As an intermediary, the financing bank might not have access to detailed information, making a comprehensive risk assessment difficult. In contemplating packaged deals, banks should be doubly cautious when one or more of the following become evident:

1. The client or structurer is unwilling to furnish additional details.
2. There is an unduly complicated structure—for example, a "round robin" involving multiple parties in different jurisdictions.
3. The transaction does not make economic sense for the parties concerned.

Some banks argue that as long as the deals originate from known or established counterparties, it is unlikely that things would go astray. While these banks might fulfill requisite client due diligence, the same could not be said of transaction due diligence. Name-lending had been and still is a dangerous business.

Conclusion

Effective fraud risk management requires bankers and risk practitioners to adopt a "Parmalat: It can, has, and will happen in Asia"[6] mentality. After all, frauds are not peculiar to any jurisdictions or financial institutions and remain an ever-present challenge. ❐

Jee Meng Chen may be contacted by e-mail at guanming_insight@hotmail.com.

Notes

1 Chung, Amber, "Banks Told to Guard Customer Data," Taipei Times, December 12, 2003.

2 "SE Asian Log Industry Hit by Fraudulent Deals," International Chamber of Commerce, CCS News Archive, London, July 21, 2003.

3 Guerin, Bill, "Just Another Indonesian Bank Scandal," Asia Times Online, November 27, 2003.

4 The Hong Kong Monetary Authority periodically publishes fraudulent Web sites (nonexhaustive: www.khiba.com, www.fortizbank.com, www.dasxin.com) on an as-and-when basis.

5 The internal auditors should not be assigned to carry out this task, as it could result in a potential conflict of interests.

6 Asia Times Online, January 6, 2004.