

Fraud Management Minimum Standard Recommendations for Financial Institutions

[ข้อเสนอแนะมาตรฐานขั้นต่ำในการตรวจสอบและป้องกันการทุจริตในสถาบันการเงิน]

24 August 2010

Table of Contents

| | |
|--|-------------------------------------|
| Introduction | 4 |
| Overview | 4 |
| Background..... | Error! Bookmark not defined. |
| Vision and Strategy..... | 5 |
| Fraud and Integrity Risks..... | 5 |
| Reasons for Minimum Standards and Practice Guides..... | 7 |
| Scope and Limitation | 7 |
| Standard..... | 9 |
| Minimum Standard Recommendations | 9 |
| Recommendations: Broken Down by Products..... | 11 |
| 1. <i>Commercial Loan</i> | 11 |
| Minimum Standards Recommendation..... | 11 |
| Practice Recommendation..... | 17 |
| 2. <i>Hire Purchase</i> | 23 |
| Minimum Standards Recommendation..... | 23 |
| Practice Recommendation..... | 28 |
| 3. <i>Merchant</i> | 32 |
| Minimum Standards Recommendation..... | 32 |
| Practice Recommendation..... | 37 |
| 4. <i>Mortgage loan</i> | 42 |
| Minimum Standards Recommendation..... | 42 |
| Practice Recommendation..... | 47 |
| 5. <i>Personal Loan</i> | 52 |
| Minimum Standard Recommendation..... | 52 |
| Practice Recommendation..... | 57 |
| 6. <i>Sale Finance</i> | 62 |
| Minimum Standards Recommendation..... | 62 |
| Practice Recommendation..... | 67 |
| When and How to Use TBA Minimum Standard Recommendations | 72 |
| The Difference between Minimum Standard Recommendations and Practice Recommendations | 72 |
| Survey Observation | 73 |
| Most Variance Response..... | 73 |
| Most Compliance | 76 |
| Least Compliance | 81 |
| Importance but not Implemented..... | 87 |

| | |
|--|-----------|
| Analysis – Fraud Management Compliance Assessment | 90 |
| Participation and Resources..... | 90 |
| Methodology for Minimum Standard Recommendations | 91 |
| Participants’ Individual Opinion and Experiences..... | 91 |
| Appendices | 95 |
| Commercial Loan..... | 95 |
| Hire Purchase | 107 |
| Merchant | 116 |
| Mortgage Loan..... | 127 |
| Personal Loan..... | 137 |
| Sales Finance | 149 |

Introduction

Background

The Thai Bankers' Associations ("TBA") was founded in September 1958. TBA has played an active role in representing the banking community in Thailand in the continuous discussions with the Bank of Thailand, Ministry of Finance, Ministry of Commerce, and other government agencies in formulating and implementing key economic and financial policies.

The Fraud and Management Club ("FMC") was founded under The Thai Banker's Association for the purposes of supporting, publishing and developing knowledge and techniques used in preventing fraud and misconduct in the financial services industry. The objective is to further build awareness, gain public recognition of fraud risk and instill the significant benefits of fraud risk management and techniques used in prevention and detection of fraud committed by internal and external parties which subsequently promote and strengthen good corporate governance within the organisation. Moreover, the FMC acts as a centre point for the consolidation of information and further communicate to the private enterprise and public sectors and to create confidence among the investors, customers and other state own enterprises and government agencies.

Overview

In general practice, many of the financial institutions who offer credit instruments to their perspective customers primarily by considering and evaluating the borrowers' repayment capabilities. Given how serious the consequences of fraud can be, financial institutions have to be more cautious with the risk exposures derive from both the internal and external factors, for instance, sources of income, internal and external fraud risks of the borrowers in accordance with the changes of economic situation and environmental changes of business operations. As a result, fraud detection and investigation should be established in the organisation to avoid potential bad debts accounts and other associated risks which may create negative effects to the bank and financial services industry as a whole.

At the present, there is no official monetary value recorded of actual losses incurred through fraudulent activity in financial institutions in Thailand or abroad. Many well-known financial institutions in the USA unofficially stated that bad debts arisen through fraud might be in the range of 12 to 15% of total bad debts in their financial institutions' portfolio. In Thailand, the number of outstanding balance under gross non-performing loans (NPLs) section for both registered domestic banks and branches of international banks represented at around Baht 371 billion overall. In the event that the financial institutions are able to isolate the root cause of their non-performing loans, whether these resulted from inadequate underwriting policy, ineffective payment collection process or other hidden fraud, etc., the bank would be able to deal with those issues in a more concrete structures and efficient methods.

A current study of recent fraud cases observes that fraud perpetrator tend to commit fraud in more than one financial product and continuously defraud many financial institutions. One of the intriguing investigative results disclose that with over facilitation of the customer experience and ineffective management of internal control in one bank may resulted in the fraud incident and financial losses in another bank due to the integration of banks' process and technology that expose loopholes for opportunity to commit fraud, among the business of providing services, financial product management, the use of external intermediaries and serving customers.

According to a 2010 survey conducted by the FMC, majority of the member banks have identical financial products with similar banking operation, however, fraud intelligent operation and fraud prevention controls drastically vary from one bank to the others. Some banks have effective suite of risk management process and framework with the utilization of advanced risk management technology while others may be limited to tactical solutions and inadequate controls due to limitations of one's size, operating budget, readiness of human resource support and risk tolerance level of the

management teams.

Fraud incidents did not happen by accident but retroactively planned and committed by individuals with malicious intent when given the right opportunity, these individuals have discovered slight flows in the process or system and were waiting for the right chances to do so. Therefore, enterprise wide fraud risk management solution (Wing-to-Wing Fraud Management) should be established to include prevention, detection, investigations and remediation (Root Cause Identification/Fraud Loss Recovery) with the use of analytics (Fraud Indicator/Red Flags) and the application of advance technology solution with capability to elevate suspicious activities in the wide spectrum of banking operations that involved customers, service providers, intermediaries and banking operators with 24/7 continuous control monitoring solutions.

Vision and Strategy

The Fraud Management Club is aware of the alarming necessity and the given limitation of effective implementation of fraud risk management as described above. As a result, the FMC have studied leading fraud management standards by gathering opinions from the member banks, leading financial advisory services companies and solution providers of fraud detection and prevention technologies, and also includes government and law enforcement agencies, together with domestic and international subject matter specialists in this area, etc. These collective efforts are studies with information used to ultimately establish the minimum standard recommendations that are tailored to Thailand's business environment and regulatory bodies that will cover fraud issues in the financial institution committed by both internal and external parties. These minimum standard recommendations, which cover wide ranges of financial products and services of the banks, such as personal loans, mortgage loans, merchant loan, hire purchase, etc., will be used as a reference to mitigate fraudulent activity in the banking industry.

This document is a collaborative result which summarised studies conducted from the 2 seminars arranged by the FMC on the following topics: "Technology and Standards in Fraud Detection and Prevention" held at the Police Club on 21 January 2010, and "Fraud Minimum Standard Recommendations for all Financial Products" held on 9 – 10 July 2010 at Pullman Pattaya Aisawan Resort, Chonburi. There were more than 1,000 attendees at these seminars. Moreover, the FMC has appointed a Performance Improvement (PI) Consulting firm, PricewaterhouseCoopers FAS Limited as a host and facilitator of this seminar, along with the request to analyse and prepare a summary of fraud minimum standard recommendations.

The FMC reserves the right to publish this article exclusively to members of the club and authorised persons. These fraud minimum standards are only recommended standards and opinions from members of Fraud Management Club. Therefore, they might not be consistent with opinions and reports from financial institutions, committees, or government agencies for both domestic and international practices.

Fraud and Integrity Risks

Fraud, by definition, refers to any intentional behaviour committed to secure an unlawful or unfair benefit. In today's face pace business environment, numerous fuelling motivations such as incentives, pressures, and opportunities are major factors contributing to fraud committed by all levels of employee in the organisations, as well as the outside constituents. It is important for organisation in financial services industry to identify potential fraud risks, the associating impacts as well as articulate strategic approach to minimise these risks effectively and efficiently.

Fraud risks can be generally categorised into three types: fraudulent financial statements, misappropriation of assets, and corruption. In the first type of fraud risk, a financial statement is intentionally manipulated to conceal their fraud, for example, an unauthorised access to core banking system and accounting transaction to mark and manipulate suspicious transactions. This risk can result in improperly inflating revenues and under reporting expenditures, and concealing unauthorised receipts and expenditures. The second type of fraud risk can be perpetrated by employees, customers, and former employees or others outside the organisation. For instance, a fictitious customer account may be created solely to receive money transferred from other customer's dormant

accounts, or an employee may steal interest bearing funds from the bank's internal accounts. Finally, bribery and gratuities, conflicts of interest, and embezzlement are some of the examples of corruption committed by fraud perpetrators which resulted from conflict of interests and collusion of customers, suppliers and employees.

To date, many organisations have suffered from fraud induced losses such as financial loss, reputation impairment, and legal liability. Financial loss can be recognised as the direct tangible impacts on business bottom line and is expected to rise. As presented by Association of Certified Fraud Examiners ("ACFE") 2010 Report to the Nation on Occupational Fraud and Abuse, the typical organisation from 106 nations loses 5% of its annual revenue through fraudulent activity. In banking and financial services, thefts of cash by individual or group of individuals have caused multi-million dollar losses.

Another significant negative effect is on the bank's brand, image and reputation. An organisation's reputation and confidence level with customers, business partners and the capital markets can be dramatically damaged by stories of fraudulent activities. The negative public perception can hinder the ability to develop new relationships or maintain existing relationships with their customers and the target prospects. In some cases, improper access to the core banking system or loan originating system could be significant weaknesses which enable a fraudster to make unauthorised transactions. The outcome can lead to decreasing customer trust in the banking system.

Legal liability such as fines, sanctions and financial penalties, are many of the potential consequences from fraud incidents. Fraudulent activities can result in the organisation being fined for not complying with the legal regulations, both domestic and international which directly hinder the ability for the bank to fully execute their business strategies. In the banking industry, banks may be penalised for making large loans to individuals or businesses without appropriate evidence of underwritings.

It is no surprise for businesses to become victims to fraud committed in a wide range of industries. Banking and financial service sector is one of the industries that have experienced a great number of frauds. As presented in the "Report to the Nations on Occupational Fraud and Abuse" by the ACFE, more than 16% of fraud cases found during the year 2008-2009 in 106 countries around the world were committed in the banking/financial services industry - in other words, banking appears among the top victims when compared with all industries. Besides the ACFE conducted by the ACFE, the financial service sector, with 44% of reported frauds from some organisations in 54 nations, was ranked number three that encountered economic crimes in 2009, according to the "PricewaterhouseCoopers (PwC) 2009 The Global Economic Crime Survey". It is noted that most critical frauds in this sector were committed by external perpetrators.

By looking at fraud schemes in the banking industry, the ACFE study reveals that the top three common schemes involve corruption, cash on hand and billing, which accounted for approximately 34%, 22% and 13% respectively of all fraud cases that occurred in victim companies. In respects to corruption, it is defined as improper use of employee's influence in such a manner that it breaches his or her duty to secure the benefit for oneself or another. Cash on hand and billing represented two of the asset misappropriation schemes. Stealing or misuse of cash from the organisation is an example of cash on hand misappropriation, whereas billing involves the submission of invoices on behalf of the bank for fictitious goods or services, or invoices for individual purchases.

Furthermore, the ACFE study examined which of the general control weaknesses in organisations which allowed fraud to happen. The primary factor was a lack of internal controls, such as inappropriate segregation of duties, which accounted for almost 38% of the cases, while an override of existing internal controls by the perpetrator was the second most exploited deficiency unveiled in over 19% of the fraud cases. In contrast, without sufficient reporting mechanism at the time the fraud was stated as the least control deficiency that contributed to fraud. In Thailand, one of the largest frauds in the banking sector resulted from the absence of segregation of duties. Access to sensitive passwords and improper setting of access authorization to the banking system has been found as the key weaknesses and cause the embezzlement to the organisation.

Characteristics or individual behaviours, known as "red flags", probably indicate the likelihood of committing fraud. In order to carry out the task of fraud detection, these should be some form of

indicators like warning signals to banking colleagues and supervisors, as well as the organisation's fraud team. In fact, losses can be minimised when fraudulent activity is detected as early as possible. There are several factors impacting on behavioural red flags. Financial difficulty was the first warning sign that motivated a perpetrator to commit fraudulent activities, which was shown approximately 50% of all employee fraud cases. By observing different level of employees' organizational hierarchy, it reveals that the staff-level fraudsters were much more likely than manager-level and owners/executives to have the motivation for committing fraud. One of the main expected reasons is that staff-level employees normally have lower incomes than management and executive level employees.

Reasons for Minimum Standards and Practice Guides

Due to the elevated risks and critical impacts resulting from fraud, many financial institutions are starting to recognise fraud risks as one of the key operation risks and begin to explore remedy action to mitigate them. However, these are still a vast portion of these companies who continue to underestimate the losses derive from fraud and implement inadequate controls. To diligently mitigate or accept these inherit risks, every organisations in banking and financial services should consider fraud prevention measure and detection of establishing sound anti-fraud practices and controls that could withstand intentional misconduct like fraud. These approach and solution will precisely vary depending on different level of risk tolerance level, the complexity of business processes, and a variety of financial products and services offered. These minimum standard and practice guides provide insights to practical precedence of critical steps that should be in place and complied with overall intention to ultimately yield direct saving from avoiding accumulating fraud loss and improve an organisation's financial performance.

Scope and Limitation

The FMC within the TBA is looking to establish minimum standards recommendation and practice guide for 23 member banks in Thailand. In keeping with these efforts, TBA and PwC have jointly developed a set of questionnaires and survey and distributed them to the 23 member banks which also include other representatives from relevant government agencies. The goal is to independently assess their current practice performance and levels of competency in the unbiased manner, and to understand the future demanding profile of the opportunities for improvement in various areas.

PwC assists FMC with the initiative to set fraud minimum standard recommendations for Banking Operational Effectiveness. TBA's approach is to have structured and transparent methodologies that deliver results that can consolidate all feedbacks and inputs among the financial services communities and government agencies in Thailand in a constructive and consistent manner to help shape Thailand's banking practice.

A "Fraud Minimum Standard Recommendation and Practice Recommendation" is developed for six key financial products in the Thai market, namely commercial loan, hire purchase, merchant, mortgage loan, personal loan, and sales finance. In addition, we categorise the due-diligence activities into sub-categories, which will be performed prior to the bank providing these financial products to the respective customers:

- a) Know your customer (KYC) – This process is to obtain granular information from the customers with risk rating to ensure that given information is accurate. Bank has to confirm the existence and authenticity of the loan applicants.
- b) Know your intermediaries (KYI) – In some cases, banks may leverage the service rendered by the third party intermediaries in the task to identify prospective customers which also includes the process of screening the information of the loan applicants. The bank needs to ensure that these intermediaries are well position to perform their work effectively and also in a transparently manner.
- c) Asset verification – Under the secured loans, borrowers have to pledge their assets as

guarantees for certain loans. Therefore, asset verification is the process of providing bank with reasonable assurance that the bank has lien over those assets with ability to liquidate the stated assets with reasonable value.

- d) Revolving Fund - Redraw Ability – Bank should follow the recommended activities under this section to ensure that revolving procedures and ability to access level of allowance credits have been complied with ways to prevent any fraud risks.
- e) Know your staff (KYS) – Human resources are one of the key success factors of bank operation to prevent from from the within. Bank should strictly follow minimum standard recommendation under each product. This will help mitigating internal fraud risks.
- f) Third party payments / disbursements – The purpose behind originating loans are for borrowers to use the fund to pay for the purchased goods and services. Bank should employ proper protocol to ensure that the lending money is paid directly to third parties and not directly to the customer.
- g) Reporting – Under this section, certain reports should be issued to relevant persons. For example, fraud management case should be issued to and followed by fraud team. The result of fraud case, which is finalised, should be updated into the system and acknowledged by all relevant parties.
- h) Operational efficiency – This section primarily emphasises the operational activities to ensure that bank's business process and operational procedure and efficient and cover all aspects of possible fraud risks.
- i) Fraud technology – For some circumstances, manual preventive control and monitoring routine cannot efficiently prevent or detect fraud. Banks should implement advance technology solution to help them detect any potential fraud. This technology can identify red flag and alert the responsible persons when it comes across suspicious activities in the organisation.

Standard across financial institution

Minimum Standard Recommendations for financial institution

Regardless of financial products, every organisation should have an understanding of effective fraud management as well as implement antifraud programs and controls. It is recommended that the Committee of Sponsoring Organisations (COSO) framework should be applied because this framework is generally accepted to use in asserting and auditing the effectiveness of internal controls. The COSO framework consists of five major components with special emphasis on the control environment where tones are set at the top of an organisation that influences the control consciousness of people. All of the components of the COSO framework comprise of the following:

1. Control Environment

The control environment refers to intangible items such as integrity, ethical values and competence of the entity's people, and management's philosophy and operating style. It also covers more concrete expressions of these intangibles, such as the way management assigns authority and responsibility, and organises and develops its people. The establishment of strong antifraud programs and controls is an essential component of a healthy control environment. Therefore, banks should consider implementing the following controls:

Code of Conduct/Ethics

An effective code of conduct is a fundamental element of an effective control environment and antifraud program. As a best practice, a code of conduct should include all employees to ensure that any observed instances of misconduct or pressure to compromise ethics standards are reported. Furthermore, an organisation must undertake reasonable measures to be sure that employees understand the concepts embodied in the code of conduct.

Ethics Hotline/Whistleblower Program

The organisation should have an ethics hotline or whistleblower program to communicate concerns, anonymously if preferred, about potential violations of the code of conduct, including unethical behaviour and actual or suspected fraud, without fear of retribution. An effective ethics hotline/whistleblower program is both a fraud deterrent and an important means of discovering actual and suspected fraud. In addition, the operating effectiveness of the hotline or whistleblower program should be assessed regularly.

Hiring and Promotion

Establishing standards for hiring and promoting the most qualified individuals should include the performance of background investigations on individuals to certain positions of trust within an organisation. An entity's failure to perform substantive background investigations for individuals being considered for employment or for promotion would be a strong indicator of a significant deficiency in internal control.

Oversight by the Audit Committee and Board

The board is responsible for assessing the risk of financial fraud by management and ensuring controls are in place to prevent, deter and detect fraud by management. Much of the audit committee's oversight is embedded in the elements of an effective antifraud program. The organisation's board of directors and audit committee significantly influence the control environment and "tone at the top." Additionally, appropriateness of oversight of the board and audit committee should be evidenced through discussions with board and audit committee members or reported in the committee meeting minutes.

Investigation/Remediation

Banks should develop a standardized process for responding to allegations or suspicions of fraud. It should not wait until fraud is detected to develop an investigative process. At the very least, management should ensure that appropriate and timely follow-up occurs. This assessment should

include an examination of a sampling of incident investigations and remediation of alleged serious misconduct.

2. Fraud Risk Assessment

Banks should consider the potential for fraud as part of their enterprise-wide risk assessment process or risk management program. Fraud risk assessment considers vulnerability to management override and potential schemes to circumvent existing control activities, which may require additional compensating control activities. In addition, assessment of fraud risk should include the potential for fraudulent financial reporting, misappropriation of assets, and unauthorised or corruption as well as incentives and pressures on management to commit fraud.

To be effective, the organisation should perform fraud risk assessments on a comprehensive and recurring basis rather than in an informal or haphazard manner.

3. Control Activities

Control activities are those actions taken by management to identify, prevent and mitigate fraud, such as fraudulent financial reporting within the department or misuse of an organization's assets. Management should evaluate whether appropriate internal controls have been implemented in any areas where management has identified as posing a higher risk of fraudulent activity (i.e., non-standard manual reconciliation prior to the office closing), as well as controls over the entity's financial reporting process and the potential for management override.

It is recommended that antifraud control activities should occur throughout the organisation, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, segregation of duties, reviews of operating performance and security of assets.

4. Information and Communication

Effective communication is critical to ensuring the success of antifraud programs and policies. Banks should ensure that antifraud policies are stated clearly and spell out each employee's responsibilities in relation to the program. All personnel must receive a clear message that the company is serious about its commitment to preventing fraud. In addition, each employee must fully understand the expectation of all relevant aspects of the company's antifraud program as they relate to following and enforcing the company's antifraud policies.

With regard to fraud, that means being able to collect and share information regarding identified fraud risks, the existing strengths and weaknesses of the as-is antifraud control activities, any suspicions and allegations about fraudulent activities and remediation efforts. The organisation should consider using its information systems and technology as important tools in these efforts.

5. Monitoring

As is the case with all internal controls, a company's antifraud controls, programs and policies must be monitored to ensure its operational effectiveness, which means that they are subjected to ongoing and periodic performance assessments. The frequency of separate evaluations or audits necessary for management to have reasonable assurance about the effectiveness of its antifraud controls is a matter of management's judgment. Banks should consider using advanced continuous controls monitoring software from fraud to enhance the effectiveness of an entity's monitoring activities. In addition, numerous software programs are readily available to enable financial service institution to search for and detect suspicious or potential fraudulent activity as they occur in real-time.

Conclusion

It is clear that the elements discussed above must all work together to form an effective antifraud

program, and thus should be considered in the aggregate as an integrated system. The absence of multiple elements should raise a concern about the adequacy of the program or a COSO framework control component.

In addition, most entities should have formal documentation of their antifraud programs. The only exception is the case of the smaller, centralized organization in which the importance and emphasis on integrity and ethical behaviour are exhibited via visible and direct involvement of the CEO and top management in employee meetings, dealings with customers and vendors, and so forth. Such exceptions with regard to documentation are generally only appropriate for entities with 50 or fewer employees and with only one location.

Recommendations: Broken Down by Products

This section is a summary of each product, including minimum standards recommendation, practice recommendation, and guidance note, which should be complied with as the bank's normal operation.

1. Commercial Loan

In general, commercial loan is given to the corporate regardless of their size of business. This loan can be approved in the form of secured or unsecured loan. Borrowers will use the proceeds of this commercial loan to fund large capital expenditures and/or operate their normal business.

Banks should follow minimum standard recommendations listed below, even though fraud risk from commercial loan is relatively low.

Minimum Standards Recommendation

We categorise each recommendation according to the relevant activities operated by the bank as follows:

a) Know your customer (KYC)

In general, commercial loan is provided to the customers in large amounts of money since the customers will utilise the fund to operate their business or to further fund the investment. Therefore, the bank should have a reasonable knowledge of the customers, such as the company profile, major shareholders, board of directors, management team, type of business and other sources of fund, etc. The Bank should have specific database to screen whether or not the customer is restricted in the sanction or blacklist for both from the credit rating agencies and known-fraudster. In addition, the bank should conduct a site visit to the company's physical location and assess their ability to pay the outstanding balance, as well as the business as-usual operation of the borrower. This process is the first step to prevent any losses which might occur in the event where that the customers are not in the position to repay the outstanding balance or the particular company is set up with malicious intent solely to defraud the bank.

Furthermore, the roles and responsibilities of the sales and the underwriting teams should be explicitly segregated from each other. Underwriter should not have any chance to deal with the targeted customers in order to avoid any conflict of interest.

Please refer to the more detailed recommended minimum standards for mitigating fraud risks in the table below:

| Rank | Description |
|------|-------------|
|------|-------------|

| Rank | Description |
|------|--|
| 1 | Bank has in place, and properly follows, written Underwriting processes to check: The Customer Company, and the following: <ul style="list-style-type: none"> - Its beneficial owners - Its Management - Its Related Companies |
| 2 | Bank has a Policy detailing: <ul style="list-style-type: none"> - requirements of customer's business in terms of quality and source of revenues (i.e. 'Target Market Definition') - minimum credit parameters and detailed rejection parameters |
| 3 | Fraud Blacklisting Capability |
| 4 | Face to Face meeting with customer (prior to submission of Credit Application for approval) an initial and regular site visit to monitor customer business health / adherence to credit conditions, etc. |
| 5 | A process to check to ensure that each approved deal conforms to the approved Credit Review Point or Product Program. |
| 6 | Bank has a process to identify and in more detail check out 'High Risk' customers, deals, transactions, for example, unusual deal structures; timeline pressures; unusual repayment requests; asset refinancing; financing of specialist businesses in which we have nil or limited experience. |
| 7 | Clear segregation between Sales and Underwriting to avoid conflicts of interest otherwise inherent |
| 8 | Adopt properly legally-approved Contracts, that include protection of the Business in the event of fraud and that cannot be over-ridden / altered without proper review / approval |
| 9 | A consolidated view of each customer's total relationship with the Business, showing any rejections by Bank (Underwriter / Credit Officer) on any / all prior credit applications by that customer or by any of its beneficial owners / management / related companies (this is comparable to Consumer Banking 'De-dupe' controls) |

b) Know your intermediaries (KYI)

Sometimes banks may require third party services to act as their intermediary to assist in finding and primary screening of their prospective customers. However, bank must ensure that those intermediaries perform their jobs transparently since they are the primary filtering mechanism for particular loan applicants. Before appointing any party as the bank's intermediary, bank should check all possible information such as company background, financial position, credit rating, etc. Bank should also perform a site visit prior and after accreditation of particular intermediaries.

Moreover, bank should have a reliable database which includes all the information of intermediaries who have blemish track records or blacklisted from doing business with other financial institutions. The bank may appoint a dedicated staff team to continually monitor the performance of the appointed intermediaries. This will help them ensure that loans given out to the customers, proposed by particular intermediaries, are the operating loans.

| Rank | Description |
|------|--|
| 1 | Robust Intermediary accreditation process – See Bank's Compliance guidelines for specific internal processes. |
| 2 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all broker groups. Checks that if Intermediary terminated then terminated across all Bank businesses / Products |

| Rank | Description |
|------|---|
| 3 | Segment and Monitor <i>Intermediary performance</i> by Underwriter and / or Sales representatives in order to identify Red Flags / suspicious trends / transactions. |
| 4 | Monthly Reporting on Intermediaries using performance triggers as review point (i.e. Approval Rates, Write Offs (W/Os), Delinquencies, Business / Sales Volume, Red Flags, overdue deliverables / corrective action, etc. |
| 5 | Broker Fraud - Included in contract with broker is reimbursement for Internal Fraud. Or encourage broker to take out insurance for internal fraud. |
| 6 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. |
| 7 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level. |

c) Asset verification

Commercial loan product can be given to the customers in both secured and unsecured manners in accordance with the principal amount. However, most of this loan is a secured loan which is pledged by the company's assets, collaterals or other form of guarantees, etc. If bank's loan is pledged by certain assets, a clear asset type and acceptability and valuation policies should be established and communicated to relevant departments. Bankers and financial service professionals are in-charge of ensuring that the proposed asset is properly valued by a reliable and independent appraiser.

Once the customer has drawn the funds from the bank, bank should have a timely control over the pledged assets to ensure that they have not been sold or transferred to the third party without any notification made to the bank. By not doing so may result in the bank losing its capability to claim such assets once the loan becomes non-operating. The table below presents more information on the minimum standards recommendation over asset verification activities.

| Rank | Description |
|------|--|
| 1 | Bank Business has a clear Asset type Acceptability and Valuation Policy. This must define acceptable Asset types and Percentage Coverage; and a robust, independent (this doesn't necessarily mean external) reliable process to initially validate (and afterwards routinely monitor) any customer-supplied or customer-directed valuations. |
| 2 | Monthly quality control on sample of assets |
| 3 | Bank Business has a Policy, and an ongoing Monitoring Program, to ensure that adequate Insurance is at all times in place, and sufficient to reimburse the Bank Business, in the event of theft, loss, destruction or damage to the collateral Bank Business's interest in the policy to be noted on that policy). |
| 4 | In the event of the Bank Business's collateral could be sold, or used again as collateral, with good title but without that business's knowledge (e.g. where no restrictive lien can be recorded to encumber the asset), that risk must be disclosed as part of the credit application/approval and the monitoring program should be modified to mitigate that serious risk as much as it can be |
| 5 | Bank Business has an effective collateral database that uniquely identifies every relevant asset and shows its ownership and valuation history and any prior/current encumbrances |
| 6 | Drive By process on high risk assets |
| 7 | In the event prolonged deal negotiations, asset verification checks refreshed immediately before signing and prior to any pay-out |
| 8 | Create Valuation Panel comprising selected professionally qualified staff that have adequate PI (Professional Indemnity) insurance and a strong financial position |

| Rank | Description |
|------|--|
| 9 | For Project Finance the bank engages the assistance of appropriately qualified professional e.g. quantity surveyor to confirm customer's claims as to completeness of project/project state prior to pay out |
| 10 | Process that allows for lawful foreclosure and recovery of assets / funds |
| 11 | In the event the Banking Business becomes aware of any improper/illegal behaviour by the customer, the fraud/credit risk implications are properly/independently assessed, e.g. where tax penalties can lead to the authorities having a prior claim to company's assets |

d) Revolving Fund - Redraw Ability

Account takeover for commercial loan is not a critical issue since bank either pays money directly to the supplier or loan is drawn directly from the company's bank account. This company account will normally be drawn only by the authorised person. Nevertheless, the bank should follow a recommended activity outlined below to identify any exception report and also mitigate fraud risks that might occur.

| Rank | Description |
|------|---|
| 1 | Company/Account Takeover Controls: Ability to identify high risk transactions and create Exception Report and/or customer mandate changes (I.e. those authorised to sign for the customer company and any restrictions on their authorities/signing rights) |

e) Know your staff (KYS)

One of the key operating successes of bank is to recruit and hire the right person. Human Resources department is a first level of due diligence effort over bank applicants. Thus, they should have effective policies and procedures in the recruitment process prior to job offering and employment any staff. One of the recommended HR guidance is to check the applicant's profile including financial status to ensure that the applicant does not have any financial pressure that could potential leads to asset misappropriation. Employment approval process and applicant's profile reviewing process should be segregated from each other.

Banks should launch effective whistle blowing practices within the organisation and also provide the employees with strict confidences that no information would be disclosed publicly. This policy should be communicated widely in the organisation and updated on a timely basis, at least once a year.

| Rank | Description |
|------|---|
| 1 | Background Employment Screening (See HR guidelines & also check financial status of employees on an annual basis to ensure they are not under any financial pressure) |
| 2 | ISM (Investigation & Security Manager) Capability with Feedback loop to Fraud Prevention team |
| 3 | Separate approval process and review process for Staff accounts |
| 4 | Exception Reporting identifying accounts that are High Risk for internal fraud |
| 5 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually |

f) Third party payments / disbursements

Borrowers enter into a loan agreement because they would like to use this source of fund to pay their suppliers for goods purchased or services rendered. Banks should ensure that this amount of money has been received directly by the suppliers instead of being spent on another purpose

as previously mentioned in the loan agreement.

| Rank | Description |
|------|---|
| 1 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid |
| 2 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns |
| 3 | Payments to dealers / suppliers against full documentation |
| 4 | Match bank payment details to staff bank accounts |
| 5 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |

g) Reporting

Reporting is an essential tool for management to prevent and early detect fraudulent activities in the organisation. For commercial loan, it is highly recommended for fraud cases that have significant impact on business be reported to the bank's headquarters. Key data related to underwriting and business transactions are recognised as important information. Therefore, these critical information should be promptly collected, gathered, consolidated and used for all the fraud investigation efforts and risk analysis processes. Additionally, there are several reports that are necessary for monitoring purposes.

Listed below are the more important reports that should be established as the minimum standard.

| Rank | Description |
|------|--|
| 1 | Fraud cases reported to the bank's headquarters. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. |
| 2 | Fraud Prevention/Detection/ Losses analyzed and reported by process weakness. |
| 3 | Monthly reporting: Gross/Net Fraud; Fraud triggers driven fraud budget; Fraud to Write off, Fraud to NI, W/O (Write-off) no payments- in line with business plan. |
| 4 | Key underwriting and transaction data tracked and used for fraud analysis. |
| 5 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. |
| 6 | Exception reports for high risk transactions. |
| 7 | Fraud Prevention/Detection/ Losses broken down by fraud type. |
| 8 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. |

h) Operational efficiency

In today's business, controls are an important mechanism implemented in the organisation. Not only to mitigate losses from fraud but they enable banks to improve their operational efficiency. Surprise audit and periodic review by Internal Audit or independent third party is strongly recommended for commercial loan. In terms of policies and procedures, management should ensure that they are clearly defined and explicitly cover important items like bad debt write-off, fraud prevention and detection, etc.

Moreover, other recommendations for banks include, for instance, the responsibilities of Risk Management function and Fraud Analyst, designated channels for reporting and monitoring of fraudulent behaviour/activities, fraud awareness training, etc.

Each of the minimum standards that banks should implement is detailed in the table below.

| Rank | Description |
|------|---|
| 1 | Surprise audit and periodic review by Internal Audit or independent third party should be in place. |
| 2 | Formalised write-off policy and procedure should be in place. |
| 3 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. |
| 4 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. |
| 5 | Formalised fraud policy and procedure should be developed. |
| 6 | Data leakage from both paper-based and electronic-based should be controlled. |
| 7 | Well promoted whistle blower program should be one of channels to report fraud case at anytime. Moreover, a case management process to deal with the reported issues should be developed. |
| 8 | Fraud analyst should analyse fraud losses and review rule sets in fraud detection tools on an ongoing basis. |
| 9 | The procedure for fraud alert process across industry peers should be developed. |
| 10 | Random checks for underwriting process compliance should be performed. |
| 11 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. |
| 12 | Fraud training programs should be conducted for Underwriting staff. |
| 13 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. |
| 14 | Fraud prevention awareness should be raised and communicated regularly in the management level. |
| 15 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. |
| 16 | Bad debt written off that is collected from customers in later period should be controlled. |

i) Fraud technology

Technology has advanced and accepted as an enabling tool for fraud prevention and detection as some Thai financial institutions have decided to license and implemented these technologies to reduce losses from fraud. For many of these technology options, the ability to interface directly with the Anti-Money Laundering (AML) application is the most important feature when choosing the suitable fraud prevention/detection solution as the system architecture and data sources are very much similar and could be complementing one another.

There are quite a number of system requirements that banks need to consider. Some of them are the compatibility and interoperability with existing core banking system, the ability to prioritise fraud cases according to risk scores, detecting fraudulent transactions in real-time and 24 hours a day, seven days a week, integrating transactions from different sources/systems, enabling users to design and generate a report template, detecting the similarity of names and addresses to surface hidden relationships, etc.

Not only are specific features provided by fraud technology itself, but it is also recommended that case management tool with workflow capability be deployed, report/dashboard should be generated in different views based on roles and responsibilities, and access to these dedicated hardware/server/database be restricted to a group of fraud specialist.

The following outlines the minimum standard recommendations for banks when implementing fraud prevention/detection technology.

| Rank | Description |
|------|--|
| 1 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. |
| 2 | Fraud technology should be deployed to combat internal fraud. |
| 3 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. |
| 4 | Fraud technology should be compatible with existing core banking system. |
| 5 | Banks should implement case management tool with workflow capability. |
| 6 | Fraud technology should be deployed to combat external fraud. |
| 7 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. |
| 8 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. |
| 9 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. |
| 10 | Fraud technology should have the ability to prioritise each fraud case according to risk scores and notify suspicious activities to the management. |
| 11 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, seven days a week. |
| 12 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. |
| 13 | Fraud technology should allow banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. |
| 14 | Fraud detection solution should enable users to design and generate a report template that can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. |
| 15 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. |
| 16 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. |
| 17 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyze and alert the responsible people in case of any unusual transactions or suspicious behaviour. |
| 18 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. |
| 19 | Social Network Analysis should be used to detect and visualise fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. |
| 20 | Banks should implement pre-built software specifically for fraud detection technology. |

Practice Recommendation

a) Know your customer (KYC)

A clear policy on granting multiple loans to the same company / address should be established and communicated to all relevant professionals within the bank. Banker should be able to identify any loans that are applied for by the same party who is currently maxing out their credit line limit. In addition, exception report should be regularly produced to summarise any unreasonable

approval from the same underwriter. More guidance should be followed to ensure bank's effectiveness in mitigating fraud risks that might occur and perpetrated by their customers.

| Rank | Description |
|------|--|
| 1 | Ability to Limit No. of loans to same name/address |
| 2 | Independent Credit Control / Admin function to carry out all initial and periodic checks and monitoring activities |
| 3 | Install KYC tool where sufficient applications available |
| 4 | Policy and resources deployed to carry out meaningful, regular, skilled and independent monitoring of financial performance, adherence to covenants, site visits, documented regular Call Reports from Sales, Exception Reports on deviations / deficiencies / breaches and suggested Corrective Actions showing any overdue / missed promises |
| 5 | - customer's justification of credit need / underlying transaction rationale - customer's reason for choosing Bank as credit provider |
| 6 | A process to both GENERATE and CAPTURE (from other Bank Businesses and from other Financial Institutions) 'Fraud Alerts' / Fraud Intelligence to minimise the possibility of falling victim to already-known fraud schemes. |
| 7 | Ability for system to capture (and permanently retain) underwriting decisions and data and to create relevant Exception Reports as required |
| 8 | Policy to protect the Business's interests and security in respect of cross-border lending or where the collateral is already, or may move, to another country |

b) Know your intermediaries (KYI)

Intermediary's operational performance should be evaluated at least once a month to ensure that the customers who are primarily screened by that particular intermediary are still the operating customers. Furthermore, bank should consistently check the financial situation of accredited intermediaries to gain some certainty that those intermediaries are not in any financial distress. Otherwise, they may collude with some customers to defraud the bank.

| Rank | Description |
|------|---|
| 1 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit / site visit processes. |
| 2 | Carry out site visits prior to accreditation of Intermediaries |
| 3 | Monthly grading process must provide for termination of intermediaries depending on performance. If intermediary offers a range of products then intermediary should be terminated across all products. |
| 4 | KYI tool installed to defined steps with risk rating mechanism for intermediaries - i.e. Actimize |
| 5 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. |
| 6 | Reward scheme for Intermediaries who detect / warn about fraud (i.e. reward, rather than punish, Good Behaviour). |
| 7 | Intermediaries have Public Indemnity Insurance to cover fraud committed by, or colluded in, by their staff |

c) Asset verification

For non-performing loans, bank should be able to seize the pledged assets and collaterals. However, these assets should be well-monitored to ensure that they have not yet been transferred or there should not be any signal of transfer pricing for specific assets. Furthermore, fraud recovery processes should be established in addition to bank's normal recovery processes. This will keep the bank alert on certain red flags that might occur with the pledged assets.

| Rank | Description |
|------|--|
| 1 | Process that allows for the clear establishment of Bank lien / charge against the title to the asset within a short time frame |
| 2 | Bank Business can deploy adequate expertise to reach out to assets owned by individuals in making claims under personal guarantees given that fraudulent transfer of assets frequently occurs |
| 3 | Bank Business pays special attention to situations where complex transfer pricing arrangements exist (especially relevant where there is intra-corporate transfer pricing) |
| 4 | Bank Business has a process to monitor and respond to environmental changes that would materially increase the risk of fraud |
| 5 | Checking against any national / industry registers that show current/prior charges (encumbrances) against those assets |
| 6 | Fraud Recoveries process in addition to 'normal' recoveries |
| 7 | Bank Business has deployed GPS tracking equipment or such like technical equipment to flag unauthorised movement of mobile assets and/or to assist in their recovery in the event of theft, consider secret (covert) deployment where lawfully allowed |

d) Revolving Fund - Redraw Ability

Even though fraud risk under revolving fund is not as high, bank should still have some processes / controls to minimise the fraud risks that might be associated with large and available credit limits.

| Rank | Description |
|------|---|
| 1 | The Bank Business has in place processes /controls to minimise the fraud risks associated with large available undrawn credit facilities (e.g. account takeover fraud in fund transfers etc.) |

e) Know your staff (KYS)

Not only does the bank have to check background information of potential employees, they should be able to identify staff and their related parties' bank accounts once the bank employs that particular person. This will enable the bank the ability to monitoring activities to avoid internal fraud from their employees since some staff may transfer funds from bank's customer accounts into their own or related parties' accounts.

In some circumstances that banker also acts as sales staff to offer some products to the customers. Bank should monitor and make some comparison over the staff sales performance to ensure that their staffs do not create many sales with low profile customers. Bank should also have a particular report to summarise sales for each staff comparing with non operating customers who are proposed by particular staff.

| Rank | Description |
|------|---|
| 1 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should neither maintain their own (customer) account, nor a related parties (customer) account. |
| 2 | Can employees access into other banks beyond the bank they are working for? |
| 3 | Ability to identify staff accounts. Monitor staff and related party accounts for internal fraud |

| Rank | Description |
|------|---|
| 4 | Business has in place an appropriate process to reward Sales, Underwriting and other staff for reducing fraud risk/loss |
| 5 | Installation of KYS tool - egg Intellinx/Footprint |

f) Third party payments / disbursements

Normally, the bank is responsible to issue direct disbursement to the seller of the property. Bank should ensure that they receive all required supporting documents and evidences prior to the issuances of the funds. Another importance note for any disbursements to the borrowers is to ensure that the recipient of money is not the bank's employee or their related parties' bank accounts.

In case of any changes to detail of recipient's bank accounts, banker should check and confirm with the recipient for any updated information to ensure that the bank makes disbursements to the right party. Bank should have a system that can identify multiple supplier payment details to the same bank account. This will help in mitigating fraud risk of disbursement to fictitious suppliers.

| Rank | Description |
|------|--|
| 1 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier |
| 2 | Ability to identify multiple dealer / supplier payment details to same bank account |
| 3 | Review triggers for \$ payments by dealer / supplier type |

g) Reporting

For commercial loan, banks should consider creating and monitoring additional reports for fraud prevention and detection efforts, for instance, the use of enterprise-wide fraud case management with monthly management and / or audit committee reports with cases relevant to external fraud and internal misconduct, etc.

Details of recommended reports are presented in the following table.

| Rank | Description |
|------|---|
| 1 | Monthly reports relevant to fraud trends and comments. |
| 2 | Fraud case management report including the progression and follow-up of fraud investigation, and exchange of fraud information/news. In addition, fraud cases should be reported to the Bank of Thailand. |
| 3 | Monthly reports including follow-up action items. |
| 4 | Fraud Prevention/Detection/ Losses broken down by portfolio. |
| 5 | Variance analysis and development of control charts. |

h) Operational efficiency

To increase the operational efficiency, it is recommended that banks consider the review of high risk application or customer accounts, their corporate code of conduct, fraud detection methods, fraud alert process, operating procedure for fraud case management, fraud awareness training, reward/incentive program, employee's KPI, etc.

Listed below are suggested practice recommendations for commercial loan.

| Rank | Description |
|------|--|
| 1 | 100% review of high risk application or accounts should be conducted. For example, |

| Rank | Description |
|------|--|
| | - 3PD or 2PD with no customer contact - Accounts that are potentially "Skip" accounts < 210 days on book - Accounts where mail has been returned from the outset of the account opening. |
| 2 | Code of conduct should include clear definition of fraud. |
| 3 | The members of the Fraud team should consist of staff from Operations and Analytics. |
| 4 | Fraud detection methods should be tailored to needs of individual portfolio. |
| 5 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. |
| 6 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. |
| 7 | Fraud Coordinator should ensure that 'Close the loop' process is finalised. |
| 8 | Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit. |
| 9 | Fraud awareness training should be provided to employees at least every six months. |
| 10 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. |
| 11 | Employee's KPIs should be established based on the risk associated with their tasks. |

i) Fraud technology

When evaluating and implementing fraud prevention/detection technology, the proposed solution should have the ability to process information efficiently and respond in acceptable period, it should includes analytics features that yield and calculate risk scores for wide ranges of potential fraud concerns, enable Fraud Intelligence team or IT staff with the ability maintain and update the configurations/business rules, etc.

Moreover, some of other recommendations are the development of common data model to capture data from different sources, and leveraging Business Intelligent (BI) technology to enhance the ability to consolidate information and detect suspicious transactions.

All of the practice recommendations include:

| Rank | Description |
|------|--|
| 1 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. |
| 2 | Social Network Analysis should be used to detect and visualise fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. |
| 3 | Banks should implement pre-built software specifically for fraud detection technology. |
| 4 | Fraud detection solution should process efficiently and respond back within targeted period. |
| 5 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. |
| 6 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. |
| 7 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. |
| 8 | Suspicious activities/transactions or exception reports can be extracted from |

| Rank | Description |
|------|---|
| | fraud technology and used for further investigation on a daily basis. |
| 9 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. |
| 10 | Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide faster and efficient support. |
| 11 | False positives created from the current technology should be reduced due to poor data quality. By definition, the false positives are transactions that fraud detection tool flags as suspicious but they are not actually fraudulent. |
| 12 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. |
| 13 | Banks should update fraud detection techniques regularly, at least once a month. |
| 14 | The pre-built data model should be created for the bank's existing systems. |

2. Hire Purchase

Hire Purchase or Car leasing is one type of popular loan product given to the borrowers who subsequently use their car as collateral and guarantee for entering into the loan agreement with the bank. Currently, many banks provide this type of loan to the market place.

Presently, fraud risk from hire purchase is quite high in comparison to other types of loan. Some customer may borrow money from the bank in the form of hire purchase and use their car as a guarantee. However, they may intentionally default their repayment to the bank and sell their cars to third party. As a result, the minimum standard recommendations below should be strictly followed to avoid and mitigate these popular fraud schemes and the associating risks.

Minimum Standards Recommendation

We categorise each recommendation according to the relevant activities operated by the bank as follows:

a) Know your customer (KYC)

In general, banks should have reasonable background knowledge over their target customers before giving out any loans to them. As a result, bank should have a policy to verify the background information of each loan applicant in order to ensure their existence and authenticity. The verification process should be performed by using public database. For example, banker should check whether the applicant's telephone number is legally registered or the provided contact address is a legitimate address. In addition, bank should have access to either internal or external databases with information of all potential blacklisted companies and individuals such as defaulted customers or fraudulent customers - the process should be in-placed to profile customer group into various segments. The update of high value fraud loss should be documented in the bank's enterprise wide case management database where all the relevant parties across different product department receiving such alerts and information on a timely basis.

| Rank | Description |
|------|--|
| 1 | Underwriting Policy noting : ID verification procedure, : employment/income verification procedure : address verification procedure : phone verification procedure : weighted bureau data |
| 2 | Fraud Blacklisting Capability |
| 3 | Centrally located underwriting, segregation between Sales and Underwriting Teams |
| 4 | High value Fraud alerts to other portfolio's at country level |
| 5 | Conforms to CRP as signed off |
| 6 | Face to Face meeting with customer (signing phase) for Vehicle |
| 7 | If business operates via Intermediaries then must have documented process to audit KYC checks conducted by intermediary |
| 8 | Approved methodology for high Risk designation using historical data and current fraud trends |
| 9 | Ability for system to capture underwriting data (create relevant Exception reports as required) |
| 10 | Install KYC tool |

b) Know your intermediaries (KYI)

Majority of the car dealers will act as the bank's intermediary since they assist their customers in finding sources of funding to purchase their cars. However, bank should ensure that those intermediaries perform their jobs in transparent manner since they are the primary filter for particular hire purchase applicants. Before appointing any party as the bank's intermediary, bank should check all possible information such as company background, financial position, credit rating, etc. Bank should also perform a site visit prior to and after accreditation of particular intermediaries.

Moreover, bank should have a reliable database with information of intermediary blacklist and also that bank should appoint some staff to continually monitor the performance of the appointed intermediaries. This will help ensure that loans given out to the customers, proposed by particular intermediaries, are the performing customers.

| Rank | Description |
|------|--|
| 1 | Robust Intermediary accreditation process – See Compliance guidelines |
| 2 | Segment and Monitor by underwriter and/or Sales rep |
| 3 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups. Checks that if Intermediary terminated then terminated across all intermediary listings. |
| 4 | Intermediary Fraud - Included in contract with Intermediary is reimbursement for Internal Fraud. Or encourage Intermediary to take out insurance for internal fraud. |
| 5 | Monthly Reporting on Intermediaries using performance triggers as review point i.e. Approval rate, W/O's, 3PD, Sales volume, delinquency, TTY, Fraud Loss. |
| 6 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level |
| 7 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. |
| 8 | Perform site visitation prior to accreditation of broker |

c) Asset verification

Normally, hire purchase agreement would require the purchased assets as the collaterals or pledged assets. Bank will transfer the title deed of this asset to the borrower once all instalments are paid in full. After hire purchase agreement has been signed, bank should consistently monitor the purchased assets and prevent them from being sold to the third party without any consent from the bank. Some of the recommending activities below should be performed to mitigate fraud risk from this type of loan.

| Rank | Description |
|------|--|
| 1 | Clearly defined asset type that will be eligible for loans, Caps on extra's as defined by policy |
| 2 | Prevent/monitor for forward sale of asset by customer |
| 3 | Process that allows clear title registration over asset within a set time frame i.e. check of Engine No., registration etc |
| 4 | If asset is not registered prior to disbursement then audit to ensure asset is secured within prescribed time frame |
| 5 | Provide Plan for ability to identify 'at risk' accounts where asset may be on sold without finalising settlement |
| 6 | Auto Asset Verification (AAV) compliant - Outbound verification calls made directly to customer - may be sample based on risk modelling of dealers |

| Rank | Description |
|------|--|
| 7 | Independent Asset validation process - valuation checked through independent database i.e. Database with range of prices for new and used vehicles by make and model |
| 8 | For inventory finance, regular vehicle inspection and random checks |

d) Know your staff (KYS)

Internal fraud is considered one of the critical issues within the bank's operation. To hire the right person to work with the organisation, bank should set a clear HR policy which should cover possible guidance to screen, attract and employ ethical people. One of the most important things is to check the background information of the applicants. Bank should check whether or not their applicant and related persons are listed in the blacklist database. Secondly, the segregation of duties between approval and credit reviewing process is another important factor to mitigate fraud risk within the organisation. The table below provides more information on "Know your staff" section.

| Rank | Description |
|------|--|
| 1 | IT Security where system access is dictated by role |
| 2 | ISM Capability with Feedback loop to Prevention |
| 3 | Monitor staff and related party accounts for internal fraud - Monitor monthly approval rates and write offs by individual staff (Sales, U/writing and Collections staff) |
| 4 | Background Employment Screening (See HR guidelines) (Also check financial status of employees on an annual basis to ensure they are not in a financial pressure) |
| 5 | Separate approval process and review process for Staff accounts |

e) Third party payments / disbursements

Normally, bank is responsible to make direct payment to the seller of the automobile. Bank should ensure that they receive all required supporting documentation before any money is paid out. Another importance factor for any disbursements to the borrowers is to ensure that the recipient account is not their own staff's or their related parties' bank accounts.

In case of any changes to the detail of recipient's bank accounts, banker should check and confirm with the recipient for any updated information to ensure that bank makes disbursements to the right party. Moreover, bank should have a system which can identify multiple supplier payment details to the same bank account. This will help mitigating fraud risk from creating fictitious suppliers.

| Rank | Description |
|------|---|
| 1 | Payments to dealers against full documentation |
| 2 | Payments directly to dealer, not to customer with expectation that supplier is paid |
| 3 | Robust process for registration of new supplier |
| 4 | Ability to identify multiple supplier payment details to same bank account |
| 5 | Independent checking/confirmation when notified of changes to payment details of supplier |

f) Reporting

Similar to commercial loan, it is strongly recommended for fraud cases that impact materially on the business dealings be reported to the bank's headquarters. Moreover, to enhance the efficiency and effectiveness of fraud prevention and detection, banks should prepare monitoring reports that, at the minimum, produce fraud incident reports monthly, fraud type analysis, summary report of fraud investigation, and fraud prevention/detection/losses report.

Listed below are the reports that should be produced and monitored as minimum standards recommendation.

| Rank | Description |
|------|--|
| 1 | Fraud cases reported to the bank's headquarters. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. |
| 2 | Monthly reporting: Gross/Net Fraud; Fraud to Sales ; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O (Write-off) no payments, Skip/Trace <90MOB; Fraud savings, Investigation, Recoveries> |
| 3 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. |
| 4 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. |
| 5 | Fraud Prevention/Detection/ Losses analyzed and reported by process weakness. |

g) Operational efficiency

As the information become more valuable in organisations, controls implemented to prevent data losses including paper-based and electronic-based is most essential for hire purchase products. It is recommended that policies and procedures be in place to cover various tasks of fraud prevention and detection, bad debt write-off, improper/unusual payment to the political exposed individuals or government officials, etc.

Some of other important standards that banks should comply with are the task of preparing check lists for the centralise loan approval process, the responsibilities assigned to Risk Management function and Fraud Analyst, code of conduct, random checks for underwriting process, fraud awareness training, channels being used for reporting and monitoring fraudulent behaviour/activities, regular Fraud Council meeting, etc.

Each of the minimum standards recommendation are listed as follows:

| Rank | Description |
|------|--|
| 1 | Data leakage from both paper-based and electronic-based should be controlled. |
| 2 | Formalised fraud policy and procedure should be developed. |
| 3 | Centrally located underwriting with documented check list of loans should be in place. |
| 4 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. |
| 5 | Formalised write-off policy and procedure should be in place. |
| 6 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. |
| 7 | Fraud analyst should analyse fraud losses and review rule sets in fraud detection tools on an ongoing basis. |
| 8 | Operating procedures should be in place and Fraud Case Management |

| Rank | Description |
|------|---|
| | should be deployed to alert fraudulent activities to Fraud team and Internal Audit. |
| 9 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. |
| 10 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. |
| 11 | Code of conduct should include clear definition of fraud. |
| 12 | Random checks for underwriting process compliance should be performed. |
| 13 | Fraud training programs should be conducted for Underwriting staff. |
| 14 | Involvement/sign off in CRP (Credit Review Point) and NPI (New Product Innovations) process |
| 15 | Fraud Coordinator should be assigned to coordinate between Fraud Risk Manager and ISM. Moreover, regular meeting between these two groups should be arranged to ensure open communication and close gaps. |
| 16 | Well promoted whistle blower program should be one of channels to report fraud cases at anytime. Moreover, a case management process to deal with the reported issues should be developed. |
| 17 | Fraud detection methods should be tailored to needs of individual portfolio. |
| 18 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. |
| 19 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. |
| 20 | Key underwriting and transaction data should be tracked and used for fraud analysis. |

h) Fraud technology

In respect to hire purchase, the most important minimum standard is to restrict access to dedicated hardware/server/database of fraud prevention/detection technology. This should be granted to Fraud/Internal Audit team.

With a rise of money-laundering, the fraud prevention/detection solution being deployed in the organisations should include the ability to interface with the Anti-Money Laundering (AML) application. Other features of fraud technology that are recommended for banks consisted of, for example, the ability to prioritise fraud cases according to risk scores, compatibility with the core banking system, ability to interface with other legacy systems, detect fraudulent transactions in real-time and 24 hours a day, seven days a week, and ability to leverage such technology for both combating external and internal fraud, etc.

The table below illustrates all of recommendations for minimum standards.

| Rank | Description |
|------|---|
| 1 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. |
| 2 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. |
| 3 | Fraud technology should be deployed to combat external fraud. |
| 4 | Fraud technology should have the ability to prioritise each fraud case according to risk scores and notify suspicious activities to the management. |
| 5 | Fraud technology should be compatible with existing core banking system. |
| 6 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week. |
| 7 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. |

| Rank | Description |
|------|---|
| 8 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. |
| 9 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. |
| 10 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. |
| 11 | Fraud technology should be deployed to combat internal fraud. |
| 12 | Banks should implement case management tool with workflow capability. |
| 13 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. |
| 14 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. |
| 15 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. |
| 16 | Banks should implement pre-built software specifically for fraud detection technology. |
| 17 | Fraud detection solution should process efficiently and respond back within targeted period. |
| 18 | Social Network Analysis should be used to detect and visualise fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. |

Practice Recommendation

a) Know your customer (KYC)

Under hire purchase agreement, bank should have a database or system identifying and updating information of the customer group that are classify as high risk profile. For example, customers who are residing in the border area of Thailand who could illegally transport and sell the vehicle in the neighbouring countries or customers who have purchased vehicles that are known to be in high demand in the black market.

Moreover, Bank should have a policy on validating the information of hire purchase applicants through the publicly available database to identify the existence and authentication of the customers. In addition, they should have a system with the ability to identify any duplicate applications which have been both approved and declined previously. In general, first hire purchase loan should be settled before applying for another hire purchase loan unless there is some evidence confirming that applicant has sufficient source of fund to repay the second hire purchase loan.

| Rank | Description |
|------|---|
| 1 | Utilise high risk profiles for additional targeting |
| 2 | Validated address/phone number through public databases |
| 3 | Policy around Foreign Nationals |
| 4 | Install Fraud Scorecard |
| 5 | De-Duplicate previous application process (approved and declined apps) |
| 6 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |
| 7 | Approved policy limiting no. of loans to same family/same address |
| 8 | No second deal to be approved before first loan payment is cleared. |

b) Know your intermediaries (KYI)

Dealers' / intermediaries' performance should be reviewed continually to ensure that they performance their work efficiently and transparently. Not only the operating performance, bank should also check the credit of the intermediary / or its financial position to identify any financial pressure. This can be done annually by bank internal departments or by independent third party.

| Rank | Description |
|------|--|
| 1 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. |
| 2 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. |
| 3 | Monthly grading process must provide for closure of intermediaries depending on Performance |
| 4 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |
| 5 | KYI tool installed - i.e. Actimize |
| 6 | Intermediaries have PI Insurance to cover Intermediary fraud |

c) Asset verification

Not only the previous minimum standard recommendation for asset verification, bank should also place some auditing process over the asset verification activities to make sure that all listed activities have been performed according and efficiently.

| Rank | Description |
|------|---|
| 1 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |

d) Know your staff (KYS)

Beyond hiring the right people to work with the bank, bank should be capable of identifying its staff bank account and related parties bank account to monitor whether there is any unusual money transferred during the period. Furthermore, bank should review sales bonus of the staff and identify any significantly variance from other staff under the same conditions such as position level, location of work, etc.

| Rank | Description |
|------|---|
| 1 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |
| 2 | Installation of KYS tool - Intellinx/Footprint |
| 3 | Can employees access into other banks beyond the bank they are working for? |
| 4 | Review process for Staff receiving Sales bonus's |
| 5 | Ability to identify staff accounts. |

e) Third party payments / disbursements

Bank should have some system to identify and match any unusual payment transfer to the staff bank's account, for example, large and frequent payment is made.

| Rank | Description |
|------|-------------|
|------|-------------|

| Rank | Description |
|------|---|
| 1 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns |
| 2 | Review triggers for \$ payments by supplier type |
| 3 | Match bank payment details to staff bank accounts |
| 4 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |

f) Reporting

To detect fraudulent activities more efficiently, there are three main reports by which banks should consider as practice recommendation for hire purchase. Details of the reports are listed in the following table.

| Rank | Description |
|------|---|
| 1 | Fraud Prevention/Detection/ Losses broken down by fraud type. |
| 2 | Monthly reports relevant to fraud trends and comments. |
| 3 | Fraud Prevention/Detection/ Losses broken down by portfolio. |
| 4 | Monthly reports including follow-up action items. |
| 5 | Variance analysis and development of control charts. |

g) Operational efficiency

For hire purchase, it is recommended that communication of and training about fraud prevention awareness, controlling the debt collection after write-off, conducting bi-annual auditing processes, reward/incentive program for those who can prevent/detect fraud are some of the practice recommendation.

Listed below are suggested practice recommendations.

| Rank | Description |
|------|--|
| 1 | Fraud prevention awareness should be raised and communicated regularly in the management level. |
| 2 | Bad debt written off that is collected from customers in later period should be controlled. |
| 3 | The members of the Fraud team should consist of staff from Operations and Analytics. |
| 4 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded. |
| 5 | The procedure for fraud alert process across industry peers should be developed. |
| 6 | Fraud awareness training should be provided to employees at least every six months. |
| 7 | Employee's KPIs should be established based on the risk associated with their tasks. |
| 8 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. |

h) Fraud technology

With the implementation of fraud prevention/detection technology, banks should consider the abilities of application, for example, integrating transactions from different sources, calculating risk scores for potential fraud, generating reports in different views, detect the similarity of names and addresses, etc.

Each of the practice recommendations are:

| Rank | Description |
|------|--|
| 1 | Fraud technology should allow banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. |
| 2 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. |
| 3 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. |
| 4 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. |
| 5 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. |
| 6 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyze and alert the responsible people in case of any unusual transactions or suspicious behaviour. |
| 7 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. |
| 8 | Banks should update fraud detection techniques regularly, at least once a month. |
| 9 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. |
| 10 | Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide faster and efficient support. |
| 11 | The pre-built data model should be created for the bank's existing systems. |
| 12 | False positives created from the current technology should be reduced due to poor data quality. By definition, the false positives are transactions that fraud detection tool flags as suspicious but they are not actually fraudulent. |
| 13 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. |

3. Merchant

In today's world, people tend to spend more money using a credit card to purchase their interests such as food, clothes, accessories, etc. Department stores and shops need to have at least a slot card machine to serve their customers' spending behaviour. As a result, bank has to provide this service to the market, and as mentioned earlier, spending behaviour has changed dramatically over recent years.

To avoid fraud risk of using credit card by both customers and shops, bank should comply with the minimum standard recommendations below. This will create some assurance for both parties that fraud would rarely occur from credit card spending.

Minimum Standards Recommendation

We categorise each recommendation according to the relevant activities operated by the bank as follows:

a) Know your customer (KYC)

In general, banks should have reasonable background knowledge over their customers before issuing any credit cards to them. As a result, bank should have a policy to verify the background information of each credit card applicant in order to ensure their existence and authenticity. The verification process should be performed by using public database. For example, banker should check whether the applicant's telephone number is registered or the provided contact address is real. In addition, bank should have available database which has the information for all potential blacklists such as default customers, fraudulent customers, etc.

Moreover, the underwriting policy should comply with risk management procedures to mitigate high risk accounts. The update of high value fraud should be done in the bank database frequently and also that the relevant parties obtain the alert information on any updated high value fraud on a timely basis. High risk profile should also be considered before any credit card applicants are approved or denied. The table below provides more information that should be followed during the reviewing and approval process of this product.

| Rank | Description |
|------|---|
| 1 | Underwriting Policy noting : ID verification procedure, predefined acceptable documents : ID verification procedure for merchant (Approved designees) : employment/income verification procedure : address verification procedure : phone verification procedure, e.g. no third party phones for 0% down payment : weighted bureau data |
| 2 | If business operates via Intermediaries then must have documented process to audit KYC checks conducted by intermediary |
| 3 | Conforms to CRP (Credit Review Point) as signed off |
| 4 | Policy around Foreign Nationals |
| 5 | Fraud Blacklisting Capability |
| 6 | Centrally located underwriting, segregation between Sales and Underwriting Teams |
| 7 | Utilize high risk profiles for additional targeting |
| 8 | High value Fraud alerts to other portfolio's at country level |
| 9 | Ability for system to capture underwriting data (create relevant Exception reports as required) |
| 10 | De-Duplicate previous application process (approved and declined apps) |

| Rank | Description |
|------|--|
| 11 | Install KYC tool where sufficient data available |

b) Know your intermediaries (KYI)

Sometimes banks may need third party to act as their intermediary to assist in finding potential customers. However, bank should be able to ensure that those intermediaries perform their jobs transparently since they are the primary filter for particular credit card applicants. Before accrediting any party as the bank's intermediary, bank should check all possible information such as company background, financial position, credit rating, etc. Bank should perform a site visit prior and after accreditation of particular intermediaries. In case that the intermediary is the individual person, bank should check whether that person is listed in the blacklist and also check the past performance of that person to ensure that he / she does not create any fake credit card applicants. Moreover bank should appoint some staff to continually monitor the performance of the appointed intermediaries. This will help them ensure that loans given out to the customers, proposed by particular intermediaries, are the operating loans.

| Rank | Description |
|------|--|
| 1 | Segment and Monitor by underwriter and/or Sales representative |
| 2 | Robust Intermediary accreditation process – See Compliance guidelines |
| 3 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups. Checks that if Intermediary terminated then terminated across all intermediary listings. |
| 4 | Monthly Reporting on Intermediaries using performance triggers as review point i.e. Approval rate, W/O's(Write Offs) , 3PD(Payments Delinquent/Default), Sales volume, delinquency, TTY, Fraud Loss. |
| 5 | Intermediary Fraud / Intermediary contract should include clauses that allow recourse to Intermediary for fraud. Or encourage Intermediary to take out insurance for internal fraud. |
| 6 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. |
| 7 | Monthly grading process must provide for closure of intermediaries depending on Performance |
| 8 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. |

c) Revolving Fund - Redraw Ability

Listed in table below are the primary activities that should be followed to mitigate all risks, especially fraud risks.

| Rank | Description |
|------|---|
| 1 | Card Mailing Controls: : Dead card mailing : IVR or voice support activation : Returned Card Procedures : Card activation on new and reissued cards : Mail disguise (Plain white envelopes) or Mail mixing strategy i.e. mixture of mail houses and cards sent over a period of time |
| 2 | Authorisation Controls : Adaptive controls for high risk transaction segmentation : Adaptive controls specific to high risk cash transactions |

| Rank | Description |
|------|--|
| 3 | Account Takeover Controls - Ability to monitor for : Address change followed by card/PIN reissue : Activity on inactive accounts : Address change requests on lost/stolen cards |
| 4 | BIN attacks : Track unissued BIN ranges or unissued card no. : When issuing large no. of cards in same BIN range ensure they have a range of expiry dates : Investigate auth or clearing requests that contain un-issued card no. or invalid expiry dates |
| 5 | Remote Channel - Card Not Present Authentication MasterCard 3D Secure Code Verified by Visa |
| 6 | Create 'high risk' re -payment model for suspect accounts or credit bust-outs |
| 7 | Card Mailing Controls : IVR (interactive Voice Response) Failure tracking : Tiered verification strategies : Outbound deliver verification calls |
| 8 | Common Point of Compromise tracking |
| 9 | Review for - large \$ payments - multiple # of payments in short time frame with large \$ value total |
| 10 | Falcon or Aristion installation - high risk strategies developed including anti-counterfeit and cross border strategies |
| 11 | Process where Open to Buy is only released on cleared funds |
| 12 | Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product |
| 13 | Remote Channel - Internet /e-business transaction monitoring : Adaptive Authentication in Host system : Geo-location Analysis |

d) Know your staff (KYS)

The important critical success factor is to hire the right person. Human Resources department is a first filter over bank applicants. Thus, they should have effective policies and procedures before employing any staff. One of the recommended HR guidance is to check the applicant's profile including financial status to ensure that the applicant does not have any financial pressure. Employment approval process and applicant's profile reviewing process should be segregated from each other.

Bank should launch an effective whistle blowing practices within the organisation and also give their employees strict confidence that no information would be disclosed publicly. This policy should be communicated widely in the organisation and updated on a timely basis, at least once a year.

| Rank | Description |
|------|--|
| 1 | IT Security create profiles where system access is dictated by role |
| 2 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually |
| 3 | Background Employment Screening (See HR guidelines & Also check financial status of employees on an annual basis to ensure they are not under any financial pressure) |
| 4 | Monitor staff and related party accounts for internal fraud - Monitor monthly approval rates and write offs by individual staff (Sales, U/writing and Collections staff) |

| Rank | Description |
|------|---|
| 5 | ISM (Investigations & Security Manager) Capability with Feedback loop to Prevention |
| 6 | Separate approval process and review process for Staff accounts |

e) Third party payments / disbursements

Degree of conformance to standards set by the bank should be at least twice a year audited to ensure that everything is in the right manner without any unusual circumstances.

| Rank | Description |
|------|---|
| 1 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |
| 2 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns |
| 3 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid |

f) Reporting

For merchants, reporting critical fraud cases found to the bank's headquarters is recognised as the first priority. To improve the prevention and detection of fraud, banks should prepare and monitor reports that include monthly report with follow-up action items, fraud type analysis, fraud case management report, and summary report of fraud investigation. In addition, banks should gather key underwriting and business transaction to be used for fraud investigation and risk analysis process.

Details of the reporting suggested as minimum standards are:

| Rank | Description |
|------|--|
| 1 | Fraud cases reported to the bank's headquarters. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. |
| 2 | Monthly reporting: Gross/Net Fraud; Fraud to Sales; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O (Write-off) no payments, Skip/Trace <90MOB (month on book); Fraud savings, Investigation, Recoveries. |
| 3 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. |
| 4 | Key underwriting and transaction data tracked and used for fraud analysis. |
| 5 | Fraud case management report including the progression and follow-up of fraud investigation, and exchange of fraud information/news. In addition, fraud cases should be reported to the Bank of Thailand. |
| 6 | Monthly reports including follow-up action Items. |
| 7 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. |

g) Operational efficiency

In terms of operational efficiency, the most important standard is involvement/sign off in credit review point and new product innovations process. Banks also should define the appropriate roles

and responsibilities of functions that are related to fraud prevention/detection, for instance, person who maintains fraud detection tools, Fraud Coordinator, Fraud Analyst, and Risk Management function.

Furthermore, some of other standards are the development of fraud alert process across portfolio, fraud policies and procedures, channels using for reporting fraud cases at anytime, bad debt write-off policy, review of high risk application or customer accounts, prevention of data leakage, conducting the review by Internal Audit or independent third party, code of conduct, etc.

It is recommended that banks should implement the minimum standards, as illustrated in the table below.

| Rank | Description |
|------|--|
| 1 | Involvement/sign off in CRP (Credit Review Point) and NPI (New Product Innovations) process. |
| 2 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. |
| 3 | Fraud Coordinator should be assigned to coordinate between Fraud Risk Manager and ISM. Moreover, regular meeting between these two groups should be arranged to ensure open communication and close gaps. |
| 4 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. |
| 5 | Fraud analyst should analyse fraud losses and review rule sets in fraud detection tools on an ongoing basis. |
| 6 | Formalised fraud policy and procedure should be developed. |
| 7 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. |
| 8 | Well promoted whistle blower program should be one of channels to report fraud case at anytime. Moreover, a case management process to deal with the reported issues should be developed. |
| 9 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. |
| 10 | Formalised write-off policy and procedure should be in place. |
| 11 | 100% review of high risk application or accounts should be conducted. For example, - 3PD or 2PD with no customer contact - Accounts that are potentially "Skip" accounts < 210 days on book - Accounts where mail has been returned from the outset of the account opening. |
| 12 | Data leakage from both paper-based and electronic-based should be controlled. |
| 13 | Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit. |
| 14 | Conducting the review by Internal Audit or independent 3 rd party should be in place. |
| 15 | Centrally located underwriting with documented check list of loans should be in place. |
| 16 | Code of conduct should include clear definition of fraud. |
| 17 | Fraud prevention awareness should be raised and communicated regularly in the management level. |
| 18 | Bad debt written off that is collected from customers in later period should be controlled. |

h) Fraud technology

The abilities of fraud prevention/detection technology are one of the important considerations. It is strongly recommended that advanced data analytical tools being deployed should be able to detect and identify anomalies or suspicious activities,

To enable effective investigation, case management tool with workflow capability should be implemented. In addition, banks should consider other system's abilities, for example, the compatibility with existing core banking system, processing and response time, combating both external and internal fraud, the use of data mining to detect unknown patterns, designing and generating a report template, detecting the similarity of names and addresses etc.

The table below presents the minimum standards recommendation for merchant.

| Rank | Description |
|------|--|
| 1 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. |
| 2 | Banks should implement case management tool with workflow capability. |
| 3 | Fraud technology should be compatible with existing core banking system. |
| 4 | Fraud detection solution should process efficiently and respond back within targeted period. |
| 5 | Fraud technology should be deployed to combat external fraud. |
| 6 | Fraud technology should be deployed to combat internal fraud. |
| 7 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week. |
| 8 | Banks should implement pre-built software specifically for fraud detection technology. |
| 9 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. |
| 10 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. |
| 11 | False positives created from the current technology should be reduced due to poor data quality. By definition, the false positives are transactions that fraud detection tool flags as suspicious but they are not actually fraudulent. |
| 12 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. |
| 13 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. |

Practice Recommendation

a) Know your customer (KYC)

Staff at the point of sales should be able to identify and give any signal once a credit card has been applied for by an unreliable person. This signal will notify and alert the underwriter to strictly validate the background of the applicants.

| Rank | Description |
|------|---|
| 1 | Use of subjective negative codes from point of sale merchants/ intermediary |
| 2 | Validated address/phone number through public databases |
| 3 | Approved methodology for High Risk designation using historical data and current fraud trends |
| 4 | Remote Channel - Internet Apps : Ability to identify high risk applications using relevant session data (i.e. geo-location data/ IP address or other PC device ID) |

| Rank | Description |
|------|---|
| 5 | Install Fraud Scorecard where sufficient data available |
| 6 | No 2 nd deal to be approved before 1 st loan payment cleared. |
| 7 | Approved policy limiting no. of loans to same family/same address |

b) Know your intermediaries (KYI)

Bank should consistently check the financial situation of accredited intermediaries to gain some certainty that those intermediaries do not face any financial stress. Otherwise, they may co-ordinate with some customers to defraud the bank. This should be performed at least once a year either by internal or external parties. Bank should pay the intermediary fee after it has received all required documents and also that the credit card has been approved to the customer. Before and after anyone / any party has been accredited as an intermediary, bank should have a site visit to the work location of these parties.

| Rank | Description |
|------|---|
| 1 | Bank holds cash deposit from merchant and is able to claw back this amount in case of merchant fraud |
| 2 | KYI tool installed to identify any unusual and give red flags to relevant people |
| 3 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. |
| 4 | Intermediaries have Public Indemnity Insurance to cover Intermediary fraud |
| 5 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level |
| 6 | Payment to Intermediary after receipt of full documentation |
| 7 | Perform site visitation prior to accreditation of broker |

c) Revolving Fund - Redraw Ability

Under this type of product, bank should implement MasterCard Secure Code or Verified by Visa to ensure that the redraw activities are safely performed. In cases whereby the bank issues shopping cards to any applicant, this card should only be for temporary purposes with short expiration period. Please refer to detail in the table below.

| Rank | Description |
|------|---|
| 1 | Implement MasterCard Secure Code or Verified by Visa |
| 2 | Remote Channel - Brand Domain Protection Anti-phishing take-down ability |
| 3 | Temporary Shopping Cards : Must be issued for a specified short period of time i.e. 2 weeks : Must only be issued for in store new accounts |
| 4 | Process that allows early identification of payments that do not have cleared funds i.e. dishonoured check process |
| 5 | Direct Debit repayments set up from commencement of loan |
| 6 | Chargeback Tracking |

d) Know your staff (KYS)

Not only does the bank have to check background information of potential employees, they should be able to identify staff and related parties' bank account once the bank employs particular staff. This will help the bank to have more monitoring activities to avoid internal fraud from their employees since some staff may transfer bank's customer account into their own account or

related parties' account.

In some circumstances where the banker also acts as sales staff to offer products to the customers, bank should monitor and make some comparison over the staff sales performance to ensure that their staff do not create numerous sales with low credit rating customers. Bank should also have a particular report to summarise sales for each staff comparing with non operating customers who are proposed by particular staff.

| Rank | Description |
|------|--|
| 1 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should neither maintain their own (customer) account nor a related party's (customer) account. |
| 2 | Ability to identify staff accounts. |
| 3 | Installation of KYS tool - Intellinx/Footprint |
| 4 | Review process for Staff receiving Sales bonus's - review at both Branch/Merchant and individual staff member level |
| 5 | Can employees access into other banks beyond the bank they are working for? |

e) Third party payments / disbursements

Normally, bank is responsible to pay directly to the seller of the property. Bank should ensure that there is no process allowing any payments made to the borrowers. In addition, the bank should receive all required documents before any money is paid out. An additional importance for any disbursements to the borrowers is to ensure that the recipient of the money is not their own staff's or related party's bank account.

In case of any changes to detail of recipient's bank accounts, banker should check and confirm with the recipient for any updated information to ensure that bank makes disbursements to the right party.

| Rank | Description |
|------|--|
| 1 | Review triggers for \$ payments by dealer / supplier type |
| 2 | Payments to dealers / suppliers against full documentation |
| 3 | Match bank payment details to staff bank accounts |
| 4 | Ability to identify multiple dealer / supplier payment details to same bank account |
| 5 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier |

f) Reporting

For merchant, it is recommended that banks should develop reports relevant to fraud prevention/detection. They should include Fraud Prevention/Detection/ Losses, quarterly reports, and monthly reports. In practice, recommendation is for all of these reports to be considered.

| Rank | Description |
|------|---|
| 1 | Fraud Prevention/Detection/ Losses broken down by portfolio. |
| 2 | Quarterly reporting that covers new global standards, such as fraud to W/O (Write-off), Fraud to NI, or reporting that is tailored to most relevant metric that would show impact to bottom line for country portfolio. |
| 3 | Fraud Prevention/Detection/ Losses analysed and reported by process weakness. |
| 4 | Monthly reports relevant to fraud trends and comments. |
| 5 | Fraud Prevention/Detection/ Losses broken down by fraud type. |
| 6 | Variance analysis and development of control charts. |

g) Operational efficiency

To increase the operational efficiency, banks should consider the fraud detection methods, monitoring customer complaints, fraud alert process, fraud training program, Fraud Council meeting, reward/incentive program, employee's KPI, etc.

Listed below are common practice recommendations.

| Rank | Description |
|------|---|
| 1 | Fraud detection methods should be tailored to needs of individual portfolio. |
| 2 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. |
| 3 | The procedure for fraud alert process across industry peers should be developed. |
| 4 | Fraud training programs should be conducted for Underwriting staff. |
| 5 | Random checks for underwriting process compliance should be performed. |
| 6 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. |
| 7 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. |
| 8 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. |
| 9 | Fraud awareness training should be provided to employees at least every six months. |
| 10 | Employee's KPIs should be established based on the risk associated with their tasks. |

h) Fraud technology

In terms of technology, some of practice recommendations are about the ability to interface between fraud detection technology and other legacy systems, interface with the Anti-Money Laundering (AML) application, extract suspicious transactions for further investigation, screen data with internal watch lists, etc.

There are a number of important considerations for merchant as follows.

| Rank | Description |
|------|---|
| 1 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. |
| 2 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. |
| 3 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. |
| 4 | Banks should update fraud detection techniques regularly, at least once a month. |
| 5 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. |
| 6 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. |
| 7 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. |
| 8 | Banks should develop common data model to capture data from different |

| Rank | Description |
|------|--|
| | sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. |
| 9 | Fraud technology should allow banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. |
| 10 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. |
| 11 | Social Network Analysis should be used to detect and visualise fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. |
| 12 | The pre-built data model should be created for the bank's existing systems. |
| 13 | Fraud technology should have the ability to prioritise each fraud case according to risk scores and notify suspicious activities to the management. |
| 14 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. |
| 15 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. |
| 16 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyse and alert the responsible people in case of any unusual transactions or suspicious behaviour. |
| 17 | Fraud technology should be supported by a vendor representative/service provider that exists in Thailand to provide faster and efficient support. |
| 18 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. |

4. Mortgage loan

The population of Thailand is increasing and with that, lifestyle changes are noticeable; people tend to purchase their own property instead of staying with their parents. However, not everyone can afford to buy his/her own property in lump-sum payment. Bank provides alternative way to assist people to buy their own property. This may be called "Mortgage loan" or "Housing loan". Normally this type of loan is secured by all types of property while the interest rate is charged by reflecting the lender's risk, such as source of fund, occupation, etc.

This loan is considered as one of bank's major portfolios. Though fraud risk from mortgage loan is not as critical as other products, banks still should comply with the following minimum standard recommendations in order to mitigate their fraud risks.

Minimum Standards Recommendation

We categorise each recommendation according to the relevant activities operated by the bank as follows:

a) Know your customer (KYC)

In general, banks should have reasonable background knowledge over their target customers before giving out any loan to them. As a result, bank should have a policy to verify the background information of each loan applicant in order to ensure their existence and authenticity. The verification process should be performed by using public database. For example, banker should check whether or not the applicant's telephone number is registered or the provided contact address is real. In addition, bank should have available database which has the information for all potential blacklists such as anti-money laundering, default customers, fraudulent customers, etc.

Moreover, the underwriting policy should comply with risk management procedures to mitigate high risk accounts. The update of high value fraud should be done in the bank database frequently and also that the relevant parties receive the alert information on any updated high value fraud on a timely basis.

| Rank | Description |
|------|--|
| 1 | Underwriting Policy noting: - ID verification procedure, - employment/income verification procedure - address verification procedure - weighted Bureau data (If applicable) |
| 2 | Underwriting Policy noting procedures for high risk accounts: (As defined by risk management) |
| 3 | High value Fraud Alerts to other portfolios at country level |
| 4 | Fraud Blacklisting Capability |
| 5 | Conforms to CRP (Credit Review Point) as signed off |
| 6 | Underwriting Policy that has different requirements for : - Self-employed applicants - Self-certified applicants (Stated income Applicants) - commercial properties (If applicable) |
| 7 | De-Duplicate previous application process (approved and declined apps) |
| 8 | Policy around Foreign Nationals |
| 9 | Policy and process whereby address/phone numbers can be validated through public databases |
| 10 | If business operates via Intermediaries (correspondents, brokers) then it must have documented process to audit the KYC verification conducted by the intermediary |

b) Know your intermediaries (KYI)

Sometimes banks may need third party to act as their intermediary to assist in finding potential customers. However, bank should be able to ensure that those intermediaries perform their jobs transparently since they are the primary filter for particular loan applicants. Before appointing any party as the bank's intermediary, bank should check all possible information such as company background, financial position, credit rating, etc. Bank should perform a site visit prior and after accreditation of particular intermediaries.

Moreover, bank should have a reliable database that includes all the information of intermediary blacklist and also that bank should appoint some staff to continually monitor the performance of the appointed intermediaries. This will help them ensure that loans given out to the customers, proposed by particular intermediaries, are the operating loans.

| Rank | Description |
|------|---|
| 1 | Robust Intermediary accreditation process – See Compliance guidelines |
| 2 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all broker groups. Checks that if intermediary has been terminated then terminated across all brokers. |
| 3 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level |
| 4 | Segment and Monitor by underwriter and/or Sales rep |
| 5 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. |
| 6 | Intermediaries have Public Indemnity Insurance to cover Intermediary fraud |
| 7 | Perform site visitation prior to accreditation of broker |
| 8 | Broker Fraud - Included in contract with broker is reimbursement for Internal Fraud. Or encourage broker to take out insurance for internal fraud. |

c) Asset verification

In case of secured loan, bank should review a title deed of any property that the borrower would like to mortgage with the bank to ensure that this title deed belongs to the customer before being mortgaged. Bank should also check the position of lien over the mortgaged assets.

Not only the title of the mortgaged assets but the current market value of this asset should be appraised by reliable appraiser either in-house or external party. For the external appraiser, bank should perform a reasonable background check prior to accreditation of any appraisers to ensure that those appraisers are independent and reliable.

| Rank | Description |
|------|--|
| 1 | Title deed review immediately before signing the loan agreement |
| 2 | Alternative valuation checking: - In house appraiser - Internal Valuation Database - External valuation Database |
| 3 | Independent valuation process generated. (Valuation not ordered by Sales staff or customer) OR If Broker orders and supply's valuation then business must conduct detailed review of 100% of all valuation |
| 4 | Drive By process on high risk properties |
| 5 | Approved accreditation process for Appraisers |
| 6 | Process that includes inside/outside photos in valuation process |

| Rank | Description |
|------|--|
| 7 | Prevent/monitor for sale of asset by customer - Can lien be removed? |
| 8 | Create Valuation Panel comprising selected professionally qualified staff that have adequate PI (Professional Indemnity) insurance and strong financial position |
| 9 | Monthly quality control on sample of properties. |
| 10 | Appropriate Property Insurance coverage. Annual check that Insurance is still current. |

d) Know your staff (KYS)

One of the key operating successes of bank is hiring the right person. Human Resources department is a first screen over bank applicants. Thus, they should have effective policies and procedures before employing their staff. One of the recommended HR guidance is to check the applicant's profile including financial status to ensure that the applicant does not have any financial stress. Employment approval process and applicant's profile reviewing process should be segregated from each other.

Bank should launch an effective whistle blowing practices within the organisation and also give their employees with high confidences that nothing would be disclosed publicly. This policy should be communicated widely in the organisation and update on a timely basis for at least once a year.

| Rank | Description |
|------|--|
| 1 | Background Employment Screening (See HR guidelines & Also check financial status of employees on an annual basis to ensure they are not in a financial pressure) |
| 2 | Separate approval process and review process for Staff accounts |
| 3 | Exception Reporting identifying accounts that are High Risk for internal fraud |

e) Third party payments / disbursements

Normally, bank is responsible to pay directly to the seller of the property. Bank should ensure that there is no process allowing any payments made to the borrowers. In addition, the bank should receive all required documents before any money is given out. Another importance for any disbursements to the borrowers is to ensure that the recipient of money is not their own staff's or related party's bank account.

In case of any changes to detail of recipient's bank accounts, banker should check and confirm with the recipient for any updated information to ensure that bank makes disbursements to the right party.

| Rank | Description |
|------|---|
| 1 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid |
| 2 | Payments to dealers / suppliers against full documentation |
| 3 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |
| 4 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns |
| 5 | Review triggers for \$ payments by dealer / supplier type |
| 6 | Match bank payment details to staff bank accounts |
| 7 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier |

f) Reporting

The most important standard for mortgage loan is preparing prevention/detection/losses report broken down by portfolio. In some circumstances, banks should report fraud cases to the bank's headquarters. Other essential reports should also be produced including summary report of fraud investigation, fraud type analysis, fraud prevention/detection/losses. Furthermore, key underwriting and business transaction should be collected and used for fraud investigation and risk analysis process.

The following table shows the details of the minimum standard recommendations.

| Rank | Description |
|------|--|
| 1 | Fraud Prevention/Detection/ Losses broken down by portfolio. |
| 2 | Fraud cases reported to the bank's headquarters. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. |
| 3 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. |
| 4 | Key underwriting and transaction data tracked and used for fraud analysis. |
| 5 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. |
| 6 | Fraud Prevention/Detection/Losses broken down by fraud type. |
| 7 | Fraud Prevention/Detection/Losses analyzed and reported by process weakness. |

g) Operational efficiency

For mortgage loan, it is highly recommended that data losses from any form of information including paper-based and electronic-based should be prevented. Additionally, some of other important standards include a periodic review by Internal Audit or independent third party, the responsibilities assigned to Risk Management function, Fraud Analyst, and personnel who maintain fraud detection tools, policies and procedures relevant to improper/unusual payment to the government, fraud prevention/detection, bad debt write-off, review of high risk application or customer accounts, the awareness of fraud prevention/detection, etc.

Listed below are the minimum standards that should be complied with.

| Rank | Description |
|------|---|
| 1 | Data leakage from both paper-based and electronic-based should be controlled. |
| 2 | Conducting the review by Internal Audit or independent third party should be in place. |
| 3 | Risk Management Function should take responsibility for fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. |
| 4 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. |
| 5 | Formalized fraud policy and procedure should be developed. |
| 6 | Formalized write-off policy and procedure should be in place. |
| 7 | Fraud training programs should be conducted for Underwriting staff. |
| 8 | Fraud analyst should analyse fraud losses and review rule sets in fraud detection tools on an ongoing basis. |
| 9 | 100% review of high risk application or accounts should be conducted. For |

| Rank | Description |
|------|--|
| | example, - 3PD or 2PD with no customer contact - Accounts that are potentially "Skip" accounts < 210 days on book - Accounts where mail has been returned from the outset of the account opening. |
| 10 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. |
| 11 | Random checks for underwriting process compliance should be performed. |
| 12 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. |

h) Fraud technology

The ability to prioritise each fraud case according to risk scores and notify suspicious activities to the management is the first priority when implementing fraud technology. In addition, there are a number of standards that banks should follow. Some of them are the ability to be compatible with existing core banking system, calculate risk scores for any potential fraud concerns, combat internal and external fraud, interface with other legacy systems, detect fraudulent transactions in real-time and 24 hours a day, 7 days a week, interface directly with the Anti-Money Laundering (AML) application, identify anomalies or suspicious activities, etc. The use of social network analysis is another important approach for fraud prevention and detection.

Details are shown in the following table for all minimum standard recommendations.

| Rank | Description |
|------|---|
| 1 | Fraud technology should have the ability to prioritise each fraud case according to risk scores and notify suspicious activities to the management. |
| 2 | Fraud technology should be compatible with existing core banking system. |
| 3 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. |
| 4 | Fraud technology should be deployed to combat internal fraud. |
| 5 | Social Network Analysis should be used to detect and visualise fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. |
| 6 | As a bank has multiple legacy applications that prevent the fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. |
| 7 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. |
| 8 | Fraud technology should be deployed to combat external fraud. |
| 9 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, seven days a week. |
| 10 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. |
| 11 | Banks should implement pre-built software specifically for fraud detection technology. |
| 12 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. |
| 13 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. |
| 14 | Banks should implement case management tool with workflow capability. |
| 15 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. |

| Rank | Description |
|------|--|
| 16 | Fraud technology should enable the fraud team or IT staff to maintain the configurations/rules. |
| 17 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. |

In addition to minimum standard recommendations, bank should apply some of the following common practice recommendations that are best suited to the organisation's operation.

Practice Recommendation

a) Know your customer (KYC)

Bank should establish its own central underwriting team. This team should not have any opportunity to meet the customers or asked to sell bank's products to any potential customers. Sales and underwriting teams should be obviously segregated from each other to avoid any conflict of interest or independent issue.

Bank should have a database that can identify any high risk profile for some types of customers. This profile will be used by underwriters for credit analysis and also fraud potential for specific profile. Bank should have any system to identify or issue exception report in some cases. For example, an exception report for non-operating loans which were approval by the same underwriter.

| Rank | Description |
|------|---|
| 1 | Ability to Limit No. of loans to same name/address |
| 2 | Centrally located underwriting, segregation between Sales and Underwriting Teams |
| 3 | Utilise high risk profiles for additional targeting as required |
| 4 | Install Fraud Scorecard where sufficient data are available |
| 5 | Install KYC tool where sufficient applications are available |
| 6 | Ability for system to capture underwriting data (create relevant Exception reports as required) |
| 7 | Face to Face meeting with customer (signing phase) for Mortgage |

b) Know your intermediaries (KYI)

Intermediary operating performance should be evaluated from time to time to ensure that the customers proposed by the particular intermediary are operating customers. Furthermore, bank should check the financial situation of accredited intermediaries on a timely basis, for example, once a year, to make sure that those intermediaries are not under financial pressure. Otherwise, they may co-ordinate with some customers to defraud the bank.

| Rank | Description |
|------|---|
| 1 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. |
| 2 | Monthly grading process must provide for termination of intermediaries depending on performance. If intermediary offers a range of products then intermediary should be terminated across all products. |
| 3 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. |
| 4 | Reward scheme for Intermediaries who detect fraud |

| Rank | Description |
|------|---|
| 5 | Monthly Reporting on Intermediaries using performance triggers as review point (i.e. Approval Rates, Write Offs (W/Os), 3PDs(Payment Delinquent /Default), Sales Volume, TTY(Time To Yes) , Delinquency Rates, Fraud Losses, etc. |
| 6 | KYI tool installed - i.e. Actimize |

c) Asset verification

In case of non-performing loans, bank must ensure that they can seize the mortgaged property and sell it in the market for some financial recovery. As a result, title deed of any mortgaged property should be verified before signing a loan agreement with the borrower. Furthermore, the process of seizing any property should be short and clear to avoid potential losses.

Secondary valuation over specific property should be performed in case of any variance occurs for at least 15 percent from the available database. If in-house appraiser is in-charge of the specific property, bank should ask the valuation service from the external appraiser for alternative decision.

| Rank | Description |
|------|---|
| 1 | Process that allows for foreclosure and recovery of monies |
| 2 | Process that allows for the clear establishment of charge against the title to the asset within a short time frame |
| 3 | Secondary checking through listed valuation databases – Investigations commenced if +/- 15% variation |
| 4 | Control that protects all persons who have an interest in the asset have knowledge over any sale or draw down against the asset e.g. 'Speak with' program where independent contact is made with all parties that have a financial interest in the loan |
| 5 | Additional controls or mitigating processes if portfolio does not have Title, Fraud or Mortgage Insurance |
| 6 | Fraud Recoveries process in addition to normal recoveries |
| 7 | Semi-annual lien registration checking |
| 8 | If Mortgage portfolio and there is the ability to re-draw then see Minimum control Guideline - Revolve fraud |

d) Revolving Fund - Redraw Ability

Under mortgage loan, there are few chances of account takeover since the loan will be paid directly to the seller of property. Hence, below activities are recommended as practice guide for some circumstances. In such case, exception report should be prepared to identify any high risk transactions or unusual activities.

| Rank | Description |
|------|---|
| 1 | Account Takeover Controls - Documented process for High Risk Transactions |
| 2 | Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product |
| 3 | Account Takeover Controls: Ability to identify high risk transactions and create Exception Report |
| 4 | Transaction Fraud Tool - e.g. Aristion (where re-draw facility completed through Credit Card transaction) |

e) Know your staff (KYS)

Not only has the bank to check background information of potential employees, they should be able to identify staff and related parties' bank account once the bank employs particular staff. This will help the bank to have more monitoring activities to avoid internal fraud from their employees since some staff may transfer bank's customer account into their own account or related parties' account.

In some circumstances that banker also acts as sales staff to offer some product to the customers. Bank should monitor and make some comparison over the staff sales performance to ensure that their staffs do not create many sales with low profile customers. Bank should also have a particular report to summarise sales for each staff comparing with non operating customers who are proposed by particular staff.

| Rank | Description |
|------|---|
| 1 | ISM (Investigation & Security Manager) Capability with Feedback loop to Prevention |
| 2 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should neither maintain their own (customer) account, nor a related parties (customer) account. |
| 3 | Can employees access into other banks beyond the bank they are working for? |
| 4 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually |
| 5 | Ability to identify staff accounts. Monitor staff and related party accounts for internal fraud |
| 6 | Installation of KYS tool - e.g. Intellinx/Footprint |
| 7 | Review process for Staff receiving Sales bonuses |

f) Third party payments / disbursements

Normally, bank is responsible to pay directly to the seller of the property. Bank should ensure that there is no process allowing any payments made to the borrowers. In addition, the bank should receive all required documents before any money is given out. Another importance for any disbursements to the borrowers is to ensure that the recipient of money is not their own staff's or related parties' bank accounts.

In case of any changes to detail of recipient's bank accounts, banker should check and confirm with the recipient for any updated information to ensure that bank makes disbursements to the right party.

| Rank | Description |
|------|---|
| 1 | Ability to identify multiple dealer / supplier payment details to same bank account |

g) Reporting

There are several reports that banks should prepare and monitor to prevent and detect fraudulent activities. Some of them are in relation to Fraud Prevention/Detection/ Losses, Fraud case management report, monthly reports, etc.

The practice recommendations are presented in the table below.

| Rank | Description |
|------|---|
| 1 | Fraud Prevention/Detection/ Losses broken down by portfolio. |
| 2 | Fraud case management report including the progression and follow-up of fraud investigation, and exchange of fraud information/news. In addition, fraud cases should be reported to the Bank of Thailand. |

| Rank | Description |
|------|---|
| 3 | Exception reports for high risk transactions. |
| 4 | Monthly reporting: Gross/Net Fraud; Fraud to Sales; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O (Write-off) no payments, Skip/Trace <90MOB (month on book); Fraud savings, Investigation, Recoveries. |
| 5 | Monthly reports relevant to fraud trends and comments. |
| 6 | Monthly reports including follow-up action Items. |
| 7 | Variance analysis and development of control charts. |

h) Operational efficiency

For mortgage loan, banks should consider the fraud case management, channels for reporting fraud cases, fraud prevention awareness, collection of debt after write-off, code of conduct, employees' KPIs, etc.

The following table shows all of the common practice recommendations.

| Rank | Description |
|------|---|
| 1 | Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit. |
| 2 | Well promoted whistle blower program should be one of channels to report fraud case at anytime. Moreover, a case management process to deal with the reported issues should be developed. |
| 3 | Fraud prevention awareness should be raised and communicated regularly in the management level. |
| 4 | Fraud Coordinator should ensure that 'Close the loop' process is finalised. |
| 5 | Bad debt written off that is collected from customers in later period should be controlled. |
| 6 | Code of conduct should include clear definition of fraud. |
| 7 | The members of the Fraud team should consist of staff from Operations and Analytics. |
| 8 | Employee's KPIs should be established based on the risk associated with their tasks. |
| 9 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. |
| 10 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. |
| 11 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. |
| 12 | The procedure for fraud alert process across industry peers should be developed. |
| 13 | Fraud detection methods should be tailored to needs of individual portfolio. |
| 14 | Fraud awareness training should be provided to employees at least every six months. |
| 15 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. |

j) Fraud technology

In general, fraud technology should have ability to design and generate a report template, integrate transactions from different sources/systems, reduce false positives, detect the similarity

of names and addresses, generate multiple views of reports, process efficiently, etc. In addition, the solution should be supported by a vendor representative in Thailand.

Banks should consider the practice recommendations in table below.

| Rank | Description |
|------|--|
| 1 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. |
| 2 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyse and alert the responsible people in case of any unusual transactions or suspicious behaviour. |
| 3 | Fraud technology should allow banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. |
| 4 | False positives created from the current technology should be reduced due to poor data quality. By definition, the false positives are transactions that fraud detection tool flags as suspicious but they are not actually fraudulent. |
| 5 | Fraud technology should be supported by a vendor representative/service provider that exists in Thailand to provide faster and efficient support. |
| 6 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. |
| 7 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. |
| 8 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. |
| 9 | Fraud detection solution should process efficiently and respond back within targeted period. |
| 10 | Banks should update fraud detection techniques regularly at least once a month. |
| 11 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. |
| 12 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. |
| 13 | The pre-built data model should be created for the bank's existing systems. |
| 14 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. |

5. Personal Loan

A personal loan is the loan granted for personal, family, or household purpose, as different from commercial use. This loan is generally obtained by the borrowers to pay for education, purchase of computer, washing machine, air conditioner, etc. The borrowers make a payment of principal and interest through fixed instalment and fixed term. As usually being unsecured loan, there is no need for collateral but, in some cases, a guarantor or co-signer might be required by the lender. In addition, such loan is offered on the basis of the customer's ability to pay and credit history.

Below are the minimum standard recommendations initiated for personal loans in order to mitigate fraud risks that might arise.

Minimum Standard Recommendation

We categorise each recommendation according to the relevant activities operated by the bank as follows:

a) Know your customer (KYC)

In general, banks should have reasonable background knowledge over their customers before entering into any loan agreements. As a result, bank should have a policy to verify the background information of each loan applicant in order to ensure their existence and authenticity. The verification process should be performed by using public database. For example, banker should check whether the applicant's telephone number is registered or the provided contact address is real. In addition, bank should have available database which has the information for all potential blacklists and also high profile target such as anti-money laundering, default customers, fraudulent customers, etc. The high profile target customers may be classified by age, occupation, location, etc.

Moreover, the underwriting policy should comply with risk management procedures to mitigate high risk accounts. The update of high value fraud should be done in the bank database frequently and also that the relevant parties get the alert information on any updated high value fraud on a timely basis. The organisation system should be able to identify and summarise any applications that have been previously applied for both approved and denied applications.

| Rank | Description |
|------|--|
| 1 | Underwriting Policy noting : ID verification procedure, : employment/income verification procedure : address verification procedure : phone verification procedure : weighted bureau data |
| 2 | Centrally located underwriting, segregation between Sales and Underwriting Teams |
| 3 | Conforms to CRP (Credit Review Point) as signed off |
| 4 | Fraud Blacklisting Capability |
| 5 | Validated address/phone number through public databases |
| 6 | Utilise high risk profiles for additional targeting |
| 7 | If business operates via Intermediaries then must have documented process to validate controls conducted by intermediary |
| 8 | High value Fraud alerts to other portfolios at country level |
| 9 | Install KYC tool where sufficient applications available |
| 10 | Policy around Foreign Nationals |
| 11 | De-Duplicate previous application process (approved and declined apps) |
| 12 | Ability for system to capture underwriting data (create relevant Exception reports as required) |

b) Know your intermediaries (KYI)

Sometimes banks may need a third party to act as their intermediary to assist in finding potential customers. However, bank should be able to ensure that those intermediaries perform their jobs transparently since they are the primary filter for particular loan applicants. Before appointing any party as the bank's intermediary, bank should check all possible information such as company background, financial position, credit rating, etc. Bank should perform a site visit prior and after accreditation of particular intermediaries.

Moreover, bank should have a reliable database which includes all the information of intermediary blacklist and also that bank should appoint some staff to continually monitor the performance of the appointed intermediaries. This will help them ensure that loans given out to the customers, proposed by particular intermediaries, are the operating loans. Bank should also review the intermediary performance at least once a month to monitor the performance of those intermediaries.

| Rank | Description |
|------|--|
| 1 | Segment and Monitor by underwriter and/or Sales rep |
| 2 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups. Checks that if Intermediary terminated then terminated across all intermediary listings. |
| 3 | Robust Intermediary accreditation process – See Compliance guidelines |
| 4 | Intermediary Fraud - Included in contract with Intermediary is reimbursement for Internal Fraud. Or encourage Intermediary to take out insurance for internal fraud. |
| 5 | Monthly Reporting on Intermediaries using performance triggers as review point i.e. Approval rate, W/O's (Write Offs), 3PD (Payment Default/Delinquent), Sales volume, delinquency, TTY 9Time To Yes), Fraud Loss. |

c) Asset verification

Bank should employ preventive and monitoring procedures to ensure that the assets which are used as the guarantees have not been sold or transferred to third party without any acknowledgement or consent from the bank.

| Rank | Description |
|------|--|
| 1 | Provide Plan for ability to identify 'at risk' accounts where asset may be on sold without finalising settlement |
| 2 | Prevent/monitor for forward sale of asset by customer |
| 3 | Clearly defined asset type that will be eligible for loans, Caps on extra's as defined by policy |
| 4 | Independent Asset validation process - valuation checked through independent database |

d) Revolving Fund - Redraw Ability

Bank normally would not have a critical concern with the account takeover issue for this type of loan. However, they should still have some processes to ensure that there is no such case occurring at any time.

| Rank | Description |
|------|--|
| 1 | Transaction Fraud Tool - e.g. Arision (where redraw facility completed is through Credit Card transaction) |

| Rank | Description |
|------|---|
| 2 | Account Takeover Controls - Documented process for High Risk Transactions |

e) Know your staff (KYS)

Bank should establish a clear HR guideline in hiring their new employees. They should check all possible information to ensure that the applicant is the right person to be hired. In addition, bank should segregate duties between application approval personnel and reviewing personnel to avoid any conflict of interest.

Moreover, bank should launch an effective whistle blowing practices within the organisation and also give their employees strict confidence that nothing will be disclosed once the employees have reported any unusual activities. This policy should be communicated widely throughout the organisation and updated on a timely basis.

| Rank | Description |
|------|--|
| 1 | IT Security create profiles where system access is dictated by role |
| 2 | Background Employment Screening (See HR guidelines) (Also check financial status of employees on an annual basis to ensure they are not in a financial pressure) |
| 3 | Separate approval process and review process for Staff accounts |
| 4 | ISM (Investigation & Security Manager) Capability with Feedback loop to Prevention |

f) Third party payments / disbursements

Bank should make should that the applied and approved personal loan has been paid directly to the supplier / or dealer once all required documents have been received.

| Rank | Description |
|------|---|
| 1 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns |
| 2 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid |
| 3 | Payments to dealers / suppliers against full documentation |
| 4 | Review triggers for \$ payments by dealer / supplier type |

g) Reporting

As a minimum standard, it is most essential for banks to report fraud cases that impact significantly on business to the bank's headquarters. Other important reports used for personal loan include, for example, fraud prevention/detection/losses, quarterly and monthly reports, fraud case management report, summary report of fraud investigation, etc.

The following table presents the details of minimum standard recommendations.

| Rank | Description |
|------|---|
| 1 | Fraud cases reported to the bank's headquarters. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. |
| 2 | Fraud Prevention/Detection/ Losses broken down by fraud type. |
| 3 | Quarterly reporting that covers new global standards, for example, fraud to W/O (Write-off), Fraud to NI, Reporting that is tailored to most relevant metric that would show impact to bottom line for country portfolio. |
| 4 | Fraud case management report including the progression and follow-up of |

| Rank | Description |
|------|--|
| | fraud investigation, and exchange of fraud information/news. In addition, fraud cases should be reported to the Bank of Thailand. |
| 5 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. |
| 6 | Fraud Prevention/Detection/ Losses analysed and reported by process weakness. |
| 7 | Monthly reports relevant to fraud trends and comments. |

h) Operational efficiency

Regarding to operational efficiency of personal loan, it is highly recommended that Fraud Manager should have the awareness of fraud prevention/detection as well as regularly update the skills for new fraud.

As a minimum standard, banks should also implement critical controls which include data leakage prevention, central check list for loan approval, development of policies and procedures relevant to bad debt write-off, improper/unusual payment to the government as well as fraud prevention/detection, fraud prevention awareness training, fraud alert process across portfolio, establishing channels to report fraud cases, review of high risk application or customer accounts, regular Fraud Council meeting, etc.

All of the minimum standards are shown in the table below.

| Rank | Description |
|------|---|
| 1 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. |
| 2 | Data leakage from both paper-based and electronic-based sources should be controlled. |
| 3 | Centrally located underwriting with documented check list of loans should be in place. |
| 4 | Formalised write-off policy and procedure should be in place. |
| 5 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. |
| 6 | Random checks for underwriting process compliance should be performed. |
| 7 | Fraud prevention awareness should be raised and communicated regularly in the management level. |
| 8 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. |
| 9 | Fraud training programs should be conducted for Underwriting staff. |
| 10 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. |
| 11 | Well promoted whistle blower program should be one of channels to report fraud case at any time. Moreover, a case management process to deal with the reported issues should be developed. |
| 12 | Fraud analyst should analyse fraud losses and review rule sets in fraud detection tools on an ongoing basis. |
| 13 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. |
| 14 | 100% review of high risk application or accounts should be conducted. For example, - 3PD or 2PD with no customer contact - Accounts that are potentially "Skip" accounts < 210 days on book |

| Rank | Description |
|------|---|
| | - Accounts where mail has been returned from the outset of the account opening. |
| 15 | Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit. |
| 16 | Formalised fraud policy and procedure should be developed. |
| 17 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. |
| 18 | Involvement/sign off in CRP (Credit Review Point) and NPI (New Product Innovations) process. |

i) Fraud technology

For personal loan, the ability of fraud prevention/detection solution to combat fraud from individuals or groups of individual in the organisation is recognised as the first priority. In addition to this feature, fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application, detect fraudulent transactions in real-time and 24 hours a day, seven days a week, combat external fraud, be compatible with core banking system, enable users to design and generate a report template, enable the Fraud team or IT staff to maintain the configurations/rules, etc. Moreover, case management tool with workflow capability should be considered.

Listed below are the minimum standards that should be complied with.

| Rank | Description |
|------|--|
| 1 | Fraud technology should be deployed to combat internal fraud. |
| 2 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. |
| 3 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, seven days a week. |
| 4 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. |
| 5 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. |
| 6 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. |
| 7 | Banks should implement case management tool with workflow capability. |
| 8 | Banks should implement pre-built software specifically for fraud detection technology. |
| 9 | Fraud technology should be deployed to combat external fraud. |
| 10 | Fraud technology should be compatible with existing core banking system. |
| 11 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. |
| 12 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. |
| 13 | Fraud technology should have the ability to prioritise each fraud case according to risk scores and notify suspicious activities to the management. |
| 14 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. |
| 15 | Banks should update fraud detection techniques regularly, at least once a |

| Rank | Description |
|------|---|
| | month. |
| 16 | Social Network Analysis should be used to detect and visualise fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. |

Practice Recommendation

a) Know your customer (KYC)

A clear methodology on approving the applied personal loans for high risk designation should be launched and strictly followed. This methodology may be developed from historical data and updated from time to time once there are any new cases. Additionally, this policy should limit no. of loans applied by the same family members or the same address.

| Rank | Description |
|------|--|
| 1 | Approved methodology for high risk designation using historical data and current fraud trends |
| 2 | Install Fraud Scorecard where sufficient data are available |
| 3 | No second deal to be approved before first loan payment is cleared. |
| 4 | Remote Channel - Internet Apps - Capture relevant session data (i.e. geo-location data/ IP address or other PC device ID) identify 'high risk accounts using these variables |
| 5 | Use of subjective negative codes from point of sale merchants |
| 6 | Approved policy limiting no. of loans to same family/same address |

b) Know your intermediaries (KYI)

If intermediary is used to find customers for personal loans, bank should have some proper contract and monitoring process over the performance of that intermediary to ensure that they perform their jobs transparently and efficiently. Bank should pay the intermediary fee after it has received all required documents and also that the personal loan has been approved to the applicant.

Bank should consistently check the financial situation of accredited intermediaries to gain some certainty that those intermediaries do not face any financial stress. Otherwise, they may coordinate with some customers to defraud the bank. This should be performed at least once a year either by internal or external parties.

| Rank | Description |
|------|---|
| 1 | Monthly grading process must provide for closure of intermediaries depending on Performance |
| 2 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. |
| 3 | Perform site visitation prior to accreditation of broker |
| 4 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level |
| 5 | Intermediaries have Personal Indemnity / Fidelity Insurance to cover Intermediary fraud |
| 6 | KYI tool installed - i.e. Actimize |
| 7 | Payment to Intermediary after receipt of full documentation |
| 8 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. |

| Rank | Description |
|------|---|
| 9 | Bank holds cash deposit from Intermediary and is able to claw back this amount in case of merchant fraud |
| 10 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. |

c) Asset verification

Personal loan is normally given to bank's customers as a secured loan. There will be some assets used to pledge with the bank as a guarantee. Therefore, bank should set a clear policy regarding the asset valuation and type of acceptable assets. Before signing a loan agreement, banker should ensure that title deed of the assets can be claimed by the bank once the customer can no longer pay the outstanding balance. Further detail is provided in below table.

| Rank | Description |
|------|---|
| 1 | If asset is not registered prior to disbursement then audit to ensure asset is secured within prescribed time frame |
| 2 | Process that allows clear title registration over asset within a set time frame |

d) Revolving Fund - Redraw Ability

Bank should be able to identify any accounts that are taken over by other people. This will help mitigating risk of default the loan payment.

| Rank | Description |
|------|---|
| 1 | Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product |
| 2 | Account Takeover Controls: Ability to identify high risk transactions and create Exception Report |

e) Know your staff (KYS)

Not only does the bank have to check background information of potential employees, they should be able to identify staff and related parties' bank account once the bank employs particular staff. This will help the bank to have more monitoring activities to avoid internal fraud from their employees since some staff may transfer bank's customer account into their own account or related parties' account.

In some circumstances that banker also acts as sales staff to offer some products to the customers. Bank should monitor and make some comparison over the staff sales performance to ensure that their staffs do not create numerous sales with low profile customers. Bank should also have a particular report to summarise sales for each staff comparing them with non operating customers who are proposed by particular staff.

| Rank | Description |
|------|---|
| 1 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually |
| 2 | Can employees access into other banks beyond the bank they are working for? |
| 3 | Monitor monthly approval rates and write offs by individual staff (Sales, U/writing and Collections staff) |
| 4 | Ability to identify staff accounts. Monitor staff accounts for internal fraud |
| 5 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should neither maintain their own (customer) account nor maintain a related parties (customer) account. |

| Rank | Description |
|------|---|
| 6 | Installation of KYS tool - Intellinx/Footprint |
| 7 | Review process for Branches and Staff receiving Sales bonus's - review at both Branch and individual staff member level |

f) Third party payments / disbursements

Normally, bank is responsible for payments directly to the seller of the property. Bank should ensure that there is no process allowing any payments made to their own staff's or related parties' bank accounts. Moreover, bank should have a system that can identify and report any multiple payments under different suppliers' name but made to the same bank account.

In case of any changes to detail of recipient's bank accounts, banker should check and confirm with the recipient for any updated information to ensure that bank makes disbursements to the right party.

| Rank | Description |
|------|---|
| 1 | Match bank payment details to staff bank accounts |
| 2 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier |
| 3 | Ability to identify multiple dealer / supplier payment details to same bank account |
| 4 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |

g) Reporting

For personal loan, banks should consider generating and monitoring monthly reports relevant to fraud, fraud type analysis report, Fraud Prevention/Detection/Losses report as well as variance analysis report, etc.

Details of recommended reports are presented in the following table.

| Rank | Description |
|------|---|
| 1 | Monthly reporting: Gross/Net Fraud; Fraud to Sales; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O (Write-off) no payments, Skip/Trace <90MOB; Fraud savings, Investigation, Recoveries. |
| 2 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. |
| 3 | Monthly reports including follow-up action Items. |
| 4 | Key underwriting and transaction data tracked and used for fraud analysis. |
| 5 | Fraud Prevention/Detection/ Losses broken down by portfolio. |
| 6 | Variance analysis and development of control charts. |

h) Operational efficiency

It is recommended that banks should consider the code of conduct, conducting review by Internal Audit or independent third party, fraud detection methods, the members of Fraud team, fraud alert process, monitoring customer complaints, collection of debt after write-off, fraud awareness training, etc.

Listed below are suggested as common practice recommendations for personal loan.

| Rank | Description |
|------|---|
| 1 | Code of conduct should include clear definition of fraud. |
| 2 | Fraud Coordinator should be assigned to coordinate between Fraud Risk Manager and ISM. Moreover, regular meeting between these two groups should be arranged to ensure open communication and close gaps. |
| 3 | Conducting the review by Internal Audit or independent third party should be in place. |
| 4 | Fraud detection methods should be tailored to needs of individual portfolio. |
| 5 | The members of the Fraud team should consist of staff from Operations and Analytics. |
| 6 | The procedure for fraud alert process across industry peers should be developed. |
| 7 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. |
| 8 | Bad debt written off that is collected from customers in later period should be controlled. |
| 9 | Fraud awareness training should be provided to employees at least every six months. |
| 10 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. |
| 11 | Employee's KPIs should be established based on the risk associated with their tasks. |

i) Fraud technology

In terms of fraud technology, there are a number of considerations to enable banks to use it more efficiently for preventing/detecting fraud. Some of them are the ability to detect the similarity of names and addresses, screen data with internal watch lists, capture data from different sources, supported by a vendor representative that exists in Thailand, process efficiently, extract suspicious activities/transactions for further investigation, etc.

The following are common practice recommendations when implementing fraud prevention/detection technology.

| Rank | Description |
|------|---|
| 1 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. |
| 2 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. |
| 3 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. |
| 4 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. |
| 5 | Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide faster and efficient support. |
| 6 | Fraud detection solution should process efficiently and respond back within targeted period. |
| 7 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. |
| 8 | Fraud technology should allows banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. |
| 9 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyse and alert the responsible people in case of any unusual transactions or suspicious behaviour. |
| 10 | Fraud technology should provide the features to calculate risk scores for any |

| Rank | Description |
|------|---|
| | potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. |
| 11 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. |
| 12 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. |
| 13 | The pre-built data model should be created for the bank's existing systems. |
| 14 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. |
| 15 | False positives created from the current technology should be reduced due to poor data quality. By definition, the false positives are transactions that fraud detection tool flags as suspicious but they are not actually fraudulent. |

6. Sale Finance

Current trend sees banks services more in demand for consuming behaviour, which changes from period to period. People tend to spend more even though they have fixed income. Thus, bank provides loan instalment services to this type of customers. Normally, this loan will be used to purchase electronic appliances such as furniture for house decoration, home theatres for self entertainment, etc.

Due to increasing demand for sales finance loan, bank should establish policies and procedures to ensure that risk of fraud has been mitigated from normal bank operation.

Minimum Standards Recommendation

We categorise each recommendation according to the relevant activities operated by the bank as follows:

a) Know your customer (KYC)

In general, banks should have reasonable background knowledge over their customers before entering into any loan agreements. As a result, bank should have a policy to verify the background information of each loan applicant in order to ensure their existence and authenticity. The verification process should be performed by using public database. For example, banker should check whether the applicant's telephone number is registered or the provided contact address is real. In addition, bank should have available database which has the information for all potential blacklists and also high profile target such as anti-money laundering, default customers, fraudulent customers, etc. The high profile target customers may be classified by age, occupation, location, etc.

Moreover, the underwriting policy, which is implemented by central function, should comply with risk management procedures to mitigate high risk accounts. The update of high value fraud should be done in the bank database frequently and also that the relevant parties get the alert information on any updated high value fraud on a timely basis. The organisation system should be able to identify and summarize any applications that have been previously applied for both approved and denied applications.

| Rank | Description |
|------|--|
| 1 | Underwriting Policy noting : ID verification procedure , predefined acceptable documents : ID verification procedure for merchant, : employment/income verification procedure : address verification procedure : phone verification procedure, e.g. no third party phones for 0% down payment : weighted bureau data |
| 2 | Validated address/phone number through public databases |
| 3 | Conforms to CRP (Credit Review Point) as signed off |
| 4 | High value fraud alerts to other portfolio's at country level |
| 5 | Policy around Foreign Nationals |
| 6 | Approved policy limiting no. of loans to same family/same address |
| 7 | Fraud Blacklisting Capability |
| 8 | Ability for system to capture underwriting data (create relevant Exception reports as required) |
| 9 | Approved methodology for high Risk designation using historical data and current fraud trends |
| 10 | De-Duplicate previous application process (approved and declined apps) |
| 11 | Use of subjective negative codes from point of sale merchants |

| Rank | Description |
|------|--|
| 12 | Centrally located underwriting, segregation between Sales and Underwriting Teams |

b) Know your intermediaries (KYI)

Sometimes banks may need a third party to act as their intermediary to assist in finding potential customers. However, bank should be able to ensure that those intermediaries perform their jobs transparently since they are the primary filter for particular loan applicants. Before appointing any party as the bank's intermediary, bank should check all possible information such as company background, financial position, credit rating, etc. Bank should perform a site visit prior and after accreditation of particular intermediaries.

Moreover, bank should have a reliable database which includes all the information of intermediary blacklist and also that bank should appoint some staff to continually monitor the performance of the appointed intermediaries. This will help them ensure that loans given out to the customers, proposed by particular intermediaries, are the operating loans. Bank should also review the intermediary performance at least once a month to monitor the performance of those intermediaries.

| Rank | Description |
|------|--|
| 1 | Monthly Reporting on Intermediaries using performance triggers as review point i.e. Approval rate, W/O's, 3PD, Sales volume, delinquency, TTY, Fraud Loss. |
| 2 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. |
| 3 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. |
| 4 | Segment and Monitor by underwriter and/or Sales rep |
| 5 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups. Checks that if Intermediary terminated then terminated across all intermediary listings. |
| 6 | Payment to Intermediary after receipt of full documentation |
| 7 | Intermediaries have PI Insurance to cover intermediary fraud |

c) Asset verification

Under this process, bank should appoint in-house appraiser or external appraiser to value the assets used as guaranteed assets. One of the key processes for asset verification is that bank should have the confidence that title deed of the assets will not be transferred to third party without any acknowledgement and consent from the bank. Further detail is summarised in the table below.

| Rank | Description |
|------|--|
| 1 | Independent Asset validation process - valuation checked through independent database |
| 2 | Provide Plan for ability to identify 'at risk' accounts where asset may be on sold without finalising settlement |

d) Revolving Fund - Redraw Ability

Guidelines in dealing with revolving fund activities are summarised in the table below.

| Rank | Description |
|------|---|
| 1 | Account Takeover Controls - Ability to monitor for : Address change followed by card/PIN reissue : Activity on inactive accounts : Address change requests on lost/stolen cards |
| 2 | Authorisation Controls : Adaptive controls for high risk transaction segmentation : Adaptive controls specific to high risk cash transactions |
| 3 | Card Mailing Controls: : Dead card mailing : IVR or voice support activation : Returned Card Procedures : Card activation on new and reissued cards : Mail disguise (Plain white envelopes) or Mail mixing strategy i.e. mixture of mail houses and cards sent over a period of time |
| 4 | BIN attacks : Track unissued BIN ranges or unissued card no. : When issuing large no. of cards in same BIN range ensure they have a range of expiry dates : Investigate auth or clearing requests that contain un-issued card no. or invalid expiry dates |
| 5 | Falcon or Ariston installation - high risk strategies developed including anti-counterfeit and cross border strategies |
| 6 | Review for - large \$ payments - multiple # of payments in short time frame with large \$ value total |
| 7 | Payments against original documents |
| 8 | Create 'high risk' re -payment model for suspect accounts or credit bust-outs |
| 9 | Card Mailing Controls : IVR Failure tracking : Tiered verification strategies : Outbound deliver verification calls |
| 10 | Direct Debit repayments set up from commencement of loan |

e) Know your staff (KYS)

Bank should set a clear HR guideline in hiring their new employees. They should check all possible information to ensure that the applicant is the right person to be hired. In addition, bank should segregate duties between application approval personnel and reviewing personnel to avoid any conflict of interest.

Moreover, bank should launch effective whistle blowing practices within the organisation and also give their employees strict confidences that nothing will be disclosed once the employees have reported any unusual activities. This policy should be communicated widely throughout the organisation and updated on a timely basis.

| Rank | Description |
|------|---|
| 1 | ISM Capability with Feedback loop to Prevention |
| 2 | IT Security where system access is dictated by role |
| 3 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually |

| Rank | Description |
|------|---|
| 4 | Separate approval process and review process for Staff accounts |
| 5 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should neither maintain their own (customer) account nor maintain a related parties (customer) account. |
| 6 | Background Employment Screening (See HR guidelines & Also check financial status of employees on an annual basis to ensure they are not under financial pressure) |

f) Third party payments / disbursements

Normally, bank is responsible for payments directly to the seller of the property. Bank should ensure that they receive all required documents before any money is paid. Another importance for any disbursements to the borrowers is to ensure that the recipient of money is not their own staff's or related parties' bank accounts.

In case of any changes to detail of recipient's bank accounts, banker should check and confirm with the recipient for any updated information to ensure that bank makes disbursements to the right party. Moreover, bank should have a system which can identify multiple supplier payment details to the same bank account. This will help mitigating fraud risk from creating fake suppliers.

| Rank | Description |
|------|--|
| 1 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid |
| 2 | Payments to dealers / suppliers against full documentation |
| 3 | Match bank payment details to staff bank accounts |
| 4 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns |
| 5 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier |
| 6 | Review triggers for \$ payments by dealer / supplier type |

g) Reporting

For sales finance, it strongly suggested that significant fraud cases should be reported to the bank's headquarters. To improve the efficiency and effectiveness of fraud prevention and detection, banks should also prepare monitoring reports which include summary report of fraud investigation, monthly reports relevant to fraud, fraud prevention/detection/losses report, and fraud type analysis. Moreover, underwriting and business transactions are recognised as the important information. As a consequence, they should be gathered and used for fraud investigation and risk analysis process.

Listed below are the reports that should be created and monitored as minimum standards.

| Rank | Description |
|------|--|
| 1 | Fraud cases reported to the bank's headquarters. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. |
| 2 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. |
| 3 | Monthly reports relevant to fraud trends and comments. |
| 4 | Fraud Prevention/Detection/ Losses analyzed and reported by process weakness. |
| 5 | Fraud type analysis that provide sufficient details about methods and causes |

| Rank | Description |
|------|---|
| | of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. |
| 6 | Key underwriting and transaction data tracked and used for fraud analysis. |

h) Operational efficiency

Development of fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to business units is the most important standard for sales finance. Not only the alert process is recommended to be implemented, but banks should also tailor fraud detection approaches to the need of individual portfolio, arrange Fraud Council meeting regularly, perform random check for underwriting process, monitor unusual incidence from customer complaints, communicate fraud prevention awareness within management level, etc.

All of the minimum standards that banks should comply with are detailed in the following table.

| Rank | Description |
|------|---|
| 1 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. |
| 2 | Fraud detection methods should be tailored to needs of individual portfolio. |
| 3 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. |
| 4 | Fraud analyst should analyse fraud losses and review rule sets in fraud detection tools on an ongoing basis. |
| 5 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. |
| 6 | Random checks for underwriting process compliance should be performed. |
| 7 | The procedure for fraud alert process across industry peers should be developed. |
| 8 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. |
| 9 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. |
| 10 | Fraud Coordinator should be assigned to coordinate between Fraud Risk Manager and ISM. Moreover, regular meeting between these two groups should be arranged to ensure open communication and close gaps. |
| 11 | Fraud prevention awareness should be raised and communicated regularly in the management level. |

i) Fraud technology

With advanced technology for fraud prevention/detection, the most essential consideration is that suspicious activities/transactions or exception reports should be able to be extracted from fraud solution. The ability to interface with the Anti-Money Laundering (AML) application is also important for sales finance.

To enhance the capability to prevent and detect fraudulent behaviour, there are several standards for fraud technology. Some of them are the compatibility with existing core banking system, processing and response time, automatic analysis and data mining to detect unknown patterns, detecting the similarity of names and addresses, combating both external and internal fraud, etc.

It is recommended that banks should implement the minimum standards, as illustrated in the table below.

| Rank | Description |
|------|---|
| 1 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. |
| 2 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. |
| 3 | Fraud technology should be compatible with existing core banking system. |
| 4 | Fraud detection solution should process efficiently and respond back within targeted period. |
| 5 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. |
| 6 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. |
| 7 | Banks should implement pre-built software specifically for fraud detection technology. |
| 8 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. |
| 9 | Banks should implement case management tool with workflow capability. |
| 10 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. |
| 11 | Banks should update fraud detection techniques regularly, at least once a month. |
| 12 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. |
| 13 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. |
| 14 | False positives created from the current technology should be reduced due to poor data quality. By definition, the false positives are transactions that fraud detection tool flags as suspicious but they are not actually fraudulent. |
| 15 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. |
| 16 | Fraud technology should be deployed to combat external fraud. |
| 17 | Fraud technology should be deployed to combat internal fraud. |
| 18 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, seven days a week. |
| 19 | Fraud technology should allow banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. |

Practice Recommendation

a) Know your customer (KYC)

A clear methodology on approving sales finance application for high risk designation should be launched and strictly followed. This methodology should be developed from historical data and updated from time to time once there are any new cases. Additionally, this policy should limit no. of loans applied by the same family members or the same address.

Although some customers submit the applicant form via intermediary, bank still has to follow internal reviewing process to ensure that the information screened by the intermediary is accurate.

| Rank | Description |
|------|--|
| 1 | No second deal to be approved before first loan payment cleared. |
| 2 | Utilise high risk profiles for additional targeting |

| | |
|---|--|
| 3 | Install KYC tool where sufficient applications are available |
| 4 | Install Fraud Scorecard where sufficient data are available |
| 5 | If business operates via Intermediaries then must have documented process to audit KYC checks conducted by intermediary |
| 6 | Remote Channel - Internet Apps - Capture relevant session data (i.e. geo-location data/ IP address or other PC device ID) identify 'high risk accounts using these variables |

b) Know your intermediaries (KYI)

Normally, bank has to pay the intermediaries for the service fee when they help the bank to find and screen the prospective customers. This fee should be paid once bank has received all required documents used to approve or deny the loan application.

Bank should consistently check the financial situation of accredited intermediaries to gain some certainty that those intermediaries do not face any financial stress. Otherwise, they may coordinate with some customers to defraud the bank. This should be performed at least once a year either by internal or external parties. More detailed activities are presented in below table.

| Rank | Description |
|------|---|
| 1 | Monthly grading process must provide for closure of intermediaries depending on Performance |
| 2 | Intermediary Fraud - Included in contract with Intermediary is reimbursement for Internal Fraud. Or encourage Intermediary to take out insurance for internal fraud. |
| 3 | Robust Intermediary accreditation process – See Compliance guidelines |
| 4 | Perform site visitation prior to accreditation of broker |
| 5 | Bank holds cash deposit from merchant and is able to claw back this amount in case of merchant fraud |
| 6 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. |
| 7 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level |
| 8 | KYI tool installed - i.e. Actimize |

c) Asset verification

Under this process, bank should appoint in-house appraiser or external appraiser to value the assets used as guaranteed assets. One of the key processes for asset verification is that bank should have the confidence that title deed of the assets will not be transferred to third party without any acknowledgement and consent from the bank. Further detail is summarised in below table.

| Rank | Description |
|------|---|
| 1 | Process that allows clear title registration over asset within a set time frame |
| 2 | If asset is not registered prior to disbursement then audit to ensure asset is secured within prescribed time frame |
| 3 | Prevent/monitor for forward sale of asset by customer |
| 4 | Clearly defined asset type that will be eligible for loans, Caps on extra's as defined by policy |

d) Revolving Fund - Redraw Ability

There are some activities that the bank should follow to mitigate fraud risk as mentioned in the table below.

| Rank | Description |
|------|---|
| 1 | Process where Open to Buy is only released on cleared funds |
| 2 | Disbursement to customer account. Ability to match customer name to bank account no. |
| 3 | Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product |
| 4 | Remote Channel - Brand Domain Protection Anti-phishing take-down ability |
| 5 | Remote Channel - Internet /e-business transaction monitoring : Adaptive Authentication in Host system : Geo-location Analysis |
| 6 | Implement MasterCard Secure Code or Verified by Visa |
| 7 | Temporary Shopping Cards : Must be issued for a specified short period of time i.e. two weeks : Must only be issued for in store new accounts |
| 8 | Remote Channel - Card Not Present Authentication MasterCard 3D Secure Code Verified by Visa |
| 9 | Common Point of Compromise tracking |
| 10 | Chargeback Tracking |
| 11 | Process that allows early identification of payments that do not have cleared funds i.e. dishonoured check process |

e) Know your staff (KYS)

To avoid fraud risk from internal staff, bank should be able to identify staff and related parties' bank account once the bank employs particular staff. This will help the bank to have more monitoring activities to avoid internal fraud from their employees since some staff may transfer bank's customer account into their own account or related parties' account.

In some circumstances that banker also acts as sales staff to offer some products to the customers. Bank should monitor and make some comparison over the staff sales performance to ensure that their staff do not create numerous sales with low profile customers. Bank should also have a particular report to summarise sales for each staff comparing these with non operating customers who are proposed by particular staff.

| Rank | Description |
|------|---|
| 1 | Can employees access into other banks beyond the bank they are working for? |
| 2 | Installation of KYS tool - Intellinx/Footprint |
| 3 | Ability to identify staff accounts. |
| 4 | Review process for Branches and Staff receiving Sales bonus's - review at both Branch and individual staff member level |

f) Third party payments / disbursements

Once bank has followed all recommended minimum standards mentioned above, they should continually monitor each activity to ensure that they are on the right track.

| Rank | Description |
|------|---|
| 1 | Ability to identify multiple dealer / supplier payment details to same bank account |
| 2 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded |

g) Reporting

For sales finance, it is important for banks to develop and monitor additional reports, for example, quarterly reports, monthly reports, Fraud Prevention/Detection/Losses, etc.

The following table shows more detail of the reports that banks should prepare.

| Rank | Description |
|------|---|
| 1 | Quarterly reporting that also covers new global standards, such as fraud to W/O (Write-off), Fraud to NI, Reporting that is tailored to most relevant metric that would show impact to bottom line for country portfolio. |
| 2 | Monthly reporting: Gross/Net Fraud; Fraud to Sales; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O (Write-off) no payments, Skip/Trace <90MOB; Fraud savings, Investigation, Recoveries. |
| 3 | Fraud Prevention/Detection/ Losses broken down by fraud type. |
| 4 | Monthly reports including follow-up action items. |
| 5 | Fraud Prevention/Detection/ Losses broken down by portfolio. |
| 6 | Variance analysis and development of control charts. |

h) Operational efficiency

To increasing the operational efficiency, it is recommended that banks should consider prevention of data losses, fraud training program, central check list of underwriting process, collection of debt after write-off, the members of Fraud team, code of conduct, fraud policy and procedure, etc.

Listed below are common practice recommendations for sales finance.

| Rank | Description |
|------|--|
| 1 | Data leakage from both paper-based and electronic-based sources should be controlled. |
| 2 | Fraud training programs should be conducted for Underwriting staff. |
| 3 | Centrally located underwriting with documented check list of loans should be in place. |
| 4 | Bad debt written off that is collected from customers in later period should be controlled. |
| 5 | The members of the Fraud team should consist of staff from Operations and Analytics. |
| 6 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. |
| 7 | Code of conduct should include clear definition of fraud. |
| 8 | Involvement/sign off in CRP (Credit Review Point) and NPI (New Product Innovations) process. |

| Rank | Description |
|------|--|
| 9 | Employee's KPIs should be established based on the risk associated with their tasks. |
| 10 | Formalised fraud policy and procedure should be developed. |
| 11 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. |

i) Fraud technology

In terms of technology, there are several practice recommendations when deploying fraud prevention/detection tools in the organisation. For instance, the ability to interface between fraud detection technology and other legacy systems, Social Network Analysis, generating different views of reports, function to calculate risk scores, the ability to prioritise each fraud case as well as enable users to design and develop a report template, etc.

Common practice recommendations for sales finance include the following:

| Rank | Description |
|------|--|
| 1 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. |
| 2 | Social Network Analysis should be used to detect and visualise fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. |
| 3 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. |
| 4 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. |
| 5 | Fraud technology should have the ability to prioritise each fraud case according to risk scores and notify suspicious activities to the management. |
| 6 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. |
| 7 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. |
| 8 | Fraud technology should be supported by a vendor representative/service provider that exists in Thailand to provide faster and efficient support. |
| 9 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. |
| 10 | The pre-built data model should be created for the bank's existing systems. |
| 11 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. |

When and How to Use TBA Minimum Standard Recommendations

Nowadays, fraudulent activities have been increased in all business sectors, including banking industry. In order to mitigate fraud risk and its potential losses, we encourage bankers to follow these five steps:

- First of all, bank should identify the products which it provides to the market and try to match with the most similar type of products mentioned above.
- Then bank should appoint a champion/project manager to form a guideline to be used in its business procedure. This guideline should be focus on the minimum standard recommendations.
- Introduce a guideline into bank's business procedure for each product.
- After bank has satisfied with this new procedure, bank should move on to the practice recommendations. This will help bank gain more confidence in mitigating fraud risk from both internal and external parties.
- Finally, bank should consistently review its business operation to ensure that the applied suggestion has been efficiently followed.

The Difference between Minimum Standard Recommendations and Practice Recommendations

Minimum standard recommendations are the activities, encouraged by FMC & PwC, which bank should include in their business operation and consistently follow to ensure that it has efficiently mitigate potential fraudulent activities committed by either internal or external parties. Even though these activities have been stated in bank's guideline of work, bank still should appoint an independent party to observe and review the bank's operation to make sure that the proposed activities have been successfully followed by all relevant parties.

While practice recommendation is less prioritised standard, bank should implement this into its business procedures if there are sufficient resources available, such as time and human resources, etc. to follow the above guideline. Another factor which encourages bank to include practice recommendation in its operation is when bank launches new product to the market. On the other hand, bank should set up the business milestone. For example, bank should set a five-year milestone to reduce and make fraud become zero. Under this milestone, bank set its first three years to successfully implement all minimum standard recommendation while the last two year is to implement practice recommendation into its business.

However, if bank experiences any fraudulent activities during the last twelve months, it is strongly recommended that bank follow both minimum and practice standard recommendation in order to improve the current operation and mitigate all possible losses from fraud.

Survey Observation

Most Variance Response

We summarize top 10 variances of each product according to its most variance response from the survey participants as below. Some participants may consider these activities as very important while others may not. Each bank should take this to its own consideration whether these activities are suitable to its product and should be implemented to its business procedures.

Commercial loan:

1. Payments to dealers / suppliers against full documentation
2. Payments directly to dealer or supplier, not to customer with proof that supplier is paid
3. Fraud Coordinator should ensure that 'Close the loop' process is finalized.
4. Independent checking/confirmation when notified of changes to payment details of dealer / supplier
5. Disbursement - Model no. of payments and \$ value and payee and review unusual patterns
6. False positives created from the current technology should be reduced due to poor data quality.
7. Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application.
8. Fraud case management report including the progression and follow-up of fraud investigation, and exchange of fraud information/news. In addition, fraud cases should be reported to the Bank of Thailand.
9. Fraud training programs should be conducted for Underwriting staff.
10. Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded

Hire purchase:

1. False positives created from the current technology should be reduced due to poor data quality.
2. The pre-built data model should be created for the bank's existing systems.
3. Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly.
4. Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management.
5. Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank.
6. Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week.
7. Banks should update fraud detection techniques regularly, at least once a month.
8. Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application.
9. De-Duplicate application process (approved and declined apps)
10. Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded

Merchant:

1. False positives created from the current technology should be reduced due to poor data quality.
2. Direct Debit repayments set up from commencement of loan
3. Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly.
4. Fraud/Internal audit team should have access to their dedicated hardware/server/database.
5. Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application.
6. Implement MasterCard SecureCode or Verified by Visa
7. Review triggers for \$ payments by dealer / supplier type
8. Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool.
9. The pre-built data model should be created for the bank's existing systems.
10. Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank.

Mortgage loan:

1. Account Takeover Controls - Documented process for High Risk Transactions
2. Payments to dealers / suppliers against full documentation
3. Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded
4. Disbursement - Model no. of payments and \$ value and payee and review unusual patterns
5. Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product
6. Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week.
7. Payments directly to dealer or supplier, not to customer with proof that supplier is paid
8. Transaction Fraud Tool - e.g. Aristion (where re-draw facility completed through Credit Card transaction)
9. Account Takeover Controls: Ability to identify high risk transactions and create Exception Report
10. False positives created from the current technology should be reduced due to poor data quality.

Personal loan:

1. Clearly defined asset type that will be eligible for loans, Caps on extra's as defined by policy
2. Process that allows clear title registration over asset within a set time frame
3. Payments directly to dealer or supplier, not to customer with proof that supplier is paid
4. Payments to dealers / suppliers against full documentation
5. Provide Plan for ability to identify 'at risk' accounts where asset may be on sold without finalizing settlement
6. Review triggers for \$ payments by dealer / supplier type
7. Prevent/monitor for forward sale of asset by customer
8. If asset is not registered prior to disbursement then audit to ensure asset is secured within prescribed time frame
9. Ability to identify multiple dealer / supplier payment details to same bank account
10. Remote Channel - Internet Apps : Capture relevant session data (i.e. geo-location data/ IP address or other PC device ID) identify 'high risk accounts using these variables

Sale finance:

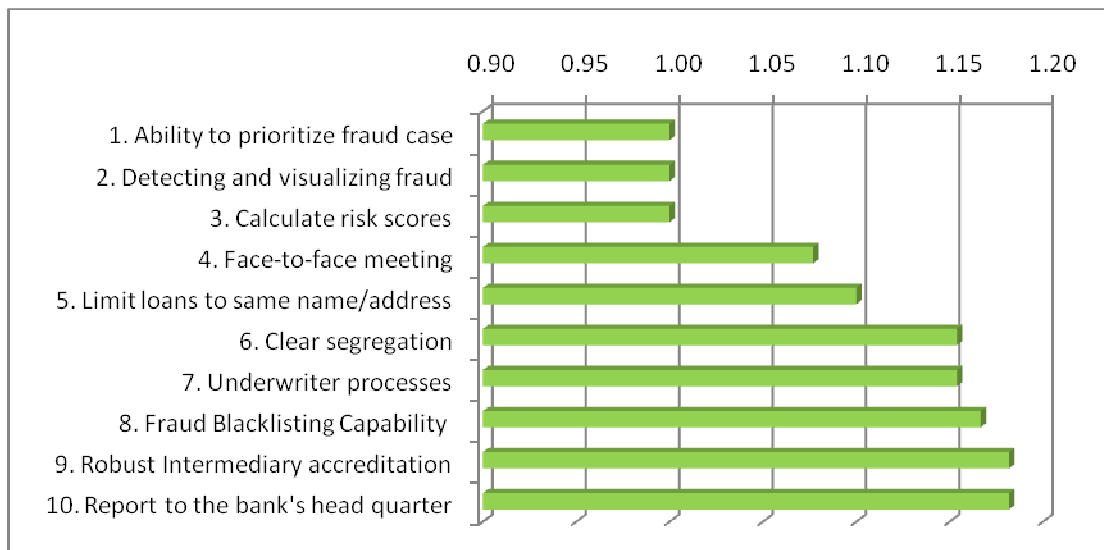
1. Remote Channel - Brand Domain Protection and Anti-phishing take-down ability
2. Remote Channel - Internet /e-business transaction monitoring
 - Adaptive Authentication in Host system
 - Geo-location Analysis
3. Disbursement to customer account. Ability to match customer name to bank account no.
4. Process where Open to Buy is only released on cleared funds
5. Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product
6. Remote Channel - Card Not Present Authentication and MasterCard 3D Secure Code Verified by Visa
7. Implement MasterCard Secure Code or Verified by Visa
8. Create 'high risk' re -payment model for suspect accounts or credit bust-outs
9. Review for
 - large \$ payments
 - multiple # of payments in short time frame with large \$ value total
10. Card Mailing Controls
 - IVR Failure tracking
 - Tiered verification strategies
 - Outbound deliver verification calls

Most Compliance

In this section, a list of the top-ten activities that bank operations have already implemented is shown below followed by a visualized graph. Score in each graph refers to the percentage of compliance by bankers; the least number refers to the most complied no. of banks.

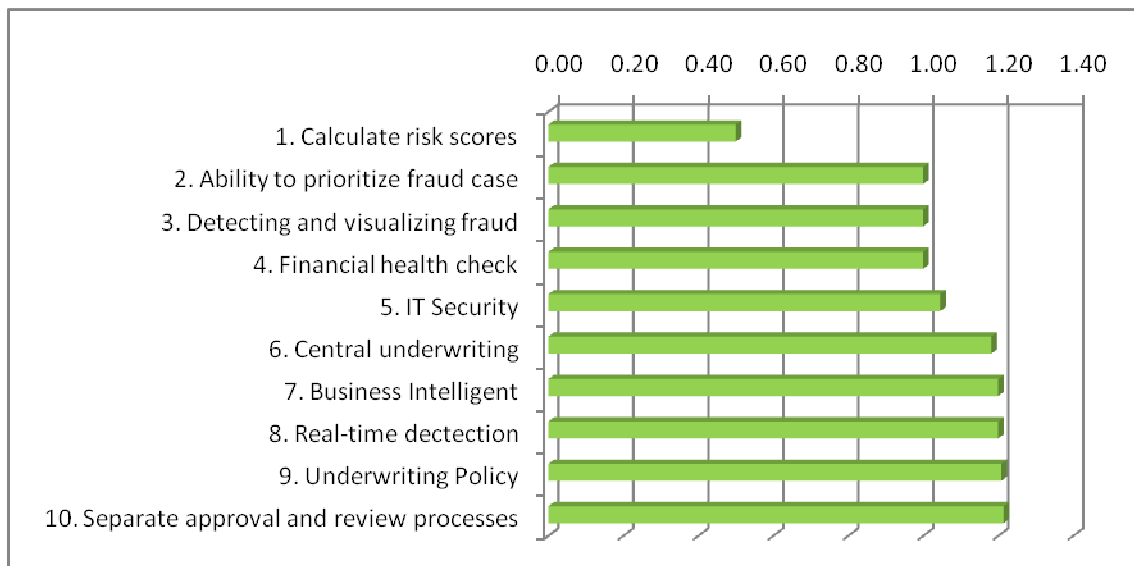
Commercial loan:

1. Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management.
2. Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank.
3. Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically.
4. Face to Face meeting with customer (prior to submission of Credit Application for approval) an initial and regular SITE VISITS to monitor customer business health / adherence to credit conditions, etc.
5. Ability to Limit No. of loans to same name/address
6. Clear segregation between Sales and Underwriting to avoid conflicts of interest otherwise inherent
7. Bank has in place, and properly follows, written Underwriting processes that check:
 - The Customer Company and
 - Its beneficial owners
 - Its Management
 - Its Related Companies
8. Fraud Blacklisting Capability
9. Robust Intermediary accreditation process – See Compliance guidelines
10. Fraud cases reported to the bank's head quarter. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital.



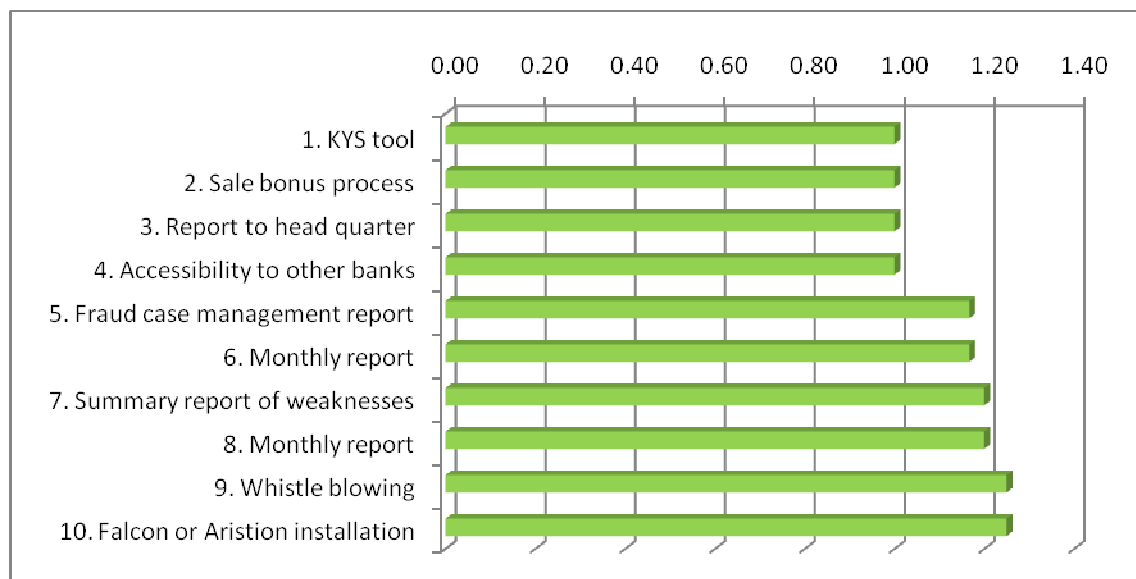
Hire Purchase:

1. Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically.
2. Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management.
3. Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank.
4. Credit of the intermediary or its financial health checks should be obtained and review as an annual basis.
5. IT Security where system access is dictated by role
6. Centrally located underwriting, segregation between Sales and Underwriting Teams
7. Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection.
8. Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week.
9. "Underwriting Policy noting
 - ID verification procedure,
 - employment/income verification procedure
 - address verification procedure
 - phone verification procedure
 - weighted bureau data
10. Separate approval process and review process for Staff accounts



Merchant:

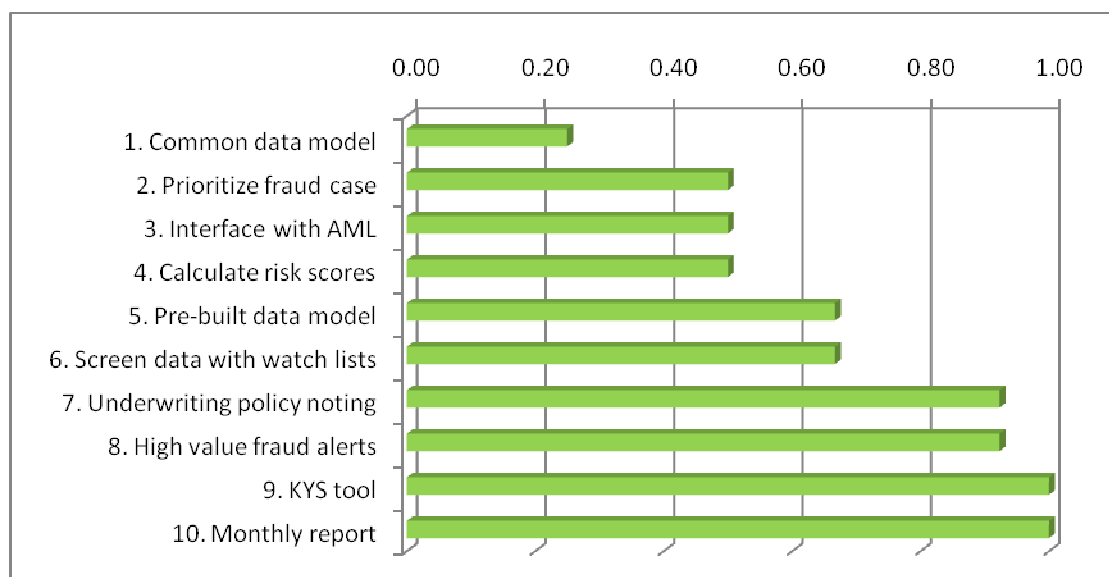
1. Installation of KYS tool - Intellinx/Footprint
2. Review process for Staff receiving Sales bonus's - review at both Branch/Merchant and individual staff member level
3. Fraud cases reported to the bank's head quarter. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital.
4. Can employees access into other banks beyond the bank they are working for?
5. Fraud case management report including the progression and follow-up of fraud investigation, and exchange of fraud information/news. In addition, fraud cases should be reported to the Bank of Thailand.
6. Monthly reporting: Gross/Net Fraud; Fraud to Sales ; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O no payments, Skip/Trace <90MOB (month on book) ; Fraud savings, Investigation, Recoveries.
7. Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue.
8. Monthly reports relevant to fraud trends and observations.
9. Whistle blowing and "Zero tolerance" policy documented and communicated at least annually
10. Falcon or Aristion installation - high risk strategies developed including ant-counterfeit and cross border strategies



Mortgage loan:

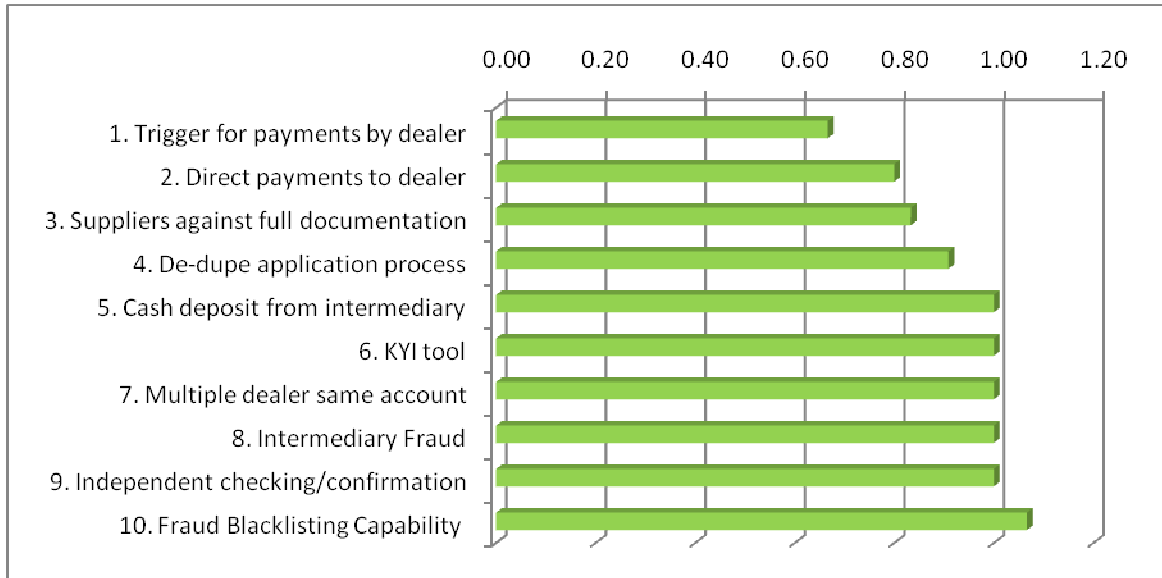
1. Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool.
2. Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management.
3. Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application.
4. Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically.
5. The pre-built data model should be created for the bank's existing systems.
6. Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc.

7. Underwriting Policy noting:
 - ID verification procedure,
 - employment/income verification procedure
 - address verification procedure
 - weighted Bureau data (If applicable)
8. High value Fraud Alerts to other portfolios at country level
9. Installation of KYS tool - e.g. Intellinx/Footprint
10. Monthly reports relevant to fraud trends and observations.



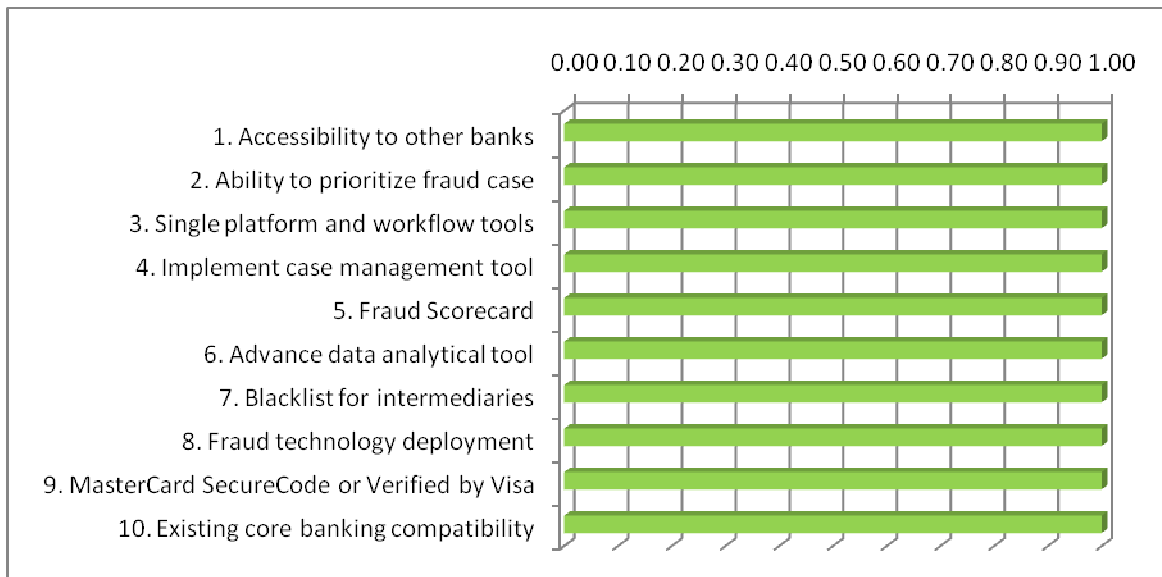
Personal loan:

1. Review triggers for \$ payments by dealer / supplier type
2. Payments directly to dealer or supplier, not to customer with proof that supplier is paid
3. Payments to dealers / suppliers against full documentation
4. De-Dupe application process (approved and declined apps)
5. Bank holds cash deposit from Intermediary and is able to claw back this amount in case of merchant fraud
6. KYI tool installed - i.e. Actimize
7. Ability to identify multiple dealer / supplier payment details to same bank account
8. Intermediary Fraud - Included in contract with Intermediary is reimbursement for Internal Fraud. Or encourage Intermediary to take out insurance for internal fraud.
9. Independent checking/confirmation when notified of changes to payment details of dealer / supplier
10. Fraud Blacklisting Capability



Sale finance:

1. Can employees access into other banks beyond the bank they are working for?
2. Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management.
3. Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns.
4. Banks should implement case management tool with workflow capability.
5. Install Fraud Scorecard where sufficient data available
6. Banks should own advance data analytical tool that can identify anomalies or suspicious activities.
7. "Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups. Checks that if Intermediary terminated then terminated across all intermediary listings."
8. Fraud technology should be deployed to combat external fraud.
9. Implement MasterCard Secure Code or Verified by Visa
10. Fraud technology should be compatible with existing core banking system.

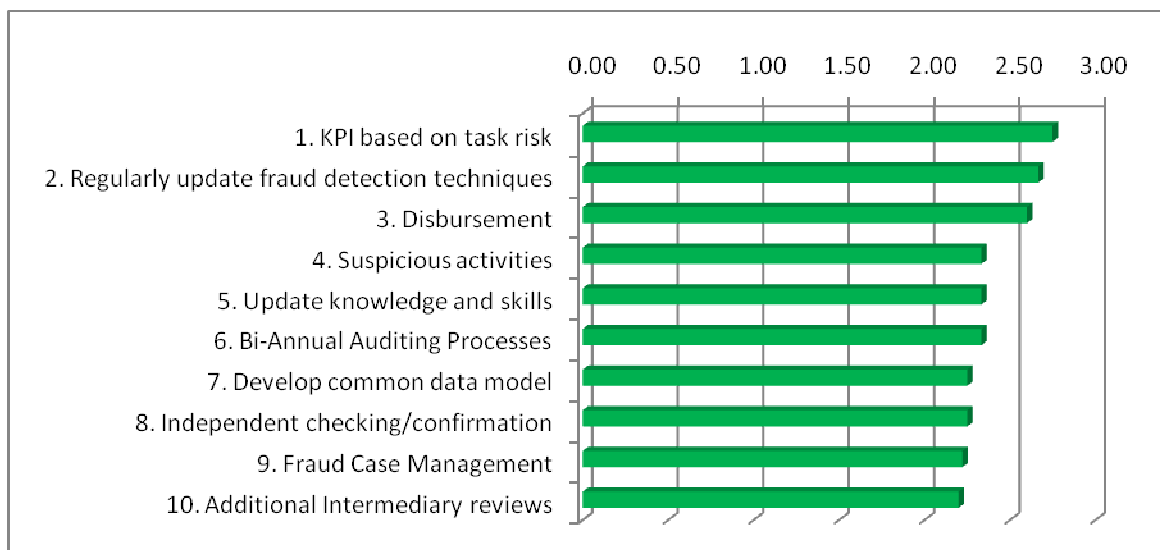


Least Compliance

This section is a summary of activities which are least complied by bank's operation. Score presented in the chart refers to the implemented percentage by the banks. The larger score refers to the least compliance by bankers.

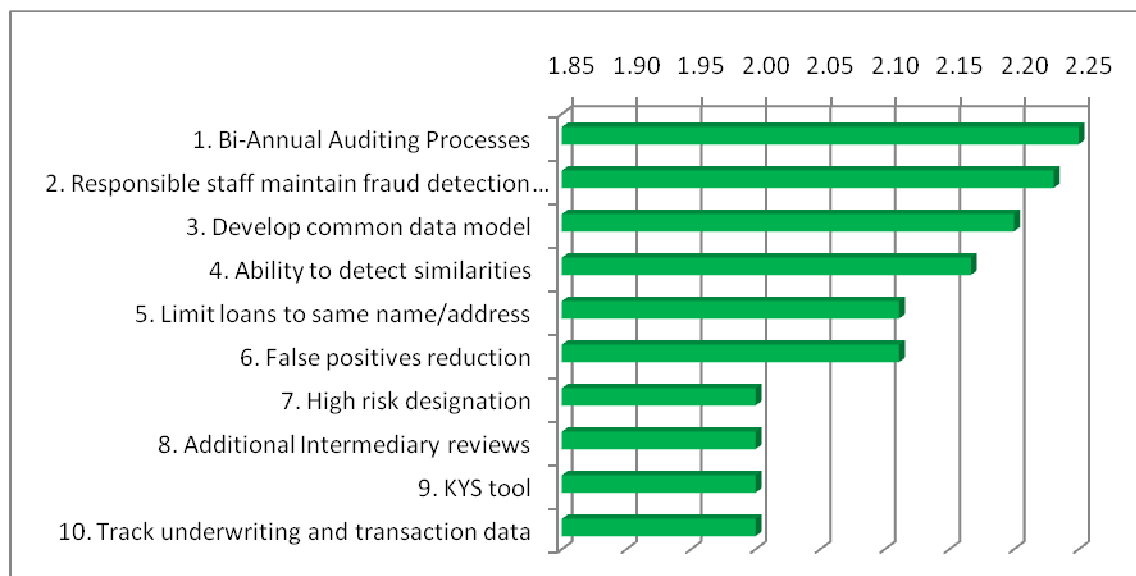
Commercial loan:

1. Employee's KPIs should be established based on the risk associated with their tasks.
2. Banks should update fraud detection techniques regularly, at least once a month.
3. Disbursement - Model no. of payments and \$ value and payee and review unusual patterns
4. Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis.
5. Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud.
6. Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded
7. Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool.
8. Independent checking/confirmation when notified of changes to payment details of dealer / supplier
9. Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit.
10. Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit / site visit processes.



Hire Purchase:

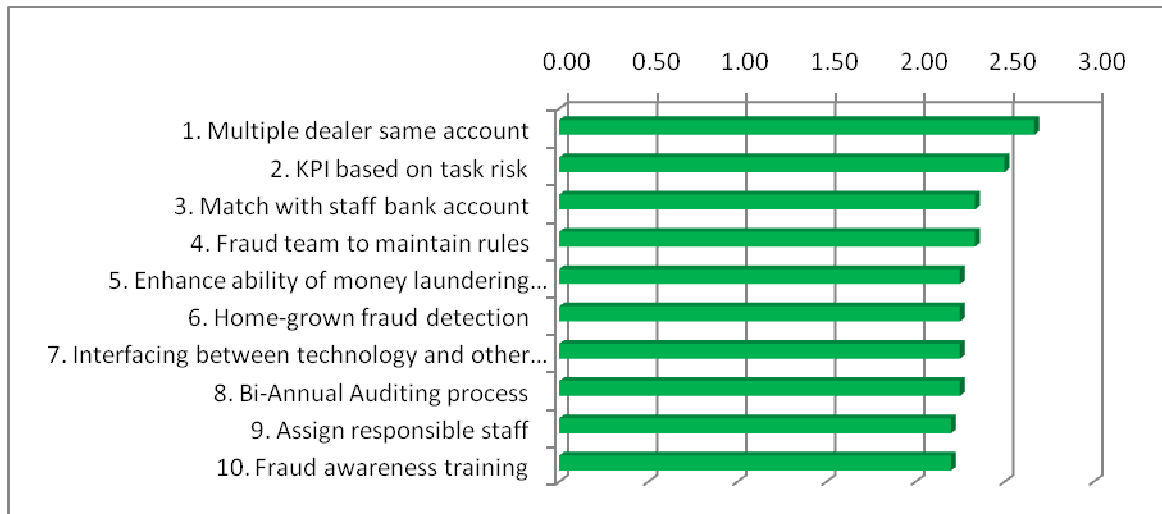
1. Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded
2. Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted.
3. Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool.
4. Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic.
5. Approved policy limiting no. of loans to same family/same address
6. False positives created from the current technology should be reduced due to poor data quality.
7. Approved methodology for high Risk designation using historical data and current fraud trends
8. Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process.
9. Installation of KYS tool - Intellinx/Footprint
10. Key underwriting and transaction data should be tracked and used for fraud analysis.



Merchant:

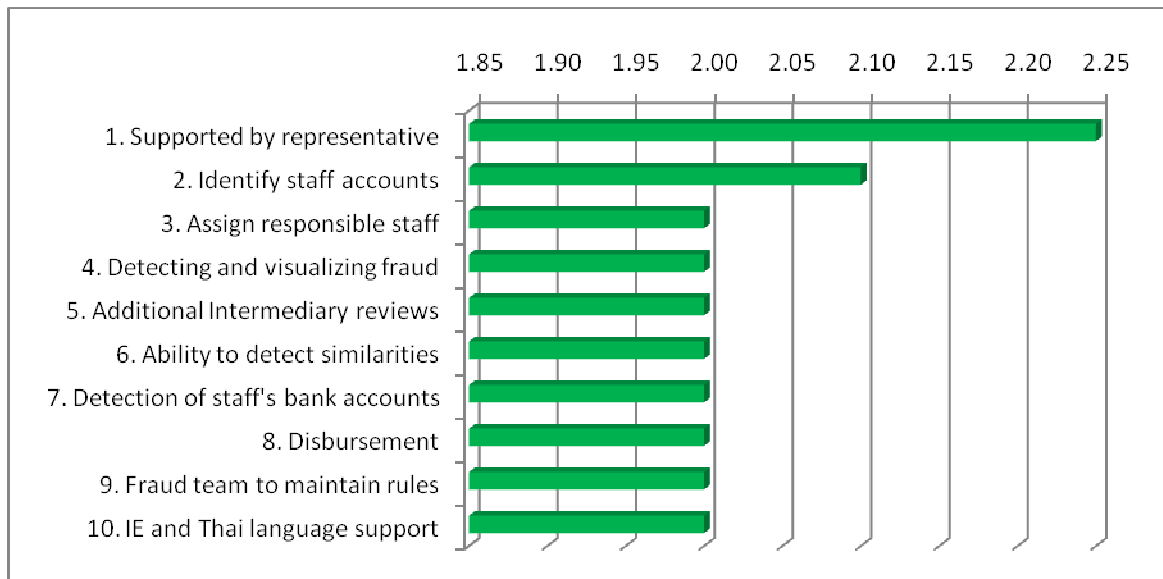
1. Ability to identify multiple dealer / supplier payment details to same bank account
2. Employee's KPIs should be established based on the risk associated with their tasks.
3. Match bank payment details to staff bank accounts
4. Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules.
5. Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection.
6. Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc.
7. As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations.
8. Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed

- above) is measured and recorded
9. Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted.
 10. Fraud awareness training should be provided to employees at least every six months.



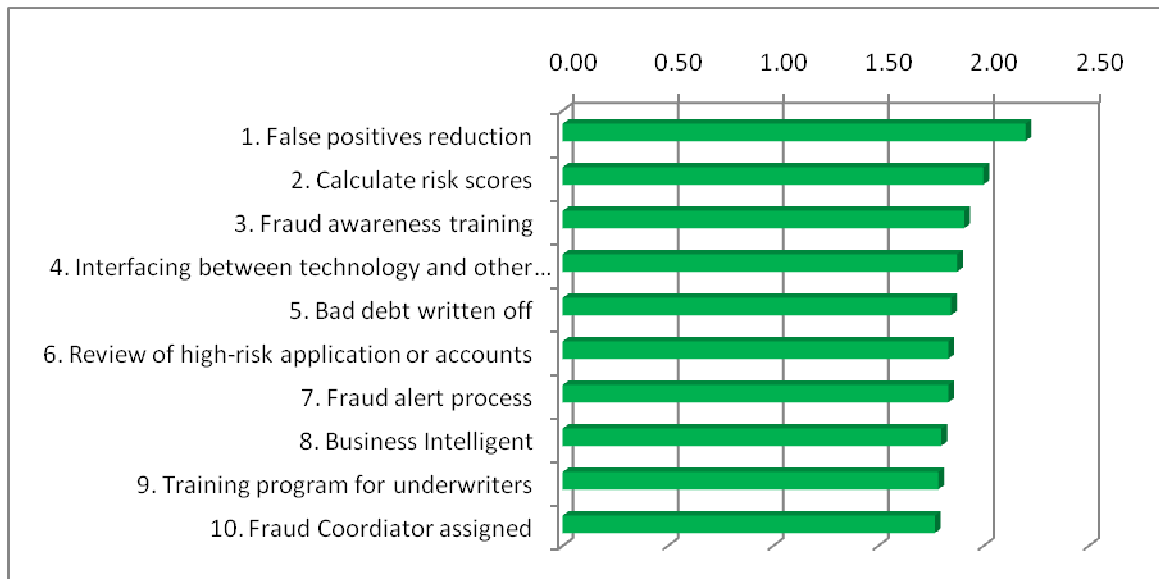
Mortgage loan:

1. Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide faster and efficient support.
2. Ability to identify staff accounts. Monitor staff and related party accounts for internal fraud
3. Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted.
4. Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank.
5. Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process.
6. Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic.
7. Fraud technology should consistently detect the staff's bank accounts and relevant people, analyze and alert the responsible people in case of any unusual transactions or suspicious behaviour.
8. Disbursement - Model no. of payments and \$ value and payee and review unusual patterns
9. Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules.
10. Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly.



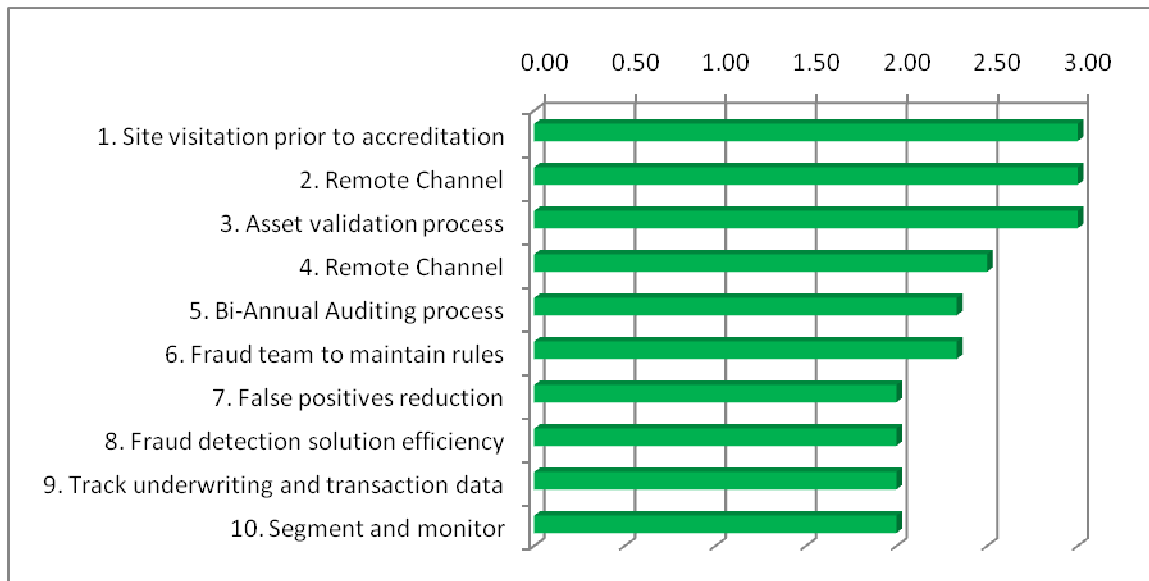
Personal loan:

1. False positives created from the current technology should be reduced due to poor data quality.
2. Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically.
3. Fraud awareness training should be provided to employees at least every six months.
4. As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations.
5. Bad debt written off that is collected from customers in later period should be controlled.
6. 100% review of high risk application or accounts should be conducted. For example,
 - 3PD or 2PD with no customer contact
 - Accounts that are potentially ""Skip"" accounts < 210 days on book
 - Accounts where mail has been returned from the outset of the account opening.
7. The procedure for fraud alert process across industry peers should be developed.
8. Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection.
9. Fraud training programs should be conducted for Underwriting staff.
10. Fraud Coordinator should be assigned to coordinate between Fraud Risk Manager and ISM. Moreover, regular meeting between these two groups should be arranged to ensure open communication and close gaps.



Sale finance:

1. Perform site visitation prior to accreditation of broker
2. Remote Channel - Card Not Present Authentication
 - MasterCard 3D Secure Code
 - Verified by Visa
3. Independent Asset validation process - valuation checked through independent database
4. Remote Channel - Internet /e-business transaction monitoring
 - Adaptive Authentication in Host system
 - Geo-location Analysis
5. Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded
6. Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules.
7. False positives created from the current technology should be reduced due to poor data quality.
8. Fraud detection solution should process efficiently and respond back within targeted period.
9. Key underwriting and transaction data tracked and used for fraud analysis.
10. Segment and Monitor by underwriter and/or Sales rep



Importance but not Implemented

We also note that some activities are considered as important activities and should be implemented in bank's operation; however, they are still not implemented by some banks. The activities ranking by their most importance are presented as follows:

Commercial loan:

1. Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed.
2. In the event the Bank Business becomes aware of any improper/illegal behaviour by the customer, the fraud/credit risk implications are properly/independently assessed, e.g. where tax penalties can lead to the authorities having a prior claim to company's assets
3. Policy to protect the Business's interests and security in respect of cross-border lending or where the collateral is already, or may move, to another country
4. Bank Business has a process to monitor and respond to environmental changes that would materially increase the risk of fraud
5. Conducting the review by Internal Audit or independent 3rd party should be in place.
6. Fraud analyst should analyze fraud losses and review rule sets in fraud detection tools on an ongoing basis.
7. Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units.
8. A consolidated view of each customer's TOTAL RELATIONSHIP with the Business, showing also any rejections by Bank (Underwriter / Credit Officer) on any / all PRIOR credit applications by that customer or by any of its beneficial owners / management / related companies (this is comparable to Consumer Banking 'De-dupe' controls)
9. Ability for system to capture (and permanently retain) underwriting decisions and data and to create relevant Exception Reports as required
10. Independent Credit Control / Admin function to carry out all initial and periodic checks and monitoring activities

Hire purchase:

1. Fraud cases reported to the bank's head quarter. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital.
2. Segment and Monitor by underwriter and/or Sales rep
3. Centrally located underwriting, segregation between Sales and Underwriting Teams
4. Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups. Checks that if Intermediary terminated then terminated across all intermediary listings.
5. High value Fraud alerts to other portfolio's at country level
6. Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating.
7. Robust Intermediary accreditation process – See Compliance guidelines
8. IT Security where system access is dictated by role
9. Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit.
10. Monthly Reporting on Intermediaries using performance triggers as review point i.e. Approval rate, W/O's, 3PD, Sales volume, delinquency, TTY, Fraud Loss.

Merchant:

1. Random checks for underwriting process compliance should be performed.
2. Fraud analyst should analyze fraud losses and review rule sets in fraud detection tools on an ongoing basis.
3. Monitor staff and related party accounts for internal fraud - Monitor monthly approval rates and write offs by individual staff (Sales, U/writing and Collections staff)
4. Fraud Blacklisting Capability
5. Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed.
6. High value Fraud alerts to other portfolio's at country level
7. Fraud detection methods should be tailored to needs of individual portfolio.
8. Authorization Controls
 - Adaptive controls for high risk transaction segmentation
 - Adaptive controls specific to high risk cash transactions
9. Fraud Prevention/Detection/ Losses broken down by portfolio.
10. BIN attacks
 - Track unissued BIN ranges or unissued card no.s
 - When issuing large no.s of cards in same BIN range ensure they have a range of expiry dates
 - Investigate auth or clearing requests that contain un-issued card no.s or invalid expiry dates

Mortgage loan:

1. Key underwriting and transaction data tracked and used for fraud analysis.
2. Exception reports for high risk transactions.
3. Underwriting Policy that has different requirements for :
 - Self-employed applicants
 - Self-certified applicants (Stated income Applicants)
 - commercial properties (If applicable)
4. De-Duplicate application applicant process (approved and declined apps)
5. Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue.
6. Policy around Foreign Nationals
7. Background Employment Screening (See HR guidelines & Also check financial status of employees on an annual basis to ensure they are not in a financial pressure)
8. Policy and process whereby address/phone numbers can be validated through public databases
9. Fraud Prevention/Detection/ Losses analyzed and reported by process weakness.
10. Fraud Prevention/Detection/ Losses broken down by fraud type.

Personal loan:

1. Validated address/phone number through public databases
2. Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit.
3. Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted.
4. High value Fraud alerts to other portfolio's at country level
5. Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud.
6. Centrally located underwriting, segregation between Sales and Underwriting Teams
7. Quarterly reporting that covers new global standards i.e. fraud to W/O, Fraud to NI, Reporting that is tailored to most relevant metric that would show impact to bottom line for country portfolio.
8. Policy around Foreign Nationals

9. Separate approval process and review process for Staff accounts
10. ISM (Investigation & Security Manager) Capability with Feedback loop to Prevention

Sale finance:

1. High value Fraud alerts to other portfolio's at country level
2. The procedure for fraud alert process across industry peers should be developed.
3. Installation of KYS tool - Intellinx/Footprint
4. Fraud detection methods should be tailored to needs of individual portfolio.
5. Variance analysis and development of control charts.
6. Fraud Prevention/Detection/ Losses broken down by portfolio.
7. Whistle blowing and "Zero tolerance" policy documented and communicated at least annually
8. Policy around Foreign Nationals
9. Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis.
10. Falcon or Aristion installation - high risk strategies developed including ant-counterfeit and cross border strategies

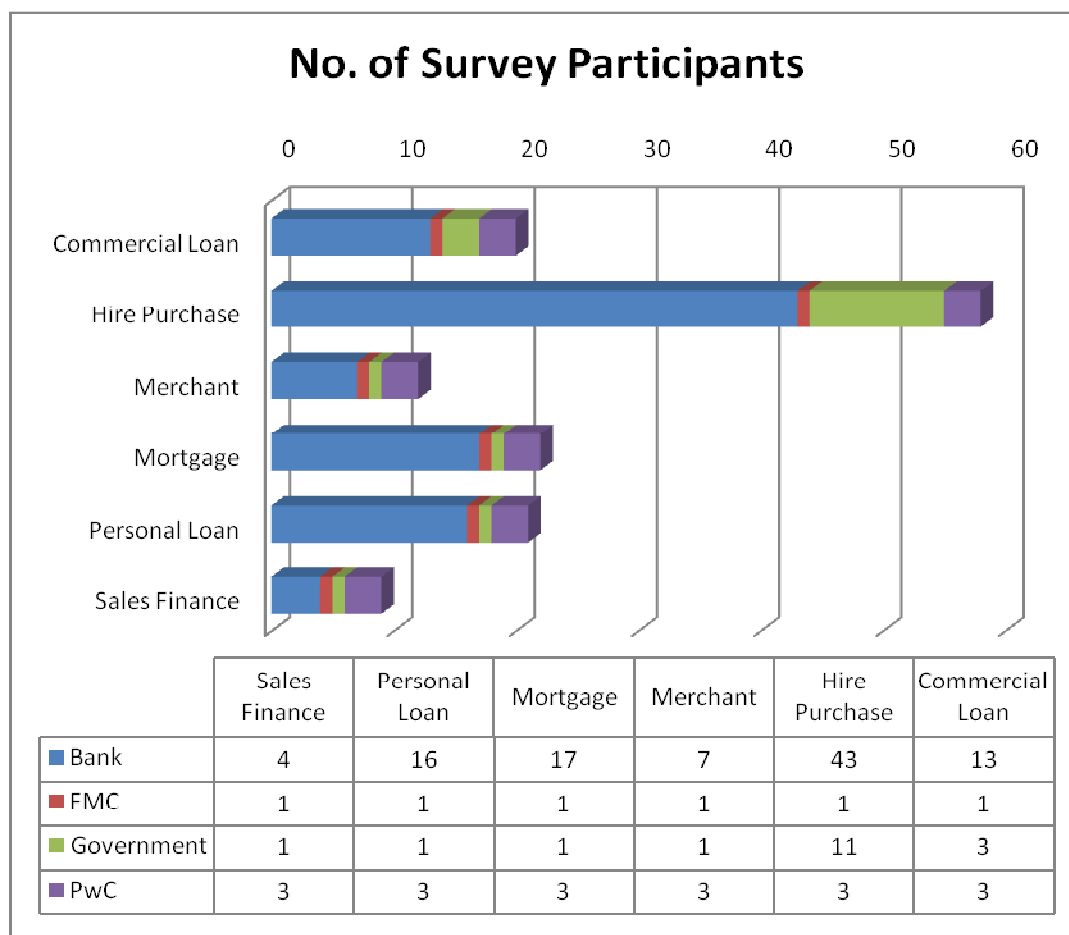
Analysis – Fraud Management Compliance Assessment

Participation and Resources

A questionnaire / survey had developed and distributed to the 23 member banks and relevant government agencies. The results consist of responses from the following parties:

- Bankers – 60% (Bankers represent bank practitioners who are part of either a fraud team or internal audit team);
- Government agencies – 10% (Government agencies are the representatives of Bank of Thailand, Department of Special Investigation, Anti-Money Laundering Office, etc.);
- Fraud Management Club – 15%; and
- PwC – 15% (PwC represents expertise in banking industry).

The summary of participants for each product is presented in below table.



19 out of 43 bank participants for Hire Purchase, 4 out of 17 bank participants for Mortgage loan, and 1 out of 16 bank participants for Personal Loan stated that their banks do not provide such product to the market; however, they believe that some activities should be included in the minimum standard recommendations since they are the key operating activities for certain business.

Methodology for Minimum Standard Recommendations

TBA and PwC have developed a questionnaire / survey and distributed to the 23 member banks and relevant government agencies in order to assess their current practice performance and levels of competency, and to understand the future demand profile for the opportunities for improvement.

The activities consist of the following:

- 2-day workshops with the goal to identify gap on current practice performance among various banks and perspectives from government agencies;
- Survey of individual opinion and experience in dealing with fraud cases in the organisation; and
- Fraud minimum standard questionnaire for the Banking Industry, developed in conjunction with FMC, which is distributed and obtained during the 2-day workshop.

Each party of the bank practitioners provides a different point of view towards banking activities to ensure that the most appropriate minimum standard is recommended to this industry.

The results from this survey will be separated into three parts:

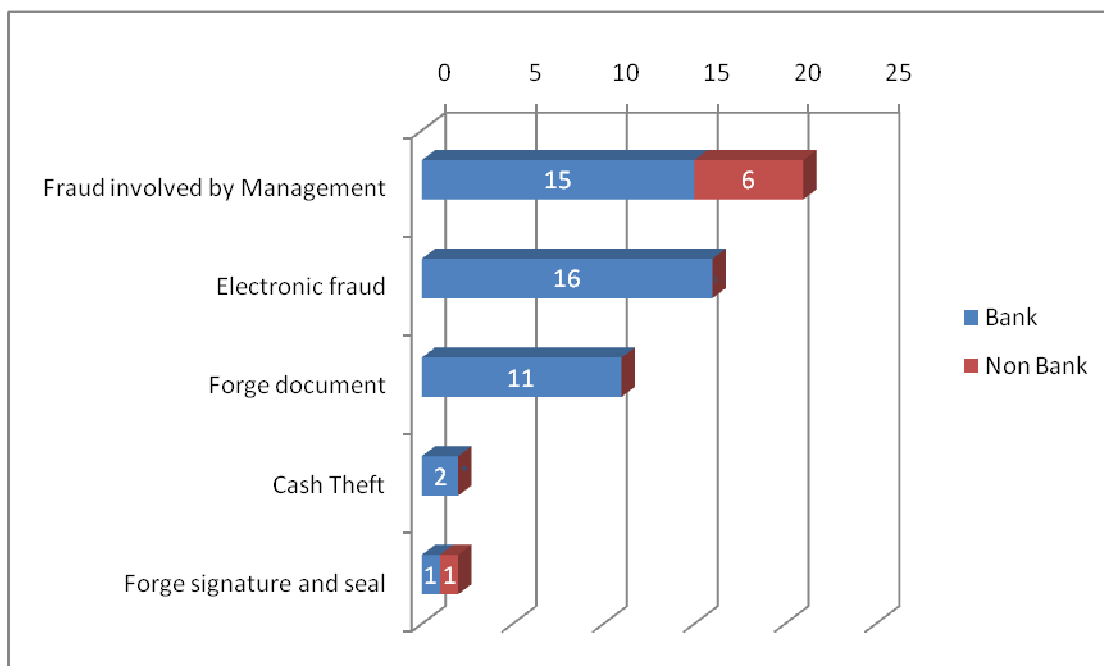
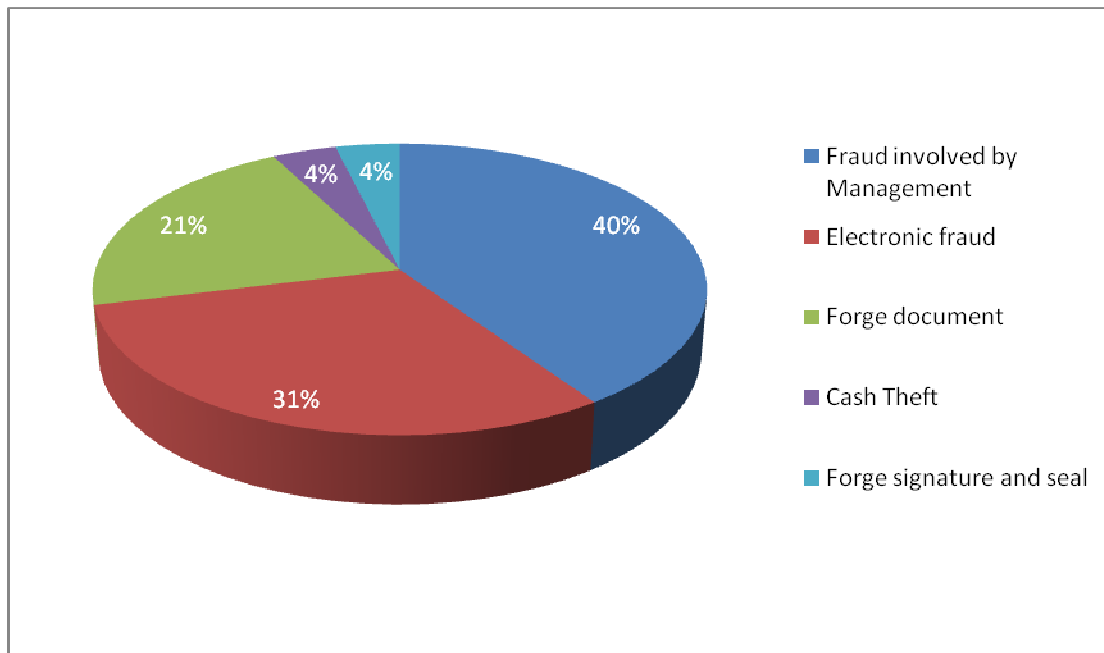
1. Minimum standard recommendation – most of the participants in this survey consider that this part is the most important part in operating banking business and the organisation should include these as minimum practices within the organisation.
2. Practice standard recommendation – while this is also important, the organisation should have their own consideration whether or not to set these as minimum standards.
3. Guidance notes – these are the summary of standards complied with by the respondents and also some comments from the survey participants.

Participants' Individual Opinion and Experiences

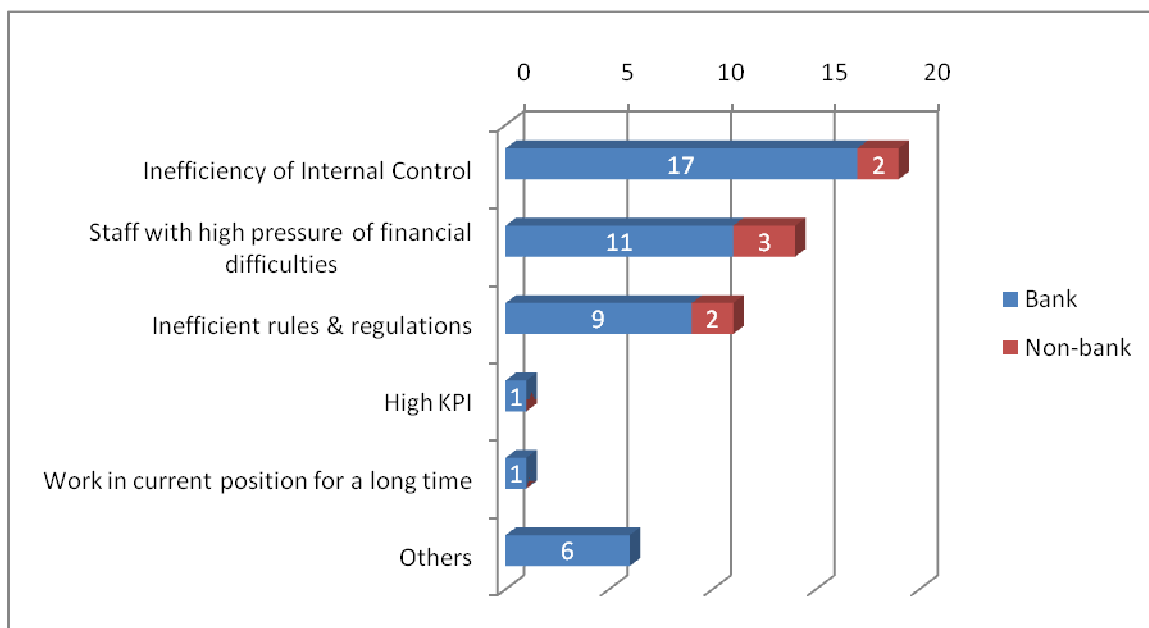
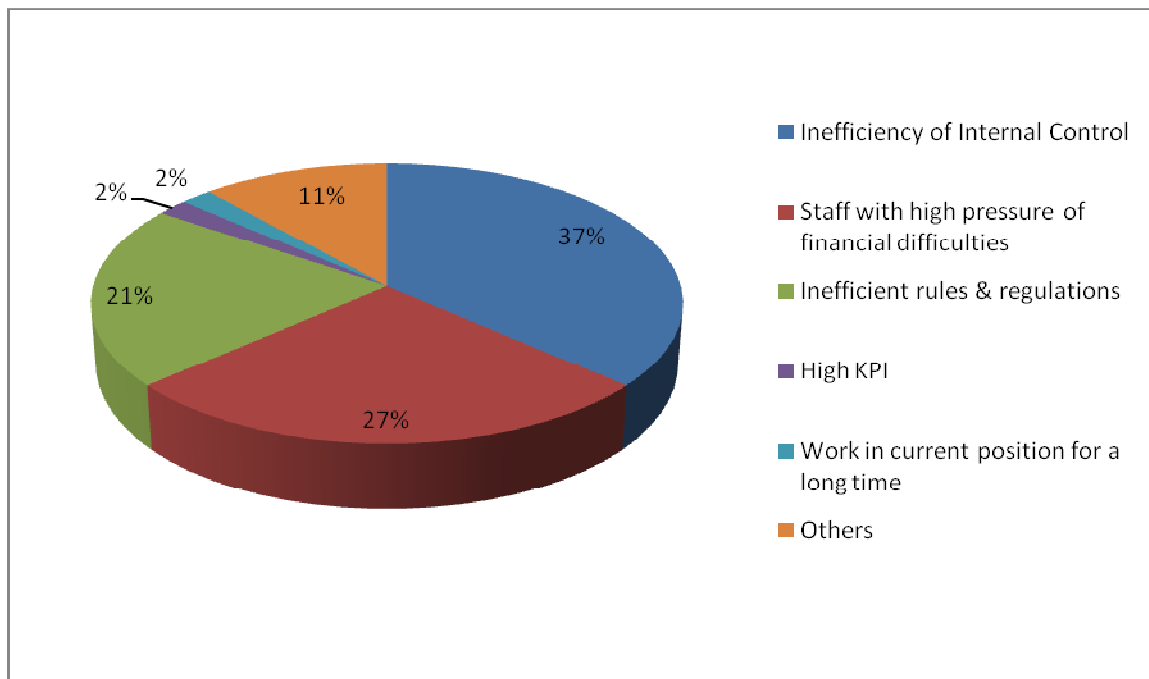
Survey of individual opinion and experience in dealing with fraud case in the organisation consists of three questions as follows:

1. What type of fraud do you most worry about in your organisation?

From the chart, twenty-one out of fifty-two are worried about fraud involving executives, while only four people are worried about cash theft and forgery endorsement.

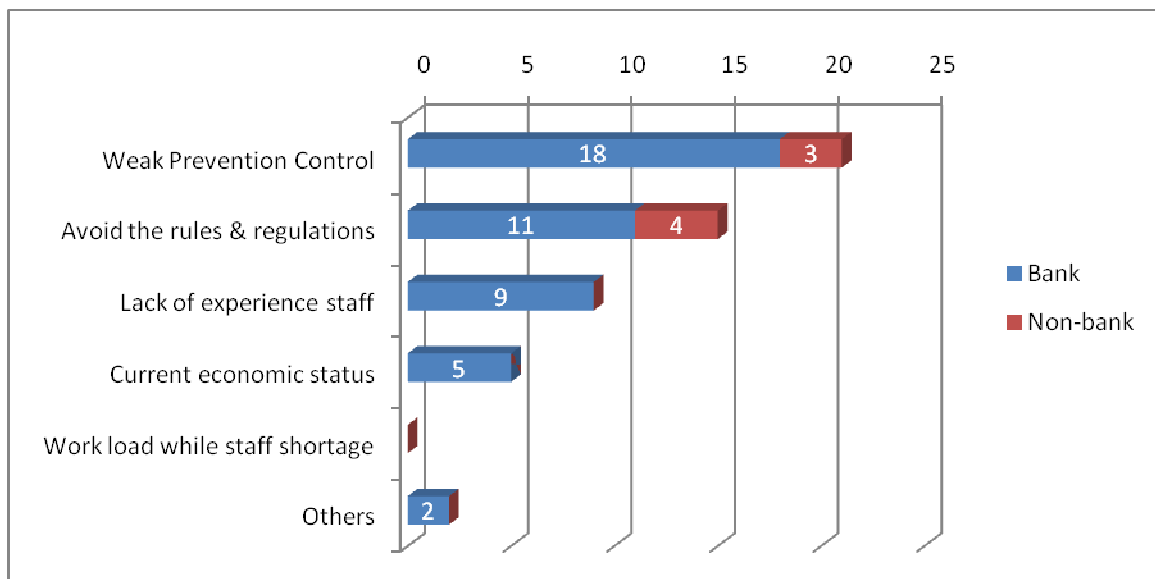
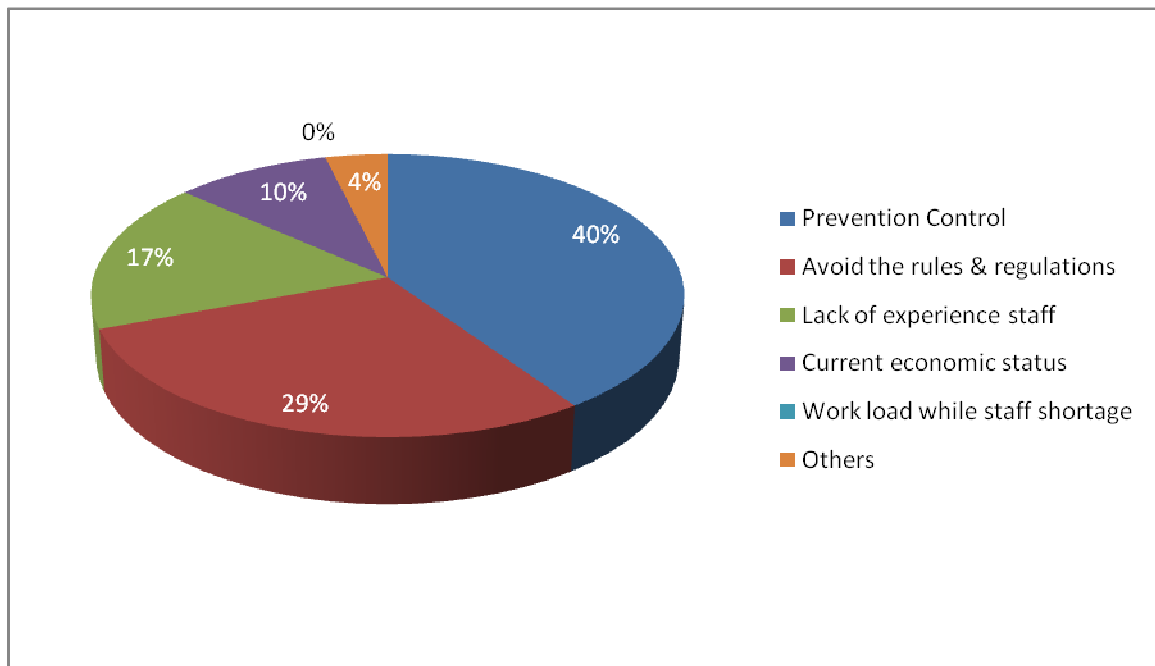


2. What is the primary cause of committing fraud by the organisational insiders?



The above table presents the number of participants, a total of 52 people, including bank and non-bank representatives. Seventeen bankers believe that the internal control of their organisation is not efficient. This is considered as a primary cause of committing fraud by internal staff. The participants believe that the organisational staff do not strictly or carefully follow the bank's rules and regulations. In addition, they also think that some staff do not have a good working motivation since they may be under significant pressure over their financial commitments. To prevent this circumstance, the bank should promote a code of conduct within the organisation. This will help create a positive working motivation among the staff.

3. What is the primary cause of committing fraud by outsiders / customers?



From above table, almost half of the participants consider weak prevention control as a primary cause of fraud committed by outsiders. Customers, who have some greed, may seek opportunity to commit fraud from a loophole that exists within the organisation.

Appendices

Details of survey results are presented in table below.

Commercial Loan

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| Section 1: Know Your Customer (KYC) | | | | | | 4.13 |
| 1 | Bank has in place, and properly follows, written Underwriting processes that check: The Customer Company and Its beneficial owners Its Management Its Related Companies | 2.82 | 0.50 | 0.75 | 0.65 | 4.72 |
| 2 | Bank has a Policy detailing: - requirements of customer's business in terms of quality and source of revenues (i.e. 'Target Market Definition') - minimum credit parameters and detailed rejection parameters | 2.82 | 0.50 | 0.75 | 0.55 | 4.62 |
| 3 | Fraud Blacklisting Capability | 2.72 | 0.43 | 0.75 | 0.65 | 4.56 |
| 4 | Face to Face meeting with customer (prior to submission of Credit Application for approval) an initial and regular SITE VISITS to monitor customer business health / adherence to credit conditions, etc. | 2.72 | 0.43 | 0.75 | 0.65 | 4.56 |
| 5 | A process to check to ensure that each approved deal conforms to the approved CRP (Credit Review Point) or Product Program | 2.82 | 0.37 | 0.75 | 0.6 | 4.53 |
| 6 | Bank has a process to identify and in more detail check out 'High Risk' customers, deals, transactions, for example unusual deal structures; timeline pressures; unusual repayment requests; asset refinancing; financing of specialist businesses in which we have nil or limited experience. | 2.54 | 0.43 | 0.75 | 0.65 | 4.37 |
| 7 | Clear segregation between Sales and Underwriting to avoid conflicts of interest otherwise inherent | 2.72 | 0.37 | 0.75 | 0.5 | 4.34 |
| 8 | Adopt properly legally-approved Contracts, that include protection of the Business in the event of fraud... and that | 2.58 | 0.30 | 0.75 | 0.6 | 4.23 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| | cannot be over-riden / altered without proper review / approval | | | | | |
| 9 | A consolidated view of each customer's TOTAL RELATIONSHIP with the Business, showing also any rejections by Bank (Underwriter / Credit Officer) on any / all PRIOR credit applications by that customer or by any of its beneficial owners / management / related companies (this is comparable to Consumer Banking 'De-dupe' controls) | 2.45 | 0.50 | 0.75 | 0.5 | 4.20 |
| 10 | Ability to Limit No. of loans to same name/address | 2.40 | 0.37 | 0.75 | 0.5 | 4.02 |
| 11 | Independent Credit Control / Admin function to carry out all initial and periodic checks and monitoring activities | 2.35 | 0.30 | 0.75 | 0.55 | 3.95 |
| 12 | Install KYC tool where sufficient applications available | 2.22 | 0.37 | 0.75 | 0.5 | 3.83 |
| 13 | Policy and resources deployed to carry out meaningful, regular, skilled and independent monitoring of financial performance, adherence to covenants, site visits, documented regular Call Reports from Sales, Exception Reports on deviations / deficiencies / breaches and suggested Corrective Actions showing any overdue / missed promises | 2.22 | 0.37 | 0.75 | 0.5 | 3.83 |
| 14 | - customer's justification of credit need / underlying transaction rationale - customer's reason for choosing Bank as credit provider | 2.26 | 0.37 | 0.75 | 0.45 | 3.83 |
| 15 | A process to both GENERATE and CAPTURE (from other Bank Businesses and from other Financial Institutions) 'Fraud Alerts' / Fraud Intelligence to minimize the possibility of falling victim to already-known fraud schemes. | 1.85 | 0.50 | 0.75 | 0.55 | 3.65 |
| 16 | Ability for system to capture (and permanently retain) underwriting decisions and data and to create relevant Exception Reports as required | 1.98 | 0.30 | 0.75 | 0.55 | 3.58 |
| 17 | Policy to protect the Business's interests and security in respect of cross-border lending or where the collateral is already, or may move, to another country | 1.85 | 0.37 | 0.75 | 0.4 | 3.36 |
| Section 2: Know Your Intermediary (KYI) using the KYI Framework | | | | | | 2.86 |
| 1 | Robust Intermediary accreditation process – See Compliance guidelines | 2.40 | 0.27 | 0.75 | 0.6 | 4.02 |
| 2 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and | 2.17 | 0.20 | 0.75 | 0.55 | 3.67 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--------------------------------------|---|------|----------|------|------|-------------|
| | all broker groups.. Checks that if Intermediary terminated then terminated across all Bank businesses / Products | | | | | |
| 3 | Segment and Monitor <i>Intermediary performance</i> by Underwriter and / or Sales rep in order to identify Red Flags / suspicious trends / transactions. | 1.71 | 0.27 | 0.75 | 0.65 | 3.37 |
| 4 | Monthly Reporting on Intermediaries using performance triggers as review point (i.e. Approval Rates, Write Offs (W/Os), Delinquencies, Business / Sales Volume, Red Flags, overdue deliverables / corrective action, etc. | 1.89 | 0.20 | 0.75 | 0.5 | 3.34 |
| 5 | Broker Fraud - Included in contract with broker is reimbursement for Internal Fraud. Or encourage broker to take out insurance for internal fraud. | 1.52 | 0.27 | 0.75 | 0.5 | 3.04 |
| 6 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. | 1.43 | 0.20 | 0.75 | 0.55 | 2.93 |
| 7 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level | 1.57 | 0.20 | 0.75 | 0.4 | 2.92 |
| 8 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit / site visit processes. | 1.52 | 0.20 | 0.45 | 0.55 | 2.72 |
| 9 | Carry out site visits prior to accreditation of Intermediaries | 1.62 | 0.20 | 0.45 | 0.45 | 2.72 |
| 10 | Monthly grading process must provide for termination of intermediaries depending on performance. If intermediary offers a range of products then intermediary should be terminated across all products. | 1.38 | 0.20 | 0.45 | 0.6 | 2.63 |
| 11 | KYI tool installed - i.e. Actimize | 1.25 | 0.13 | 0.75 | 0.4 | 2.53 |
| 12 | Credit of the intermediary or its financial health check should be obtained and review as an annual basis. | 1.52 | 0.13 | 0.45 | 0.3 | 2.41 |
| 13 | Reward scheme for Intermediaries who detect / warn us about fraud (i.e. reward, rather than punish, Good Behaviour). | 1.02 | 0.13 | 0.45 | 0.25 | 1.85 |
| 14 | Intermediaries have Public Indemnity Insurance to cover fraud committed by, or colluded in, by their staff | 1.38 | 0.20 | 0 | 0.25 | 1.83 |
| Section 3: Asset Verification | | | | | | 3.49 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| 1 | Bank Business has a clear Asset type Acceptability and Valuation Policy. This must define acceptable Asset types and Percentage Coverage; and a robust, independent (this doesn't necessarily mean external) reliable process to initially validate (and afterwards routinely monitor) any customer-supplied or customer-directed valuations. | 2.58 | 0.27 | 0.75 | 0.5 | 4.10 |
| 2 | Monthly quality control on sample of assets | 2.49 | 0.27 | 0.75 | 0.45 | 3.96 |
| 3 | Bank Business has a Policy, and an ongoing Monitoring Program, to ensure that adequate Insurance is at all times in place, and sufficient to reimburse the Bank Business, in the event of theft, loss, destruction or damage to the collateral Bank Business's interest in the policy to be noted on that policy). | 2.49 | 0.20 | 0.75 | 0.45 | 3.89 |
| 4 | In the event of the Bank Business's collateral could be sold, or used again as collateral, with good title but without that business's knowledge (e.g. where no restrictive lien can be recorded to encumber the asset), that risk must be disclosed as part of the credit application/approval and the monitoring program should be modified to mitigate that serious risk as much as it can be | 2.26 | 0.20 | 0.75 | 0.65 | 3.86 |
| 5 | Bank Business has an effective collateral database that uniquely identifies every relevant asset and shows its ownership and valuation history and any prior/current encumbrances | 2.49 | 0.27 | 0.75 | 0.35 | 3.86 |
| 6 | Drive By process on high risk assets | 2.26 | 0.33 | 0.75 | 0.45 | 3.79 |
| 7 | In the event prolonged deal negotiations, asset verification checks refreshed immediately before signing and prior to any pay-out | 2.31 | 0.27 | 0.75 | 0.45 | 3.77 |
| 8 | Create Valuation Panel comprising selected professionally qualified staff that have adequate PI (Professional Indemnity) insurance and a strong financial position | 2.26 | 0.27 | 0.75 | 0.45 | 3.73 |
| 9 | For Project Finance Bank business gets the assistance of appropriately qualified professional e.g. quantity surveyor to confirm customer's claims as to completeness of project/project state prior to pay out | 2.31 | 0.20 | 0.75 | 0.45 | 3.71 |
| 10 | Process that allows for lawful foreclosure and recovery of | 2.03 | 0.27 | 0.75 | 0.55 | 3.60 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| | assets / funds | | | | | |
| 11 | In the event the Bank Business becomes aware of any improper/illegal behaviour by the customer, the fraud/credit risk implications are properly/independently assessed, e.g. where tax penalties can lead to the authorities having a prior claim to company's assets | 2.12 | 0.27 | 0.75 | 0.35 | 3.49 |
| 12 | Process that allows for the clear establishment of Bank lien / charge against the title to the asset within a short time frame | 1.98 | 0.27 | 0.75 | 0.45 | 3.45 |
| 13 | Bank Business can deploy adequate expertise to reach out to assets owned by individuals in making claims under personal guarantees given that fraudulent transfer of assets frequently occurs | 2.08 | 0.27 | 0.75 | 0.35 | 3.44 |
| 14 | Bank Business pays special attention to situations where complex transfer pricing arrangements exist (especially relevant where there is intra-corporate transfer pricing) | 1.89 | 0.20 | 0.75 | 0.45 | 3.29 |
| 15 | Bank Business has a process to monitor and respond to environmental changes that would materially increase the risk of fraud | 2.03 | 0.27 | 0.45 | 0.45 | 3.20 |
| 16 | Checking against any national / industry registers that show current/prior charges (encumbrances) against those assets | 1.75 | 0.20 | 0.45 | 0.55 | 2.95 |
| 17 | Fraud Recoveries process in addition to 'normal' recoveries | 1.48 | 0.20 | 0.75 | 0.45 | 2.88 |
| 18 | Bank Business has deployed GPS tracking equipment or such like technical equipment to flag unauthorised movement of mobile assets and/or to assist in their recovery in the event of theft, consider secret (covert) deployment where lawfully allowed | 1.25 | 0.27 | 0 | 0.25 | 1.76 |
| Section 4: Revolving Fund - Re draw ability | | | | | | 2.12 |
| 1 | The Bank Business has in place processes /controls to minimize the fraud risks associated with large available undrawn credit facilities (e.g. account takeover, fraud in fund transfers etc.) | 1.52 | 0.27 | 0 | 0.35 | 2.14 |
| 2 | Company/Account Takeover Controls: Ability to identify high risk transactions and create Exception Report and/or customer mandate changes (I.e. those authorised to sign for the customer company and any restrictions on their authorities/signing rights) | 1.38 | 0.27 | 0 | 0.45 | 2.10 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| | | | | | | |
| Section 5: Know Your Staff (KYS) | | | | | | 3.16 |
| 1 | Background Employment Screening (See HR guidelines & Also check financial status of employees on an annual basis to ensure they are not in a financial pressure) | 2.40 | 0.33 | 0.75 | 0.55 | 4.03 |
| 2 | ISM (Investigation & Security Manager) Capability with Feedback loop to Prevention | 2.08 | 0.33 | 0.75 | 0.5 | 3.66 |
| 3 | Separate approval process and review process for Staff accounts | 1.98 | 0.33 | 0.75 | 0.55 | 3.62 |
| 4 | Exception Reporting identifying accounts that are High Risk for internal fraud | 1.75 | 0.27 | 0.75 | 0.55 | 3.32 |
| 5 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually | 1.75 | 0.27 | 0.75 | 0.5 | 3.27 |
| 6 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should neither maintain their own (customer) account nor maintain a related parties (customer) account. | 1.66 | 0.20 | 0.75 | 0.5 | 3.11 |
| 7 | Can employees access into other banks beyond the bank they are working for? | 1.40 | 0.20 | 0.75 | 0.4 | 2.75 |
| 8 | Ability to identify staff accounts. Monitor staff and related party accounts for internal fraud | 1.48 | 0.27 | 0.45 | 0.45 | 2.64 |
| 9 | Business has in place an appropriate process to reward Sales, Underwriting and other staff for reducing fraud risk/loss | 1.38 | 0.27 | 0.45 | 0.45 | 2.55 |
| 10 | Installation of KYS tool - e.g. Intellinx/Footprint | 1.52 | 0.20 | 0.45 | 0.3 | 2.47 |
| Section 6: 3rd Party Payments / Disbursements | | | | | | 1.91 |
| 1 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid | 1.52 | 0.27 | 0 | 0.4 | 2.19 |
| 2 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns | 1.34 | 0.27 | 0 | 0.55 | 2.16 |
| 3 | Payments to dealers / suppliers against full documentation | 1.43 | 0.27 | 0 | 0.4 | 2.10 |
| 4 | Match bank payment details to staff bank accounts | 1.25 | 0.27 | 0 | 0.55 | 2.06 |
| 5 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 1.25 | 0.27 | 0 | 0.45 | 1.96 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| 6 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier | 1.11 | 0.27 | 0 | 0.4 | 1.77 |
| 7 | Ability to identify multiple dealer / supplier payment details to same bank account | 1.02 | 0.27 | 0 | 0.3 | 1.58 |
| 8 | Review triggers for \$ payments by dealer / supplier type | 0.88 | 0.27 | 0 | 0.3 | 1.44 |
| Section 7: Reporting | | | | | | 3.30 |
| 1 | Fraud cases reported to the bank's head quarter. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. | 2.08 | 0.33 | 0.75 | 0.75 | 3.91 |
| 2 | Fraud Prevention/Detection/ Losses analyzed and reported by process weakness. | 1.94 | 0.27 | 0.75 | 0.65 | 3.61 |
| 3 | Monthly reporting: Gross/Net Fraud; Fraud triggers driven fraud budget ; Fraud to Write off, Fraud to NI, W/O no payments- in line with business plan. | 1.98 | 0.27 | 0.75 | 0.55 | 3.55 |
| 4 | Key underwriting and transaction data tracked and used for fraud analysis. | 1.94 | 0.27 | 0.75 | 0.5 | 3.46 |
| 5 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. | 1.80 | 0.27 | 0.75 | 0.6 | 3.42 |
| 6 | Exception reports for high risk transactions. | 1.85 | 0.20 | 0.75 | 0.6 | 3.40 |
| 7 | Fraud Prevention/Detection/ Losses broken down by fraud type. | 1.71 | 0.27 | 0.75 | 0.65 | 3.37 |
| 8 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. | 1.80 | 0.27 | 0.75 | 0.5 | 3.32 |
| 9 | Monthly reports relevant to fraud trends and observations. | 1.71 | 0.20 | 0.75 | 0.55 | 3.21 |
| 10 | Fraud case management report including the progression and follow-up of fraud investigation, and exchange of fraud information/news. In addition, fraud cases should be reported to the Bank of Thailand. | 1.52 | 0.27 | 0.75 | 0.55 | 3.09 |
| 11 | Monthly reports including follow-up action Items. | 1.66 | 0.27 | 0.45 | 0.65 | 3.03 |
| 12 | Fraud Prevention/Detection/ Losses broken down by portfolio. | 1.75 | 0.27 | 0.45 | 0.55 | 3.02 |
| 13 | Variance analysis and development of control charts. | 1.43 | 0.27 | 0.45 | 0.4 | 2.55 |
| Section 8: Operational Efficiency | | | | | | 3.32 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| 1 | Conducting the review by Internal Audit or independent 3rd party should be in place. | 2.54 | 0.20 | 0.75 | 0.5 | 3.99 |
| 2 | Formalized write-off police and procedure should be in place. | 2.45 | 0.27 | 0.75 | 0.5 | 3.96 |
| 3 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. | 2.17 | 0.33 | 0.75 | 0.65 | 3.90 |
| 4 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. | 2.45 | 0.27 | 0.75 | 0.4 | 3.86 |
| 5 | Formalized fraud policy and procedure should be developed. | 2.22 | 0.33 | 0.75 | 0.5 | 3.80 |
| 6 | Data leakage from both paper-based and electronic-based should be controlled. | 2.17 | 0.33 | 0.75 | 0.45 | 3.70 |
| 7 | Well publicize whistle blower program should be one of channels to report fraud case at anytime. Moreover, a case management process to deal with the reported issues should be developed. | 2.22 | 0.20 | 0.75 | 0.5 | 3.67 |
| 8 | Fraud analyst should analyze fraud losses and review rule sets in fraud detection tools on an ongoing basis. | 1.98 | 0.27 | 0.75 | 0.55 | 3.55 |
| 9 | The procedure for fraud alert process across industry peers should be developed. | 1.98 | 0.27 | 0.75 | 0.55 | 3.55 |
| 10 | Random checks for underwriting process compliance should be performed. | 2.08 | 0.20 | 0.75 | 0.5 | 3.53 |
| 11 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. | 1.98 | 0.20 | 0.75 | 0.55 | 3.48 |
| 12 | Fraud training programs should be conducted for Underwriting staff. | 1.80 | 0.27 | 0.75 | 0.65 | 3.47 |
| 13 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. | 1.85 | 0.27 | 0.75 | 0.6 | 3.46 |
| 14 | Fraud prevention awareness should be raised and communicated regularly in the management level. | 1.89 | 0.33 | 0.75 | 0.45 | 3.43 |
| 15 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. | 1.75 | 0.33 | 0.75 | 0.55 | 3.39 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------------------------------------|--|------|----------|------|------|-------------|
| 16 | Bad debt written off that is collected from customers in later period should be controlled. | 1.98 | 0.20 | 0.75 | 0.4 | 3.33 |
| 17 | 100% review of high risk application or accounts should be conducted. For example, - 3PD or 2PD with no customer contact - Accounts that are potentially "Skip" accounts < 210 days on book - Accounts where mail has been returned from the outset of the account opening. | 1.85 | 0.20 | 0.75 | 0.45 | 3.25 |
| 18 | Code of conduct should include clear definition of fraud. | 1.85 | 0.20 | 0.75 | 0.45 | 3.25 |
| 19 | The members of the Fraud team should consist of staff from Operations and Analytics. | 1.89 | 0.33 | 0.45 | 0.55 | 3.23 |
| 20 | Fraud detection methods should be tailored to needs of individual portfolio. | 1.71 | 0.27 | 0.75 | 0.4 | 3.12 |
| 21 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. | 1.38 | 0.27 | 0.75 | 0.55 | 2.95 |
| 22 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. | 1.43 | 0.20 | 0.75 | 0.55 | 2.93 |
| 23 | Fraud Coordinator should ensure that 'Close the loop' process is finalized. | 1.57 | 0.33 | 0.75 | 0.25 | 2.90 |
| 24 | Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit. | 1.57 | 0.33 | 0.45 | 0.55 | 2.90 |
| 25 | Fraud awareness training should be provided to employees at least every six months. | 1.57 | 0.20 | 0.45 | 0.45 | 2.67 |
| 26 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. | 1.25 | 0.13 | 0.45 | 0.35 | 2.18 |
| 27 | Employee's KPIs should be established based on the risk associated with their tasks. | 1.11 | 0.00 | 0.45 | 0.5 | 2.06 |
| Section 9: Fraud Technology | | | | | | 2.55 |
| 1 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. | 1.52 | 0.33 | 0.75 | 0.65 | 3.26 |
| 2 | Fraud technology should be deployed to combat internal fraud. | 1.75 | 0.27 | 0.75 | 0.4 | 3.17 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| 3 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. | 1.66 | 0.20 | 0.75 | 0.55 | 3.16 |
| 4 | Fraud technology should be compatible with existing core banking system. | 1.75 | 0.27 | 0.45 | 0.6 | 3.07 |
| 5 | Banks should implement case management tool with workflow capability. | 1.66 | 0.33 | 0.45 | 0.5 | 2.94 |
| 6 | Fraud technology should be deployed to combat external fraud. | 1.52 | 0.27 | 0.75 | 0.4 | 2.94 |
| 7 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. | 1.38 | 0.27 | 0.75 | 0.5 | 2.90 |
| 8 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. | 1.57 | 0.27 | 0.45 | 0.5 | 2.79 |
| 9 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. | 1.43 | 0.33 | 0.45 | 0.5 | 2.71 |
| 10 | Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management. | 1.25 | 0.27 | 0.75 | 0.45 | 2.71 |
| 11 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week. | 1.15 | 0.33 | 0.75 | 0.45 | 2.69 |
| 12 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. | 1.15 | 0.27 | 0.75 | 0.45 | 2.62 |
| 13 | Fraud technology should allows banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. | 1.43 | 0.33 | 0.45 | 0.4 | 2.61 |
| 14 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. | 1.34 | 0.27 | 0.75 | 0.25 | 2.61 |
| 15 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. | 1.29 | 0.33 | 0.45 | 0.5 | 2.58 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| 16 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. | 1.38 | 0.27 | 0.45 | 0.45 | 2.55 |
| 17 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyze and alert the responsible people in case of any unusual transactions or suspicious behaviour. | 1.43 | 0.27 | 0.45 | 0.4 | 2.55 |
| 18 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. | 1.25 | 0.33 | 0.45 | 0.5 | 2.53 |
| 19 | Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. | 1.25 | 0.20 | 0.75 | 0.3 | 2.50 |
| 20 | Banks should implement pre-built software specifically for fraud detection technology. | 1.20 | 0.33 | 0.45 | 0.5 | 2.48 |
| 21 | Fraud detection solution should process efficiently and respond back within targeted period. | 1.11 | 0.33 | 0.45 | 0.55 | 2.44 |
| 22 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. | 1.34 | 0.20 | 0.45 | 0.45 | 2.44 |
| 23 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. | 0.97 | 0.27 | 0.75 | 0.45 | 2.44 |
| 24 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. | 0.88 | 0.20 | 0.75 | 0.55 | 2.38 |
| 25 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. | 1.06 | 0.27 | 0.45 | 0.45 | 2.23 |
| 26 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. | 1.06 | 0.27 | 0.45 | 0.4 | 2.18 |
| 27 | Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide faster and efficient support. | 0.97 | 0.20 | 0.45 | 0.5 | 2.12 |
| 28 | False positives created from the current technology should be reduced due to poor data quality. | 1.11 | 0.27 | 0 | 0.65 | 2.02 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| 29 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. | 1.34 | 0.27 | 0 | 0.35 | 1.96 |
| 30 | Banks should update fraud detection techniques regularly, at least once a month. | 0.88 | 0.20 | 0.45 | 0.25 | 1.78 |
| 31 | The pre-built data model should be created for the bank's existing systems. | 1.06 | 0.27 | 0 | 0.4 | 1.73 |

Hire Purchase

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| Section 1: Know Your Customer (KYC) | | | | | | 3.85 |
| 1 | Underwriting Policy noting : ID verification procedure, : employment/income verification procedure : address verification procedure : phone verification procedure : weighted bureau data | 2.94 | 0.46 | 0.75 | 0.7 | 4.86 |
| 2 | Fraud Blacklisting Capability | 2.72 | 0.46 | 0.75 | 0.65 | 4.58 |
| 3 | Centrally located underwriting, segregation between Sales and Underwriting Teams | 2.65 | 0.38 | 0.75 | 0.65 | 4.43 |
| 4 | High value Fraud alerts to other portfolio's at country level | 2.50 | 0.45 | 0.75 | 0.6 | 4.29 |
| 5 | Conforms to CRP as signed off | 2.53 | 0.33 | 0.75 | 0.65 | 4.25 |
| 6 | Face to Face meeting with customer (signing phase) for Vehicle | 2.50 | 0.43 | 0.75 | 0.55 | 4.22 |
| 7 | If business operates via Intermediaries then must have documented process to audit KYC checks conducted by intermediary | 2.30 | 0.43 | 0.75 | 0.6 | 4.08 |
| 8 | Approved methodology for high Risk designation using historical data and current fraud trends | 2.22 | 0.41 | 0.75 | 0.65 | 4.03 |
| 9 | Ability for system to capture underwriting data (create relevant Exception reports as required) | 2.16 | 0.39 | 0.75 | 0.65 | 3.95 |
| 10 | Install KYC tool | 2.29 | 0.35 | 0.75 | 0.55 | 3.94 |
| 11 | Utilize high risk profiles for additional targeting | 2.12 | 0.37 | 0.75 | 0.55 | 3.79 |
| 12 | Validated address/phone number through public databases | 2.36 | 0.37 | 0.45 | 0.55 | 3.73 |
| 13 | Policy around Foreign Nationals | 2.00 | 0.37 | 0.75 | 0.55 | 3.67 |
| 14 | Install Fraud Scorecard | 2.07 | 0.29 | 0.75 | 0.25 | 3.36 |
| 15 | De-Duplicate application process (approved and declined apps) | 1.80 | 0.40 | 0.45 | 0.55 | 3.20 |
| 16 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 2.09 | 0.41 | 0.15 | 0.5 | 3.15 |
| 17 | Approved policy limiting no. of loans to same family/same address | 1.49 | 0.25 | 0.45 | 0.4 | 2.59 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| 18 | No 2 nd deal to be approved before 1 st loan payment cleared. | 1.31 | 0.26 | 0.45 | 0.25 | 2.28 |
| Section 2: Know Your Intermediary (KYI) using the KYI Framework | | | | | | 3.49 |
| 1 | Robust Intermediary accreditation process – See Compliance guidelines | 2.71 | 0.39 | 0.75 | 0.6 | 4.45 |
| 2 | Segment and Monitor by underwriter and/or Sales rep | 2.47 | 0.43 | 0.75 | 0.65 | 4.30 |
| 3 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups.. Checks that if Intermediary terminated then terminated across all intermediary listings. | 2.68 | 0.36 | 0.75 | 0.5 | 4.29 |
| 4 | Intermediary Fraud - Included in contract with Intermediary is reimbursement for Internal Fraud. Or encourage Intermediary to take out insurance for internal fraud. | 2.29 | 0.39 | 0.75 | 0.5 | 3.93 |
| 5 | Monthly Reporting on Intermediaries using performance triggers as review point i.e. Approval rate, W/O's, 3PD, Sales volume, delinquency, TTY, Fraud Loss. | 2.23 | 0.35 | 0.75 | 0.55 | 3.88 |
| 6 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level | 2.05 | 0.39 | 0.75 | 0.4 | 3.59 |
| 7 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. | 1.95 | 0.34 | 0.75 | 0.55 | 3.59 |
| 8 | Perform site visitation prior to accreditation of broker | 1.93 | 0.37 | 0.75 | 0.45 | 3.50 |
| 9 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. | 1.91 | 0.39 | 0.45 | 0.55 | 3.30 |
| 10 | Credit of the intermediary or its financial health check should be obtained and review as an annual basis. | 2.12 | 0.32 | 0.45 | 0.35 | 3.24 |
| 11 | Monthly grading process must provide for closure of intermediaries depending on Performance | 1.86 | 0.27 | 0.45 | 0.6 | 3.18 |
| 12 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 2.01 | 0.35 | 0.45 | 0.35 | 3.16 |
| 13 | KYI tool installed - i.e. Actimize | 1.55 | 0.30 | 0.75 | 0.4 | 3.00 |
| 14 | Intermediaries have PI Insurance to cover Intermediary fraud | 1.90 | 0.32 | 0.45 | 0.25 | 2.92 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|---|--|------|----------|------|------|-------------|
| Section 3: Asset Verification | | | | | | 3.61 |
| 1 | Clearly defined asset type that will be eligible for loans, Caps on extra's as defined by policy | 2.36 | 0.38 | 0.75 | 0.45 | 3.94 |
| 2 | Prevent/monitor for forward sale of asset by customer | 2.27 | 0.35 | 0.75 | 0.55 | 3.92 |
| 3 | Process that allows clear title registration over asset within a set time frame i.e. check of Engine No., registration etc | 2.48 | 0.37 | 0.45 | 0.55 | 3.86 |
| 4 | If asset is not registered prior to disbursement then audit to ensure asset is secured within prescribed time frame | 2.22 | 0.33 | 0.75 | 0.55 | 3.85 |
| 5 | Provide Plan for ability to identify 'at risk' accounts where asset may be on sold without finalizing settlement | 2.12 | 0.32 | 0.75 | 0.65 | 3.84 |
| 6 | Auto Asset Verification (AAV) compliant - Outbound verification calls made directly to customer - may be sample based on risk modeling of dealers | 2.16 | 0.33 | 0.75 | 0.55 | 3.79 |
| 7 | Independent Asset validation process - valuation checked through independent database i.e. Database with range of prices for new and used vehicles by make and model | 2.25 | 0.36 | 0.45 | 0.65 | 3.71 |
| 8 | For inventory finance, regular vehicle inspection and random checks | 2.26 | 0.29 | 0.75 | 0.35 | 3.65 |
| 9 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 1.98 | 0.35 | 0.45 | 0.45 | 3.23 |
| Section 4: Know Your Staff (KYS) | | | | | | 3.37 |
| 1 | IT Security where system access is dictated by role | 2.65 | 0.43 | 0.75 | 0.55 | 4.38 |
| 2 | ISM Capability with Feedback loop to Prevention | 2.44 | 0.43 | 0.75 | 0.55 | 4.17 |
| 3 | Monitor staff and related party accounts for internal fraud - Monitor monthly approval rates and write offs by individual staff (Sales, U/writing and Collections staff) | 2.30 | 0.41 | 0.75 | 0.45 | 3.91 |
| 4 | Background Employment Screening (See HR guidelines) (Also check financial status of employees on an annual basis to ensure they are not in a financial pressure) | 2.25 | 0.39 | 0.75 | 0.45 | 3.84 |
| 5 | Separate approval process and review process for Staff accounts | 2.04 | 0.34 | 0.75 | 0.55 | 3.67 |
| 6 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 1.90 | 0.35 | 0.45 | 0.45 | 3.15 |
| 7 | Installation of KYS tool - Intellinx/Footprint | 1.88 | 0.45 | 0.45 | 0.25 | 3.03 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| 8 | Can employees access into other banks beyond the bank they are working for? | 1.73 | 0.39 | 0.45 | 0.45 | 3.02 |
| 9 | Review process for Staff receiving Sales bonus's | 1.87 | 0.34 | 0.45 | 0.35 | 3.01 |
| 10 | Ability to identify staff accounts. | 1.87 | 0.37 | 0.15 | 0.45 | 2.84 |
| Section 5: 3rd Party Payments / Disbursements | | | | | | 3.40 |
| 1 | Payments to dealers against full documentation | 2.58 | 0.37 | 0.75 | 0.4 | 4.10 |
| 2 | Payments directly to dealer, not to customer with expectation that supplier is paid | 2.44 | 0.30 | 0.75 | 0.4 | 3.89 |
| 3 | Robust process for registration of new supplier | 2.29 | 0.37 | 0.75 | 0.4 | 3.81 |
| 4 | Ability to identify multiple supplier payment details to same bank account | 2.15 | 0.34 | 0.75 | 0.2 | 3.44 |
| 5 | Independent checking/confirmation when notified of changes to payment details of supplier | 2.04 | 0.34 | 0.75 | 0.3 | 3.42 |
| 6 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns | 2.05 | 0.37 | 0.45 | 0.45 | 3.32 |
| 7 | Review triggers for \$ payments by supplier type | 1.95 | 0.27 | 0.75 | 0.3 | 3.28 |
| 8 | Match bank payment details to staff bank accounts | 2.00 | 0.35 | 0.45 | 0.45 | 3.25 |
| 9 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 1.88 | 0.37 | 0.45 | 0.35 | 3.06 |
| Section 6: Reporting | | | | | | 3.57 |
| 1 | Fraud cases reported to the bank's head quarter. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. | 2.33 | 0.35 | 0.75 | 0.75 | 4.18 |
| 2 | Monthly reporting: Gross/Net Fraud; Fraud to Sales ; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O no payments, Skip/Trace <90MOB; Fraud savings, Investigation, Recoveries> | 2.30 | 0.43 | 0.75 | 0.55 | 4.03 |
| 3 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. | 2.27 | 0.41 | 0.75 | 0.55 | 3.98 |
| 4 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of | 2.16 | 0.40 | 0.75 | 0.55 | 3.86 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| | benchmark for each bank, for example, capital, net asset, and net revenue. | | | | | |
| 5 | Fraud Prevention/Detection/ Losses analyzed and reported by process weakness. | 2.19 | 0.29 | 0.45 | 0.65 | 3.58 |
| 6 | Fraud Prevention/Detection/ Losses broken down by fraud type. | 2.16 | 0.27 | 0.45 | 0.65 | 3.54 |
| 7 | Monthly reports relevant to fraud trends and observations. | 2.09 | 0.37 | 0.45 | 0.55 | 3.47 |
| 8 | Fraud Prevention/Detection/ Losses broken down by portfolio. | 2.13 | 0.32 | 0.45 | 0.55 | 3.45 |
| 9 | Monthly reports including follow-up action items. | 1.94 | 0.34 | 0.45 | 0.65 | 3.38 |
| 10 | Variance analysis and development of control charts. | 1.69 | 0.32 | 0.45 | 0.45 | 2.91 |
| Section 7: Operational Efficiency | | | | | | 3.40 |
| 1 | Data leakage from both paper-based and electronic-based should be controlled. | 2.58 | 0.36 | 0.75 | 0.65 | 4.35 |
| 2 | Formalized fraud policy and procedure should be developed. | 2.39 | 0.48 | 0.75 | 0.55 | 4.17 |
| 3 | Centrally located underwriting with documented check list of loans should be in place. | 2.48 | 0.41 | 0.75 | 0.45 | 4.09 |
| 4 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. | 2.22 | 0.46 | 0.75 | 0.65 | 4.08 |
| 5 | Formalized write-off policy and procedure should be in place. | 2.37 | 0.41 | 0.75 | 0.55 | 4.08 |
| 6 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. | 2.32 | 0.41 | 0.75 | 0.55 | 4.03 |
| 7 | Fraud analyst should analyze fraud losses and review rule sets in fraud detection tools on an ongoing basis. | 2.16 | 0.39 | 0.75 | 0.55 | 3.85 |
| 8 | Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit. | 2.34 | 0.46 | 0.45 | 0.55 | 3.81 |
| 9 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. | 2.36 | 0.41 | 0.45 | 0.55 | 3.77 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| 10 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. | 2.01 | 0.42 | 0.75 | 0.55 | 3.73 |
| 11 | Code of conduct should include clear definition of fraud. | 2.05 | 0.37 | 0.75 | 0.55 | 3.72 |
| 12 | Random checks for underwriting process compliance should be performed. | 2.36 | 0.34 | 0.45 | 0.55 | 3.69 |
| 13 | Fraud training programs should be conducted for Underwriting staff. | 2.15 | 0.41 | 0.45 | 0.65 | 3.66 |
| 14 | Involvement/sign off in CRP and new product innovations (NPI) process | 2.08 | 0.34 | 0.75 | 0.45 | 3.62 |
| 15 | Fraud Coordinator should be assigned to coordinate between Fraud Risk Manager and ISM. Moreover, regular meeting between these two groups should be arranged to ensure open communication and close gaps. | 2.01 | 0.37 | 0.75 | 0.45 | 3.58 |
| 16 | Well publicize whistle blower program should be one of channels to report fraud case at anytime. Moreover, a case management process to deal with the reported issues should be developed. | 2.20 | 0.34 | 0.45 | 0.55 | 3.54 |
| 17 | Fraud detection methods should be tailored to needs of individual portfolio. | 2.04 | 0.30 | 0.75 | 0.45 | 3.54 |
| 18 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. | 2.01 | 0.41 | 0.45 | 0.65 | 3.52 |
| 19 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. | 2.09 | 0.41 | 0.45 | 0.55 | 3.50 |
| 20 | Key underwriting and transaction data should be tracked and used for fraud analysis. | 2.04 | 0.41 | 0.45 | 0.55 | 3.45 |
| 21 | Fraud prevention awareness should be raised and communicated regularly in the management level. | 2.01 | 0.35 | 0.45 | 0.55 | 3.36 |
| 22 | Bad debt written off that is collected from customers in later period should be controlled. | 1.98 | 0.33 | 0.45 | 0.45 | 3.21 |
| 23 | The members of the Fraud team should consist of staff from Operations and Analytics. | 1.98 | 0.32 | 0.45 | 0.45 | 3.20 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------------------------------------|---|------|----------|------|------|-------------|
| 24 | The procedure for fraud alert process across industry peers should be developed. | 1.83 | 0.34 | 0.45 | 0.55 | 3.16 |
| 25 | Bi-Annual Auditing Processes are in place where degree of conformance to standards is measured and recorded. | 1.83 | 0.39 | 0.45 | 0.45 | 3.12 |
| 26 | Fraud awareness training should be provided to employees at least every six months. | 1.72 | 0.28 | 0.45 | 0.55 | 3.00 |
| 27 | Employee's KPIs should be established based on the risk associated with their tasks. | 1.74 | 0.34 | 0.45 | 0.45 | 2.98 |
| 28 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. | 1.55 | 0.28 | 0.45 | 0.25 | 2.53 |
| Section 8: Fraud Technology | | | | | | 3.30 |
| 1 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. | 2.18 | 0.45 | 0.75 | 0.55 | 3.92 |
| 2 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. | 1.93 | 0.46 | 0.75 | 0.65 | 3.79 |
| 3 | Fraud technology should be deployed to combat external fraud. | 2.15 | 0.41 | 0.75 | 0.4 | 3.71 |
| 4 | Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management. | 1.94 | 0.40 | 0.75 | 0.55 | 3.64 |
| 5 | Fraud technology should be compatible with existing core banking system. | 2.13 | 0.45 | 0.45 | 0.6 | 3.63 |
| 6 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week. | 1.98 | 0.48 | 0.75 | 0.4 | 3.61 |
| 7 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. | 1.91 | 0.39 | 0.75 | 0.55 | 3.60 |
| 8 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. | 2.01 | 0.39 | 0.75 | 0.45 | 3.60 |
| 9 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. | 2.00 | 0.39 | 0.75 | 0.45 | 3.59 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| 10 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. | 2.19 | 0.45 | 0.45 | 0.5 | 3.59 |
| 11 | Fraud technology should be deployed to combat internal fraud. | 2.05 | 0.38 | 0.75 | 0.4 | 3.58 |
| 12 | Banks should implement case management tool with workflow capability. | 2.15 | 0.43 | 0.45 | 0.5 | 3.53 |
| 13 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. | 2.11 | 0.43 | 0.45 | 0.5 | 3.48 |
| 14 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. | 1.86 | 0.37 | 0.75 | 0.5 | 3.48 |
| 15 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. | 2.12 | 0.45 | 0.45 | 0.45 | 3.47 |
| 16 | Banks should implement pre-built software specifically for fraud detection technology. | 2.04 | 0.45 | 0.45 | 0.5 | 3.43 |
| 17 | Fraud detection solution should process efficiently and respond back within targeted period. | 1.91 | 0.43 | 0.45 | 0.6 | 3.39 |
| 18 | Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. | 1.73 | 0.43 | 0.75 | 0.45 | 3.36 |
| 19 | Fraud technology should allows banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. | 1.94 | 0.45 | 0.45 | 0.4 | 3.23 |
| 20 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. | 1.59 | 0.43 | 0.75 | 0.45 | 3.22 |
| 21 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. | 1.93 | 0.34 | 0.45 | 0.5 | 3.21 |
| 22 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, | 1.91 | 0.45 | 0.45 | 0.35 | 3.16 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| | Load) tool. | | | | | |
| 23 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. | 1.73 | 0.45 | 0.45 | 0.5 | 3.13 |
| 24 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyze and alert the responsible people in case of any unusual transactions or suspicious behaviour. | 1.83 | 0.43 | 0.45 | 0.4 | 3.11 |
| 25 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. | 1.80 | 0.45 | 0.45 | 0.4 | 3.10 |
| 26 | Banks should update fraud detection techniques regularly, at least once a month. | 1.97 | 0.43 | 0.45 | 0.25 | 3.09 |
| 27 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. | 2.04 | 0.34 | 0.45 | 0.25 | 3.07 |
| 28 | Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide faster and efficient support. | 1.60 | 0.35 | 0.45 | 0.5 | 2.91 |
| 29 | The pre-built data model should be created for the bank's existing systems. | 1.81 | 0.35 | 0 | 0.45 | 2.62 |
| 30 | False positives created from the current technology should be reduced due to poor data quality. | 1.62 | 0.32 | 0 | 0.65 | 2.59 |
| 31 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. | 1.77 | 0.31 | 0 | 0.35 | 2.43 |

Merchant

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| Section 1: Know Your Customer (KYC) | | | | | | 3.74 |
| 1 | Underwriting Policy noting : ID verification procedure , predefined acceptable documents : ID verification procedure for merchant (Approved designees) : employment/income verification procedure : address verification procedure : phone verification procedure, e.g. no third party phones for 0% down payment : weighted bureau data | 3.00 | 0.50 | 0.75 | 0.75 | 5.00 |
| 2 | If business operates via Intermediaries then must have documented process to audit KYC checks conducted by intermediary | 3.00 | 0.50 | 0.75 | 0.6 | 4.85 |
| 3 | Conforms to CRP (Credit Review Point) as signed off | 3.00 | 0.30 | 0.75 | 0.65 | 4.70 |
| | Policy around Foreign Nationals | 2.83 | 0.50 | 0.75 | 0.55 | 4.63 |
| 4 | Fraud Blacklisting Capability | 2.83 | 0.30 | 0.75 | 0.65 | 4.53 |
| 5 | Centrally located underwriting, segregation between Sales and Underwriting Teams | 2.66 | 0.30 | 0.75 | 0.65 | 4.36 |
| 6 | Utilize high risk profiles for additional targeting | 2.66 | 0.30 | 0.75 | 0.55 | 4.26 |
| | High value Fraud alerts to other portfolio's at country level | 2.49 | 0.30 | 0.75 | 0.6 | 4.14 |
| 7 | Ability for system to capture underwriting data (create relevant Exception reports as required) | 2.40 | 0.30 | 0.75 | 0.65 | 4.10 |
| 8 | De-Dupe process (approved and declined apps) | 2.23 | 0.30 | 0.75 | 0.5 | 3.78 |
| 9 | Install KYC tool where sufficient data available | 2.14 | 0.30 | 0.75 | 0.55 | 3.74 |
| | Use of subjective negative codes from point of sale merchants/ intermediary | 2.14 | 0.30 | 0.75 | 0.5 | 3.69 |
| 10 | Validated address/phone number through public databases | 2.14 | 0.50 | 0.45 | 0.55 | 3.64 |
| 11 | Approved methodology for High Risk designation using historical data and current fraud trends | 1.63 | 0.30 | 0.45 | 0.65 | 3.03 |
| 12 | Remote Channel - Internet Apps : Ability to identify high risk applications using relevant session data (i.e. geo-location data/ IP address or other PC | 1.80 | 0.50 | 0 | 0.35 | 2.65 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| | device ID) | | | | | |
| | Install Fraud Scorecard where sufficient data available | 1.71 | 0.30 | 0 | 0.25 | 2.26 |
| 13 | No 2nd deal to be approved before 1st loan payment cleared. | 1.46 | 0.30 | 0 | 0.3 | 2.06 |
| 14 | Approved policy limiting no. of loans to same family/same address | 1.29 | 0.30 | 0 | 0.4 | 1.99 |
| Section 2: Know Your Intermediary (KYI) using the KYI framework | | | | | | 3.08 |
| 1 | Segment and Monitor by underwriter and/or Sales rep | 2.40 | 0.30 | 0.75 | 0.65 | 4.10 |
| 2 | Robust Intermediary accreditation process – See Compliance guidelines | 2.40 | 0.30 | 0.75 | 0.6 | 4.05 |
| 3 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups. Checks that if Intermediary terminated then terminated across all intermediary listings. | 2.40 | 0.30 | 0.75 | 0.5 | 3.95 |
| 4 | Monthly Reporting on Intermediaries using performance triggers as review point i.e. Approval rate, W/O's(Write Offs) , 3PD(Payments Delinquent/Default), Sales volume, delinquency, TTY, Fraud Loss. | 2.14 | 0.30 | 0.75 | 0.55 | 3.74 |
| 5 | Intermediary Fraud / Intermediary contract should include clauses that allow recourse to Intermediary for fraud. Or encourage Intermediary to take out insurance for internal fraud. | 2.14 | 0.30 | 0.75 | 0.5 | 3.69 |
| 6 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. | 1.71 | 0.30 | 0.75 | 0.55 | 3.31 |
| 7 | Monthly grading process must provide for closure of intermediaries depending on Performance | 1.54 | 0.30 | 0.75 | 0.6 | 3.19 |
| 8 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. | 1.54 | 0.30 | 0.75 | 0.55 | 3.14 |
| 9 | Bank holds cash deposit from merchant and is able to claw back this amount in case of merchant fraud | 1.97 | 0.30 | 0.45 | 0.35 | 3.07 |
| 10 | KYI tool installed | 1.54 | 0.30 | 0.75 | 0.4 | 2.99 |
| 11 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. | 1.37 | 0.30 | 0.75 | 0.35 | 2.77 |
| 12 | Intermediaries have Public Indemnity Insurance to cover | 1.54 | 0.30 | 0.45 | 0.25 | 2.54 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| | Intermediary fraud | | | | | |
| 13 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level | 1.54 | 0.30 | 0 | 0.4 | 2.24 |
| 14 | Payment to Intermediary after receipt of full documentation | 1.11 | 0.30 | 0 | 0.35 | 1.76 |
| 15 | Perform site visitation prior to accreditation of broker | 0.94 | 0.30 | 0 | 0.45 | 1.69 |
| Section 3: Revolving fund - Re draw ability | | | | | | 3.41 |
| 1 | Card Mailing Controls: : Dead card mailing : IVR or voice support activation : Returned Card Procedures : Card activation on new and reissued cards : Mail disguise (Plain white envelopes) or Mail mixing strategy i.e. mixture of mail houses and cards sent over a period of time | 3.00 | 0.50 | 0.75 | 0.3 | 4.55 |
| 2 | Authorization Controls : Adaptive controls for high risk transaction segmentation : Adaptive controls specific to high risk cash transactions | 3.00 | 0.30 | 0.75 | 0.3 | 4.35 |
| 3 | Account Takeover Controls - Ability to monitor for : Address change followed by card/PIN reissue : Activity on inactive accounts : Address change requests on lost/stolen cards | 3.00 | 0.30 | 0.75 | 0.3 | 4.35 |
| 4 | BIN attacks : Track unissued BIN ranges or unissued card no.s : When issuing large no.s of cards in same BIN range ensure they have a range of expiry dates : Investigate auth or clearing requests that contain un-issued card no.s or invalid expiry dates | 2.83 | 0.30 | 0.75 | 0.3 | 4.18 |
| 5 | Remote Channel - Card Not Present Authentication MasterCard 3D Secure Code Verified by Visa | 2.57 | 0.30 | 0.75 | 0.3 | 3.92 |
| 6 | Create 'high risk' re -payment model for suspect accounts or credit bust-outs | 2.57 | 0.30 | 0.75 | 0.3 | 3.92 |
| 7 | Card Mailing Controls : IVR (interactive Voice Response) Failure tracking : Tiered verification strategies | 2.23 | 0.50 | 0.75 | 0.3 | 3.78 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|-----------------------------------|---|------|----------|------|------|-------------|
| | : Outbound deliver verification calls | | | | | |
| 8 | Common Point of Compromise tracking | 2.40 | 0.30 | 0.75 | 0.3 | 3.75 |
| 9 | Review for - large \$ payments - multiple # of payments in short time frame with large \$ value total | 2.40 | 0.30 | 0.75 | 0.3 | 3.75 |
| 10 | Falcon or Aristion installation - high risk strategies developed including ant-counterfeit and cross border strategies | 2.23 | 0.30 | 0.75 | 0.3 | 3.58 |
| 11 | Process where Open to Buy is only released on cleared funds | 2.23 | 0.30 | 0.75 | 0.3 | 3.58 |
| 12 | Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product | 2.23 | 0.30 | 0.75 | 0.3 | 3.58 |
| 13 | Remote Channel - Internet /e-business transaction monitoring : Adaptive Authentication in Host system : Geo-location Analysis | 1.97 | 0.50 | 0.75 | 0.3 | 3.52 |
| 14 | Implement MasterCard Secure Code or Verified by Visa | 1.80 | 0.30 | 0.75 | 0.3 | 3.15 |
| 15 | Remote Channel - Brand Domain Protection Anti-phishing take-down ability | 1.80 | 0.30 | 0.45 | 0.3 | 2.85 |
| 16 | Temporary Shopping Cards : Must be issued for a specified short period of time i.e. 2 weeks : Must only be issued for in store new accounts | 1.54 | 0.30 | 0.75 | 0.2 | 2.79 |
| 17 | Process that allows early identification of payments that do not have cleared funds i.e. dishonored cheque process | 1.80 | 0.30 | 0 | 0.3 | 2.40 |
| 18 | Direct Debit repayments set up from commencement of loan | 1.80 | 0.30 | 0 | 0.3 | 2.40 |
| 19 | CVC 1&2 checking - monitor for failures | 1.11 | 0.00 | 0.75 | 0.1 | 1.96 |
| 20 | Chargeback Tracking | 0.77 | 0.30 | 0.45 | 0.3 | 1.82 |
| Section 4: Know Your Staff | | | | | | 3.28 |
| 1 | IT Security create profiles where system access is dictated by role | 2.23 | 0.50 | 0.75 | 0.55 | 4.03 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| 2 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually | 2.14 | 0.50 | 0.75 | 0.5 | 3.89 |
| 3 | Background Employment Screening (See HR guidelines & Also check financial status of employees on an annual basis to ensure they are not in a financial pressure) | 2.06 | 0.50 | 0.75 | 0.45 | 3.76 |
| 4 | Monitor staff and related party accounts for internal fraud - Monitor monthly approval rates and write offs by individual staff (Sales, U/writing and Collections staff) | 2.23 | 0.30 | 0.75 | 0.45 | 3.73 |
| 5 | ISM (Investigations & Security Manager) Capability with Feedback loop to Prevention | 2.06 | 0.30 | 0.75 | 0.55 | 3.66 |
| 6 | Separate approval process and review process for Staff accounts | 2.06 | 0.30 | 0.75 | 0.55 | 3.66 |
| 7 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should not action or maintain their own (customer) account, nor action or maintain a related parties (customer) account. | 1.54 | 0.30 | 0.75 | 0.55 | 3.14 |
| 8 | Ability to identify staff accounts. | 1.46 | 0.30 | 0.45 | 0.45 | 2.66 |
| 9 | Installation of KYS tool - Intellinx/Footprint | 1.54 | 0.30 | 0.45 | 0.3 | 2.59 |
| 10 | Review process for Staff receiving Sales bonus's - review at both Branch/Merchant and individual staff member level | 1.37 | 0.30 | 0.45 | 0.45 | 2.57 |
| 11 | Can employees access into other banks beyond the bank they are working for? | 1.20 | 0.30 | 0.45 | 0.45 | 2.40 |
| Section 5: 3rd Party Payments / Disbursements | | | | | | 1.99 |
| 1 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 1.71 | 0.30 | 0 | 0.35 | 2.36 |
| 2 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns | 1.54 | 0.30 | 0 | 0.45 | 2.29 |
| 3 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid | 1.29 | 0.30 | 0 | 0.45 | 2.04 |
| 4 | Review triggers for \$ payments by dealer / supplier type | 1.29 | 0.30 | 0 | 0.35 | 1.94 |
| 5 | Payments to dealers / suppliers against full documentation | 1.11 | 0.30 | 0 | 0.45 | 1.86 |
| 6 | Match bank payment details to staff bank accounts | 1.11 | 0.30 | 0 | 0.45 | 1.86 |
| 7 | Ability to identify multiple dealer / supplier payment details to same bank account | 1.29 | 0.30 | 0 | 0.25 | 1.84 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|-----------------------------|--|------|----------|------|------|-------------|
| 8 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier | 1.11 | 0.30 | 0 | 0.35 | 1.76 |
| Section 6: Reporting | | | | | | 3.74 |
| 1 | Fraud cases reported to the bank's head quarter. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. | 2.14 | 0.50 | 0.75 | 0.75 | 4.14 |
| 2 | Monthly reporting: Gross/Net Fraud; Fraud to Sales; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O no payments, Skip/Trace <90MOB (month on book); Fraud savings, Investigation, Recoveries. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 3 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 4 | Key underwriting and transaction data tracked and used for fraud analysis. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 5 | Fraud case management report including the progression and follow-up of fraud investigation, and exchange of fraud information/news. In addition, fraud cases should be reported to the Bank of Thailand. | 2.23 | 0.30 | 0.75 | 0.55 | 3.83 |
| 6 | Monthly reports including follow-up action items. | 2.06 | 0.30 | 0.75 | 0.65 | 3.76 |
| 7 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. | 2.14 | 0.30 | 0.75 | 0.55 | 3.74 |
| 8 | Fraud Prevention/Detection/ Losses broken down by portfolio. | 2.06 | 0.30 | 0.75 | 0.55 | 3.66 |
| 9 | Quarterly reporting that covers new global standards, such as fraud to W/O, Fraud to NI, or reporting that is tailored to most relevant metric that would show impact to bottom line for country portfolio. | 2.23 | 0.30 | 0.75 | 0.35 | 3.63 |
| 10 | Fraud Prevention/Detection/ Losses analyzed and reported by process weakness. | 1.89 | 0.30 | 0.75 | 0.65 | 3.59 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| 11 | Monthly reports relevant to fraud trends and observations. | 1.80 | 0.30 | 0.75 | 0.65 | 3.50 |
| 12 | Fraud Prevention/Detection/ Losses broken down by fraud type. | 2.06 | 0.30 | 0.45 | 0.65 | 3.46 |
| 13 | Variance analysis and development of control charts. | 2.06 | 0.30 | 0.45 | 0.45 | 3.26 |
| Section 7: Operational Efficiency | | | | | | 3.30 |
| 1 | Involvement/sign off in CRP and new product innovations (NPI) process. | 2.23 | 0.30 | 0.75 | 0.55 | 3.83 |
| 2 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. | 2.23 | 0.30 | 0.75 | 0.55 | 3.83 |
| 3 | Fraud Coordinator should be assigned to coordinate between Fraud Risk Manager and ISM. Moreover, regular meeting between these two groups should be arranged to ensure open communication and close gaps. | 2.23 | 0.30 | 0.75 | 0.65 | 3.93 |
| 4 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. | 2.06 | 0.30 | 0.75 | 0.55 | 3.66 |
| 5 | Fraud analyst should analyze fraud losses and review rule sets in fraud detection tools on an ongoing basis. | 2.23 | 0.30 | 0.75 | 0.55 | 3.83 |
| 6 | Formalized fraud policy and procedure should be developed. | 2.40 | 0.00 | 0.75 | 0.65 | 3.80 |
| 7 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. | 2.40 | 0.00 | 0.75 | 0.55 | 3.70 |
| 8 | Well publicize whistle blower program should be one of channels to report fraud case at anytime. Moreover, a case management process to deal with the reported issues should be developed. | 2.23 | 0.00 | 0.75 | 0.55 | 3.53 |
| 9 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. | 1.80 | 0.50 | 0.75 | 0.45 | 3.50 |
| 10 | Formalized write-off police and procedure should be in place. | 2.40 | 0.00 | 0.75 | 0.55 | 3.70 |
| 11 | 100% review of high risk application or accounts should be conducted. For example, - 3PD or 2PD with no customer contact | 2.06 | 0.30 | 0.75 | 0.55 | 3.66 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| | - Accounts that are potentially "Skip" accounts < 210 days on book - Accounts where mail has been returned from the outset of the account opening. | | | | | |
| 12 | Data leakage from both paper-based and electronic-based should be controlled. | 2.40 | 0.00 | 0.75 | 0.45 | 3.60 |
| 13 | Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit. | 2.23 | 0.00 | 0.75 | 0.45 | 3.43 |
| 14 | Conducting the review by Internal Audit or independent 3rd party should be in place. | 2.23 | 0.00 | 0.75 | 0.45 | 3.43 |
| 15 | Centrally located underwriting with documented check list of loans should be in place. | 2.06 | 0.00 | 0.75 | 0.55 | 3.36 |
| 16 | Code of conduct should include clear definition of fraud. | 2.06 | 0.00 | 0.75 | 0.65 | 3.46 |
| 17 | Fraud prevention awareness should be raised and communicated regularly in the management level. | 2.06 | 0.00 | 0.75 | 0.55 | 3.36 |
| 18 | Bad debt written off that is collected from customers in later period should be controlled. | 2.06 | 0.00 | 0.75 | 0.55 | 3.36 |
| 19 | Fraud detection methods should be tailored to needs of individual portfolio. | 1.80 | 0.00 | 0.75 | 0.65 | 3.20 |
| 20 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. | 1.80 | 0.00 | 0.75 | 0.25 | 2.80 |
| 21 | The procedure for fraud alert process across industry peers should be developed. | 2.06 | 0.00 | 0.45 | 0.55 | 3.06 |
| 22 | Fraud training programs should be conducted for Underwriting staff. | 1.89 | 0.00 | 0.45 | 0.55 | 2.89 |
| 23 | Random checks for underwriting process compliance should be performed. | 1.80 | 0.00 | 0.75 | 0 | 2.55 |
| 24 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. | 1.54 | 0.00 | 0.75 | 0.5 | 2.79 |
| 25 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. | 1.89 | 0.00 | 0.45 | 0.5 | 2.84 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------------------------------------|--|------|----------|------|------|-------------|
| 26 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. | 1.20 | 0.00 | 0.45 | 0.6 | 2.25 |
| 27 | Fraud awareness training should be provided to employees at least every six months. | 1.71 | 0.00 | 0.45 | 0.6 | 2.76 |
| 28 | Employee's KPIs should be established based on the risk associated with their tasks. | 0.77 | 0.30 | 0.45 | 0.55 | 2.07 |
| Section 8: Fraud technology | | | | | | 3.03 |
| 1 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. | 2.40 | 0.00 | 0.75 | 0.5 | 3.65 |
| 2 | Banks should implement case management tool with workflow capability. | 2.40 | 0.00 | 0.75 | 0.5 | 3.65 |
| 3 | Fraud technology should be compatible with existing core banking system. | 2.23 | 0.00 | 0.75 | 0.6 | 3.58 |
| 4 | Fraud detection solution should process efficiently and respond back within targeted period. | 2.23 | 0.00 | 0.75 | 0.6 | 3.58 |
| 5 | Fraud technology should be deployed to combat external fraud. | 2.40 | 0.00 | 0.75 | 0.4 | 3.55 |
| 6 | Fraud technology should be deployed to combat internal fraud. | 2.40 | 0.00 | 0.75 | 0.4 | 3.55 |
| 7 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week. | 2.40 | 0.00 | 0.75 | 0.4 | 3.55 |
| 8 | Banks should implement pre-built software specifically for fraud detection technology. | 2.23 | 0.00 | 0.75 | 0.5 | 3.48 |
| 9 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. | 2.23 | 0.00 | 0.75 | 0.5 | 3.48 |
| 10 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. | 2.23 | 0.00 | 0.75 | 0.35 | 3.33 |
| 11 | False positives created from the current technology should be reduced due to poor data quality. | 1.71 | 0.00 | 0.75 | 0.65 | 3.11 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| 12 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. | 1.80 | 0.00 | 0.75 | 0.5 | 3.05 |
| 13 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. | 1.80 | 0.00 | 0.75 | 0.5 | 3.05 |
| 14 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. | 1.71 | 0.00 | 0.75 | 0.55 | 3.01 |
| 15 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. | 1.80 | 0.00 | 0.75 | 0.4 | 2.95 |
| 16 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. | 1.54 | 0.00 | 0.75 | 0.65 | 2.94 |
| 17 | Banks should update fraud detection techniques regularly, at least once a month. | 1.80 | 0.00 | 0.75 | 0.35 | 2.90 |
| 18 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. | 1.80 | 0.00 | 0.75 | 0.35 | 2.90 |
| 19 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. | 1.63 | 0.00 | 0.75 | 0.5 | 2.88 |
| 20 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. | 1.54 | 0.00 | 0.75 | 0.55 | 2.84 |
| 21 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. | 1.71 | 0.00 | 0.75 | 0.35 | 2.81 |
| 22 | Fraud technology should allows banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. | 1.63 | 0.00 | 0.75 | 0.4 | 2.78 |
| 23 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. | 1.46 | 0.00 | 0.75 | 0.55 | 2.76 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| 24 | Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. | 1.54 | 0.00 | 0.75 | 0.45 | 2.74 |
| 25 | The pre-built data model should be created for the bank's existing systems. | 1.54 | 0.00 | 0.75 | 0.45 | 2.74 |
| 26 | Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management. | 1.54 | 0.00 | 0.75 | 0.45 | 2.74 |
| 27 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. | 1.54 | 0.00 | 0.75 | 0.4 | 2.69 |
| 28 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. | 1.54 | 0.00 | 0.75 | 0.35 | 2.64 |
| 29 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyze and alert the responsible people in case of any unusual transactions or suspicious behaviour. | 1.29 | 0.00 | 0.75 | 0.4 | 2.44 |
| 30 | Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide faster and efficient support. | 1.11 | 0.00 | 0.75 | 0.5 | 2.36 |
| 31 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. | 0.94 | 0.00 | 0.75 | 0.45 | 2.14 |

Mortgage Loan

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| Section 1: Know Your Customer (KYC) | | | | | | 4.09 |
| 1 | Underwriting Policy noting: - ID verification procedure, - employment/income verification procedure - address verification procedure - weighted Bureau data (If applicable) | 3.00 | 0.50 | 0.75 | 0.75 | 5.00 |
| 2 | Underwriting Policy noting procedures for high risk accounts: (As defined by risk management) | 2.79 | 0.50 | 0.75 | 0.65 | 4.69 |
| 3 | High value Fraud Alerts to other portfolios at country level | 2.86 | 0.50 | 0.75 | 0.55 | 4.66 |
| 4 | Fraud Blacklisting Capability | 2.86 | 0.50 | 0.75 | 0.5 | 4.61 |
| 5 | Conforms to CRP (Credit Review Point) as signed off | 2.86 | 0.30 | 0.75 | 0.65 | 4.56 |
| 6 | Underwriting Policy that has different requirements for : - Self-employed applicants - Self-certified applicants (Stated income Applicants) - commercial properties (If applicable) | 2.79 | 0.50 | 0.75 | 0.5 | 4.54 |
| 7 | De-Dupe applicant process (approved and declined apps) | 2.51 | 0.50 | 0.75 | 0.55 | 4.31 |
| 8 | Policy around Foreign Nationals | 2.51 | 0.30 | 0.75 | 0.55 | 4.11 |
| 9 | Policy and process whereby address/phone numbers can be validated through public databases | 2.40 | 0.30 | 0.75 | 0.65 | 4.10 |
| 10 | If business operates via Intermediaries (correspondents, brokers) then it must have documented process to audit the KYC verification conducted by the intermediary | 2.29 | 0.50 | 0.75 | 0.55 | 4.09 |
| 11 | Ability to Limit No. of loans to same name/address | 2.33 | 0.30 | 0.75 | 0.65 | 4.03 |
| 12 | Centrally located underwriting, segregation between Sales and Underwriting Teams | 2.22 | 0.50 | 0.75 | 0.5 | 3.97 |
| 13 | Utilize high risk profiles for additional targeting as required | 2.15 | 0.30 | 0.75 | 0.6 | 3.80 |
| 14 | Install Fraud Scorecard where sufficient data available | 2.05 | 0.30 | 0.75 | 0.55 | 3.65 |
| 15 | Install KYC tool where sufficient applications available | 2.22 | 0.30 | 0.45 | 0.45 | 3.42 |
| 16 | Ability for system to capture underwriting data (create relevant Exception reports as required) | 2.12 | 0.30 | 0.75 | 0.25 | 3.42 |
| 17 | Face to Face meeting with customer (signing phase) for Mortgage | 1.94 | 0.50 | 0 | 0.6 | 3.04 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| Section 2: Know Your Intermediary (KYI) using the KYI Framework | | | | | | 2.88 |
| 1 | Robust Intermediary accreditation process – See Compliance guidelines | 2.26 | 0.30 | 0.75 | 0.6 | 3.91 |
| 2 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all broker groups.. Checks that if Intermediary terminated then terminated across all brokers. | 2.26 | 0.30 | 0.75 | 0.5 | 3.81 |
| 3 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level | 2.19 | 0.10 | 0.75 | 0.6 | 3.64 |
| 4 | Segment and Monitor by underwriter and/or Sales rep | 1.98 | 0.10 | 0.75 | 0.55 | 3.38 |
| 5 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. | 1.80 | 0.30 | 0.75 | 0.5 | 3.35 |
| 6 | Intermediaries have Public Indemnity Insurance to cover Intermediary fraud | 2.05 | 0.30 | 0.45 | 0.4 | 3.20 |
| 7 | Perform site visitation prior to accreditation of broker | 1.59 | 0.10 | 0.75 | 0.55 | 2.99 |
| 8 | Broker Fraud - Included in contract with broker is reimbursement for Internal Fraud. Or encourage broker to take out insurance for internal fraud. | 1.76 | 0.10 | 0.45 | 0.65 | 2.96 |
| 9 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. | 1.62 | 0.10 | 0.75 | 0.4 | 2.87 |
| 10 | Monthly grading process must provide for termination of intermediaries depending on performance. If intermediary offers a range of products then intermediary should be terminated across all products. | 1.55 | 0.10 | 0.45 | 0.55 | 2.65 |
| 11 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. | 1.48 | 0.00 | 0.75 | 0.4 | 2.63 |
| 12 | Reward scheme for Intermediaries who detect fraud | 1.80 | 0.00 | 0.45 | 0.35 | 2.60 |
| 13 | Monthly Reporting on Intermediaries using performance triggers as review point (i.e. Approval Rates, Write Offs (W/Os), 3PDs(Payment Delinquent /Default), Sales Volume, TTY(Time To Yes) , Delinquency Rates, Fraud Losses, etc. | 1.38 | 0.30 | 0.45 | 0.25 | 2.38 |
| 14 | KYI tool installed - i.e. Actimize | 1.09 | 0.10 | 0.45 | 0.25 | 1.89 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--------------------------------------|---|------|----------|------|------|-------------|
| Section 3: Asset Verification | | | | | | 3.74 |
| 1 | Title deed review immediately before signing the loan agreement | 2.79 | 0.30 | 0.75 | 0.55 | 4.39 |
| 2 | Alternative valuation checking: - In house appraiser - Internal Valuation Database - External valuation Database | 2.86 | 0.30 | 0.75 | 0.45 | 4.36 |
| 3 | Independent valuation process generated. (Valuation not ordered by Sales staff or customer) OR If Broker orders and supply's valuation then business must conduct detailed review of 100% of all valuation | 2.65 | 0.30 | 0.75 | 0.55 | 4.25 |
| 4 | Drive By process on high risk properties | 2.58 | 0.30 | 0.75 | 0.55 | 4.18 |
| 5 | Approved accreditation process for Appraisers | 2.65 | 0.30 | 0.75 | 0.45 | 4.15 |
| 6 | Process that includes inside/outside photos in valuation process | 2.65 | 0.30 | 0.75 | 0.45 | 4.15 |
| 7 | Prevent/monitor for sale of asset by customer - Can lien be removed. | 2.54 | 0.30 | 0.75 | 0.45 | 4.04 |
| 8 | Create Valuation Panel comprising selected professionally qualified staff that have adequate PI (Professional Indemnity) insurance and strong financial position | 2.44 | 0.30 | 0.75 | 0.55 | 4.04 |
| 9 | Monthly quality control on sample of properties. | 2.44 | 0.30 | 0.75 | 0.55 | 4.04 |
| 10 | Appropriate Property Insurance coverage. Annual check that Insurance is still current. | 2.72 | 0.00 | 0.75 | 0.35 | 3.82 |
| 11 | Process that allows for foreclosure and recovery of monies | 2.12 | 0.10 | 0.75 | 0.55 | 3.52 |
| 12 | Process that allows for the clear establishment of charge against the title to the asset within a short time frame | 2.19 | 0.10 | 0.75 | 0.45 | 3.49 |
| 13 | Secondary checking through listed valuation databases – Investigations commenced if +/- 15% variation | 1.91 | 0.30 | 0.75 | 0.45 | 3.41 |
| 14 | Control that protects all persons who have an interest in the asset have knowledge over any sale or draw down against the asset e.g. 'Speak with' program where independent contact is made with all parties that have a financial interest in the loan | 2.12 | 0.00 | 0.75 | 0.45 | 3.32 |
| 15 | Additional controls or mitigating processes if portfolio does | 1.69 | 0.30 | 0.75 | 0.45 | 3.19 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| | not have Title, Fraud or Mortgage Insurance | | | | | |
| 16 | Fraud Recoveries process in addition to normal recoveries | 1.87 | 0.10 | 0.75 | 0.45 | 3.17 |
| 17 | Semi-annual lien registration checking | 1.98 | 0.00 | 0.75 | 0.35 | 3.08 |
| 18 | If Mortgage portfolio and there is the ability to re-draw then see Minimum control Guideline - Revolve fraud | 2.01 | 0.00 | 0.45 | 0.55 | 3.01 |
| Section 4: Revolving Fund - Re draw ability | | | | | | 1.99 |
| 1 | Account Takeover Controls - Documented process for High Risk Transactions | 1.84 | 0.00 | 0 | 0.3 | 2.14 |
| 2 | Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product | 1.84 | 0.00 | 0 | 0.3 | 2.14 |
| 3 | Account Takeover Controls: Ability to identify high risk transactions and create Exception Report | 1.69 | 0.00 | 0 | 0.4 | 2.09 |
| 4 | Transaction Fraud Tool - e.g. Aristion (where re-draw facility completed through Credit Card transaction) | 1.76 | 0.00 | 0 | 0.3 | 2.06 |
| Section 5: Know Your Staff (KYS) | | | | | | 3.27 |
| 1 | Background Employment Screening (See HR guidelines & Also check financial status of employees on an annual basis to ensure they are not in a financial pressure) | 2.58 | 0.50 | 0.75 | 0.45 | 4.28 |
| 2 | Separate approval process and review process for Staff accounts | 2.36 | 0.50 | 0.75 | 0.55 | 4.16 |
| 3 | Exception Reporting identifying accounts that are High Risk for internal fraud | 1.98 | 0.30 | 0.75 | 0.35 | 3.38 |
| 4 | ISM (Investigation & Security Manager) Capability with Feedback loop to Prevention | 2.05 | 0.00 | 0.75 | 0.45 | 3.25 |
| 5 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should not action or maintain their own (customer) account, nor action or maintain a related parties (customer) account. | 1.94 | 0.00 | 0.75 | 0.55 | 3.24 |
| 6 | Can employees access into other banks beyond the bank they are working for? | 2.01 | 0.30 | 0.45 | 0.45 | 3.21 |
| 7 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually | 1.91 | 0.00 | 0.75 | 0.55 | 3.21 |
| 8 | Ability to identify staff accounts. Monitor staff and related party accounts for internal fraud | 1.91 | 0.00 | 0.75 | 0.45 | 3.11 |
| 9 | Installation of KYS tool - e.g. Intellinx/Footprint | 1.73 | 0.30 | 0.45 | 0.25 | 2.73 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| 10 | Review process for Staff receiving Sales bonuses | 1.55 | 0.30 | 0.45 | 0.35 | 2.65 |
| Section 6: 3rd Party Payments / Disbursements | | | | | | 2.23 |
| 1 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid | 2.15 | 0.00 | 0 | 0.45 | 2.60 |
| 2 | Payments to dealers / suppliers against full documentation | 2.05 | 0.00 | 0 | 0.45 | 2.50 |
| 3 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 2.12 | 0.00 | 0 | 0.35 | 2.47 |
| 4 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns | 1.91 | 0.00 | 0 | 0.45 | 2.36 |
| 5 | Review triggers for \$ payments by dealer / supplier type | 1.94 | 0.00 | 0 | 0.35 | 2.29 |
| 6 | Match bank payment details to staff bank accounts | 1.84 | 0.00 | 0 | 0.45 | 2.29 |
| 7 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier | 1.91 | 0.00 | 0 | 0.35 | 2.26 |
| 8 | Ability to identify multiple dealer / supplier payment details to same bank account | 1.76 | 0.00 | 0 | 0.25 | 2.01 |
| Section 7: Reporting | | | | | | 3.81 |
| 1 | Fraud cases reported to the bank's head quarter. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. | 2.65 | 0.30 | 0.75 | 0.75 | 4.45 |
| 2 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. | 2.58 | 0.30 | 0.75 | 0.55 | 4.18 |
| 3 | Key underwriting and transaction data tracked and used for fraud analysis. | 2.51 | 0.30 | 0.75 | 0.55 | 4.11 |
| 4 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. | 2.40 | 0.50 | 0.75 | 0.45 | 4.10 |
| 5 | Fraud Prevention/Detection/ Losses broken down by fraud type. | 2.58 | 0.30 | 0.45 | 0.65 | 3.98 |
| 6 | Fraud Prevention/Detection/ Losses analyzed and reported by process weakness. | 2.51 | 0.30 | 0.45 | 0.65 | 3.91 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| 7 | Fraud Prevention/Detection/ Losses broken down by portfolio. | 2.51 | 0.30 | 0.45 | 0.55 | 3.81 |
| 8 | Fraud case management report including the progression and follow-up of fraud investigation, and exchange of fraud information/news. In addition, fraud cases should be reported to the Bank of Thailand. | 2.47 | 0.00 | 0.75 | 0.45 | 3.67 |
| 9 | Exception reports for high risk transactions. | 2.44 | 0.30 | 0.45 | 0.45 | 3.64 |
| 10 | Monthly reporting: Gross/Net Fraud; Fraud to Sales ; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O no payments, Skip/Trace <90MOB (month on book) ; Fraud savings, Investigation, Recoveries. | 2.33 | 0.00 | 0.75 | 0.55 | 3.63 |
| 11 | Monthly reports relevant to fraud trends and observations. | 2.15 | 0.30 | 0.45 | 0.65 | 3.55 |
| 12 | Monthly reports including follow-up action Items. | 2.01 | 0.30 | 0.45 | 0.65 | 3.41 |
| 13 | Variance analysis and development of control charts. | 2.05 | 0.30 | 0.45 | 0.55 | 3.35 |
| Section 8: Operational Efficiency | | | | | | 3.81 |
| 1 | Data leakage from both paper-based and electronic-based should be controlled. | 2.54 | 0.50 | 0.75 | 0.65 | 4.44 |
| 2 | Conducting the review by Internal Audit or independent 3rd party should be in place. | 2.61 | 0.50 | 0.75 | 0.55 | 4.41 |
| 3 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. | 2.51 | 0.50 | 0.75 | 0.65 | 4.41 |
| 4 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. | 2.47 | 0.50 | 0.75 | 0.55 | 4.27 |
| 5 | Formalized fraud policy and procedure should be developed. | 2.44 | 0.50 | 0.75 | 0.55 | 4.24 |
| 6 | Formalized write-off police and procedure should be in place. | 2.44 | 0.50 | 0.75 | 0.55 | 4.24 |
| 7 | Fraud training programs should be conducted for Underwriting staff. | 2.51 | 0.30 | 0.75 | 0.65 | 4.21 |
| 8 | Fraud analyst should analyze fraud losses and review rule sets in fraud detection tools on an ongoing basis. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| 9 | 100% review of high risk application or accounts should be conducted. For example, - 3PD or 2PD with no customer contact - Accounts that are potentially "Skip" accounts < 210 days on book - Accounts where mail has been returned from the outset of the account opening. | 2.26 | 0.50 | 0.75 | 0.45 | 3.96 |
| 10 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. | 2.33 | 0.30 | 0.75 | 0.55 | 3.93 |
| 11 | Random checks for underwriting process compliance should be performed. | 2.58 | 0.30 | 0.45 | 0.55 | 3.88 |
| 12 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. | 2.36 | 0.50 | 0.45 | 0.55 | 3.86 |
| 13 | Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit. | 2.47 | 0.30 | 0.45 | 0.55 | 3.77 |
| 14 | Well publicize whistle blower program should be one of channels to report fraud case at anytime. Moreover, a case management process to deal with the reported issues should be developed. | 2.33 | 0.30 | 0.45 | 0.55 | 3.63 |
| 15 | Fraud prevention awareness should be raised and communicated regularly in the management level. | 2.33 | 0.30 | 0.45 | 0.55 | 3.63 |
| 16 | Fraud Coordinator should ensure that 'Close the loop' process is finalized. | 2.19 | 0.30 | 0.75 | 0.35 | 3.59 |
| 17 | Bad debt written off that is collected from customers in later period should be controlled. | 2.08 | 0.50 | 0.45 | 0.55 | 3.58 |
| 18 | Code of conduct should include clear definition of fraud. | 1.98 | 0.30 | 0.75 | 0.55 | 3.58 |
| 19 | The members of the Fraud team should consist of staff from Operations and Analytics. | 2.26 | 0.30 | 0.45 | 0.55 | 3.56 |
| 20 | Employee's KPIs should be established based on the risk associated with their tasks. | 2.33 | 0.30 | 0.45 | 0.45 | 3.53 |
| 21 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. | 2.22 | 0.30 | 0.45 | 0.55 | 3.52 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------------------------------------|---|------|----------|------|------|-------------|
| 22 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. | 1.91 | 0.50 | 0.45 | 0.65 | 3.51 |
| 23 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. | 2.19 | 0.00 | 0.75 | 0.45 | 3.39 |
| 24 | The procedure for fraud alert process across industry peers should be developed. | 2.05 | 0.30 | 0.45 | 0.55 | 3.35 |
| 25 | Fraud detection methods should be tailored to needs of individual portfolio. | 2.12 | 0.00 | 0.75 | 0.45 | 3.32 |
| 26 | Fraud awareness training should be provided to employees at least every six months. | 2.01 | 0.30 | 0.45 | 0.55 | 3.31 |
| 27 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. | 1.84 | 0.30 | 0.45 | 0.25 | 2.84 |
| Section 9: Fraud Technology | | | | | | 2.97 |
| 1 | Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management. | 1.98 | 0.30 | 0.75 | 0.45 | 3.48 |
| 2 | Fraud technology should be compatible with existing core banking system. | 1.91 | 0.50 | 0.45 | 0.6 | 3.46 |
| 3 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. | 1.91 | 0.30 | 0.75 | 0.45 | 3.41 |
| 4 | Fraud technology should be deployed to combat internal fraud. | 1.94 | 0.30 | 0.75 | 0.4 | 3.39 |
| 5 | Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. | 1.84 | 0.30 | 0.75 | 0.45 | 3.34 |
| 6 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. | 1.76 | 0.30 | 0.75 | 0.5 | 3.31 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| 7 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. | 1.69 | 0.30 | 0.75 | 0.55 | 3.29 |
| 8 | Fraud technology should be deployed to combat external fraud. | 1.84 | 0.30 | 0.75 | 0.4 | 3.29 |
| 9 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week. | 1.84 | 0.30 | 0.75 | 0.4 | 3.29 |
| 10 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. | 1.55 | 0.30 | 0.75 | 0.65 | 3.25 |
| 11 | Banks should implement pre-built software specifically for fraud detection technology. | 1.98 | 0.30 | 0.45 | 0.5 | 3.23 |
| 12 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. | 1.98 | 0.30 | 0.45 | 0.5 | 3.23 |
| 13 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. | 1.98 | 0.30 | 0.45 | 0.5 | 3.23 |
| 14 | Banks should implement case management tool with workflow capability. | 1.98 | 0.30 | 0.45 | 0.5 | 3.23 |
| 15 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. | 1.66 | 0.30 | 0.75 | 0.5 | 3.21 |
| 16 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. | 1.45 | 0.30 | 0.75 | 0.55 | 3.05 |
| 17 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. | 1.84 | 0.30 | 0.45 | 0.4 | 2.99 |
| 18 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. | 1.55 | 0.30 | 0.75 | 0.35 | 2.95 |
| 19 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyze and alert the responsible people in case of any unusual transactions or suspicious behaviour. | 1.76 | 0.30 | 0.45 | 0.4 | 2.91 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| 20 | Fraud technology should allow banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. | 1.69 | 0.30 | 0.45 | 0.4 | 2.84 |
| 21 | False positives created from the current technology should be reduced due to poor data quality. | 1.66 | 0.50 | 0 | 0.65 | 2.81 |
| 22 | Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide faster and efficient support. | 1.55 | 0.30 | 0.45 | 0.5 | 2.80 |
| 23 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. | 1.55 | 0.30 | 0.45 | 0.5 | 2.80 |
| 24 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. | 1.55 | 0.30 | 0.45 | 0.5 | 2.80 |
| 25 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. | 1.69 | 0.30 | 0.45 | 0.35 | 2.79 |
| 26 | Fraud detection solution should process efficiently and respond back within targeted period. | 1.41 | 0.30 | 0.45 | 0.6 | 2.76 |
| 27 | Banks should update fraud detection techniques regularly, at least once a month. | 1.48 | 0.30 | 0.45 | 0.35 | 2.58 |
| 28 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. | 1.48 | 0.30 | 0.45 | 0.35 | 2.58 |
| 29 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. | 1.45 | 0.00 | 0.45 | 0.55 | 2.45 |
| 30 | The pre-built data model should be created for the bank's existing systems. | 1.38 | 0.30 | 0 | 0.45 | 2.13 |
| 31 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. | 1.48 | 0.30 | 0 | 0.3 | 2.08 |

Personal Loan

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| Section 1: Know Your Customer (KYC) | | | | | | 3.86 |
| 1 | Underwriting Policy noting : ID verification procedure, : employment/income verification procedure : address verification procedure : phone verification procedure : weighted bureau data | 3.00 | 0.50 | 0.75 | 0.75 | 5.00 |
| 2 | Centrally located underwriting, segregation between Sales and Underwriting Teams | 2.74 | 0.50 | 0.75 | 0.65 | 4.64 |
| 3 | Conforms to CRP (Credit Review Point) as signed off | 2.55 | 0.50 | 0.75 | 0.65 | 4.45 |
| 4 | Fraud Blacklisting Capability | 2.51 | 0.50 | 0.75 | 0.65 | 4.41 |
| 5 | Validated address/phone number through public databases | 2.40 | 0.50 | 0.75 | 0.55 | 4.20 |
| 6 | Utilize high risk profiles for additional targeting | 2.36 | 0.50 | 0.75 | 0.55 | 4.16 |
| 7 | If business operates via Intermediaries then must have documented process to validate controls conducted by intermediary | 2.29 | 0.50 | 0.75 | 0.6 | 4.14 |
| 8 | High value Fraud alerts to other portfolio's at country level | 2.29 | 0.50 | 0.75 | 0.6 | 4.14 |
| 9 | Install KYC tool where sufficient applications available | 2.29 | 0.50 | 0.75 | 0.55 | 4.09 |
| 10 | Policy around Foreign Nationals | 2.48 | 0.30 | 0.75 | 0.55 | 4.08 |
| 11 | De-Dupe application process (approved and declined apps) | 2.25 | 0.50 | 0.75 | 0.5 | 4.00 |
| 12 | Ability for system to capture underwriting data (create relevant Exception reports as required) | 2.10 | 0.50 | 0.75 | 0.65 | 4.00 |
| 13 | Approved methodology for high Risk designation using historical data and current fraud trends | 2.10 | 0.30 | 0.45 | 0.65 | 3.50 |
| 14 | Install Fraud Scorecard where sufficient data available | 1.99 | 0.50 | 0.75 | 0.25 | 3.49 |
| 15 | No 2nd deal to be approved before 1st loan payment cleared. | 2.06 | 0.10 | 0.75 | 0.25 | 3.16 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| 16 | Remote Channel - Internet Apps - Capture relevant session data (i.e. geo-location data/ IP address or other PC device ID) identify 'high risk accounts using these variables | 1.84 | 0.50 | 0 | 0.55 | 2.89 |
| 17 | Use of subjective negative codes from point of sale merchants | 1.73 | 0.30 | 0 | 0.5 | 2.53 |
| 18 | Approved policy limiting no. of loans to same family/same address | 1.65 | 0.30 | 0 | 0.4 | 2.35 |
| Section 2: Know Your Intermediary (KYI) | | | | | | 3.47 |
| 1 | Segment and Monitor by underwriter and/or Sales rep | 2.51 | 0.50 | 0.75 | 0.5 | 4.26 |
| 2 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups.. Checks that if Intermediary terminated then terminated across all intermediary listings. | 2.36 | 0.50 | 0.45 | 0.6 | 3.91 |
| 3 | Robust Intermediary accreditation process – See Compliance guidelines | 2.29 | 0.50 | 0.45 | 0.6 | 3.84 |
| 4 | Intermediary Fraud - Included in contract with Intermediary is reimbursement for Internal Fraud. Or encourage Intermediary to take out insurance for internal fraud. | 1.99 | 0.50 | 0.75 | 0.55 | 3.79 |
| 5 | Monthly Reporting on Intermediaries using performance triggers as review point i.e. Approval rate, W/O's (Write Offs) , 3PD(Payment Default/ Delinquent), Sales volume, delinquency, TTY 9Time To Yes) , Fraud Loss. | 1.91 | 0.50 | 0.75 | 0.6 | 3.76 |
| 6 | Monthly grading process must provide for closure of intermediaries depending on Performance | 1.88 | 0.50 | 0.45 | 0.55 | 3.38 |
| 7 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. | 1.65 | 0.50 | 0.75 | 0.55 | 3.45 |
| 8 | Perform site visitation prior to accreditation of broker | 1.73 | 0.50 | 0.75 | 0.4 | 3.38 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| 9 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level | 1.76 | 0.50 | 0.45 | 0.25 | 2.96 |
| 10 | Intermediaries have Personal Indemnity / Fidelity Insurance to cover Intermediary fraud | 1.50 | 0.50 | 0.75 | 0.6 | 3.35 |
| 11 | KYI tool installed - i.e. Actimize | 1.54 | 0.50 | 0.75 | 0.45 | 3.24 |
| 12 | Payment to Intermediary after receipt of full documentation | 1.65 | 0.50 | 0.75 | 0.55 | 3.45 |
| 13 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. | 1.73 | 0.50 | 0.75 | 0.45 | 3.43 |
| 14 | Bank holds cash deposit from Intermediary and is able to claw back this amount in case of merchant fraud | 1.58 | 0.50 | 0.45 | 0.3 | 2.83 |
| 15 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. | 1.80 | 0.30 | 0 | 0.55 | 2.65 |
| Section 3: Asset Verification | | | | | | 2.46 |
| 1 | Provide Plan for ability to identify 'at risk' accounts where asset may be on sold without finalizing settlement | 1.65 | 0.50 | 0 | 0.55 | 2.70 |
| 2 | Prevent/monitor for forward sale of asset by customer | 1.54 | 0.50 | 0 | 0.65 | 2.69 |
| 3 | Clearly defined asset type that will be eligible for loans, Caps on extra's as defined by policy | 1.69 | 0.50 | 0 | 0.4 | 2.59 |
| 4 | Independent Asset validation process - valuation checked through independent database | 1.35 | 0.50 | 0 | 0.65 | 2.50 |
| 5 | If asset is not registered prior to disbursement then audit to ensure asset is secured within prescribed time frame | 1.58 | 0.30 | 0 | 0.4 | 2.28 |
| 6 | Process that allows clear title registration over asset within a set time frame | 1.69 | 0.10 | 0 | 0.4 | 2.19 |
| Section 4: Revolving Fund - Re draw ability | | | | | | 3.69 |
| 1 | Transaction Fraud Tool - e.g. Arision (where re-draw facility completed through Credit Card | 2.18 | 0.50 | 0.75 | 0.45 | 3.88 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|---|--|------|----------|------|------|-------------|
| | transaction) | | | | | |
| 2 | Account Takeover Controls - Documented process for High Risk Transactions | 1.99 | 0.50 | 0.75 | 0.55 | 3.79 |
| 3 | Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product | 1.88 | 0.50 | 0.75 | 0.55 | 3.68 |
| 4 | Account Takeover Controls: Ability to identify high risk transactions and create Exception Report | 1.91 | 0.50 | 0.45 | 0.55 | 3.41 |
| Section 5: Know Your Staff (KYS) | | | | | | 3.58 |
| 1 | IT Security create profiles where system access is dictated by role | 2.66 | 0.50 | 0.75 | 0.45 | 4.36 |
| 2 | Background Employment Screening (See HR guidelines) (Also check financial status of employees on an annual basis to ensure they are not in a financial pressure) | 2.55 | 0.50 | 0.75 | 0.55 | 4.35 |
| 3 | Separate approval process and review process for Staff accounts | 2.40 | 0.50 | 0.75 | 0.55 | 4.20 |
| 4 | ISM (Investigation & Security Manager) Capability with Feedback loop to Prevention | 2.29 | 0.50 | 0.75 | 0.55 | 4.09 |
| 5 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually | 1.95 | 0.30 | 0.75 | 0.45 | 3.45 |
| 6 | Can employees access into other banks beyond the bank they are working for? | 1.58 | 0.50 | 0.75 | 0.55 | 3.38 |
| 7 | Monitor monthly approval rates and write offs by individual staff (Sales, U/writing and Collections staff) | 1.76 | 0.50 | 0.75 | 0.35 | 3.36 |
| 8 | Ability to identify staff accounts. Monitor staff accounts for internal fraud | 1.69 | 0.30 | 0.75 | 0.45 | 3.19 |
| 9 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should not action or maintain their own (customer) account, nor action or maintain a related parties (customer) account. | 1.69 | 0.30 | 0.75 | 0.45 | 3.19 |
| 10 | Installation of KYS tool - Intellinx/Footprint | 1.84 | 0.50 | 0.45 | 0.25 | 3.04 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| 11 | Review process for Branches and Staff receiving Sales bonus's - review at both Branch and individual staff member level | 1.73 | 0.30 | 0.45 | 0.55 | 3.03 |
| Section 6: 3rd Party Payments / Disbursements | | | | | | 1.98 |
| 1 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns | 1.46 | 0.30 | 0 | 0.55 | 2.31 |
| 2 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid | 1.31 | 0.50 | 0 | 0.4 | 2.21 |
| 3 | Payments to dealers / suppliers against full documentation | 1.31 | 0.50 | 0 | 0.4 | 2.21 |
| 4 | Review triggers for \$ payments by dealer / supplier type | 1.24 | 0.50 | 0 | 0.3 | 2.04 |
| 5 | Match bank payment details to staff bank accounts | 1.20 | 0.30 | 0 | 0.45 | 1.95 |
| 6 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier | 1.20 | 0.50 | 0 | 0.2 | 1.90 |
| 7 | Ability to identify multiple dealer / supplier payment details to same bank account | 1.35 | 0.30 | 0 | 0.2 | 1.85 |
| 8 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 1.13 | 0.30 | 0 | 0.35 | 1.78 |
| Section 7: Reporting | | | | | | 3.94 |
| 1 | Fraud cases reported to the bank's head quarter. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. | 2.40 | 0.50 | 0.75 | 0.75 | 4.40 |
| 2 | Fraud Prevention/Detection/ Losses broken down by fraud type. | 2.33 | 0.50 | 0.75 | 0.65 | 4.23 |
| 3 | Quarterly reporting that covers new global standards i.e. fraud to W/O, Fraud to NI, Reporting that is tailored to most relevant metric that would show impact to bottom line for country portfolio. | 2.51 | 0.50 | 0.75 | 0.45 | 4.21 |
| 4 | Fraud case management report including the progression and follow-up of fraud investigation, and exchange of fraud information/news. In | 2.48 | 0.30 | 0.75 | 0.65 | 4.18 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| | addition, fraud cases should be reported to the Bank of Thailand. | | | | | |
| 5 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark for each bank, for example, capital, net asset, and net revenue. | 2.25 | 0.50 | 0.75 | 0.55 | 4.05 |
| 6 | Fraud Prevention/Detection/ Losses analyzed and reported by process weakness. | 2.14 | 0.50 | 0.75 | 0.65 | 4.04 |
| 7 | Monthly reports relevant to fraud trends and observations. | 2.06 | 0.50 | 0.75 | 0.65 | 3.96 |
| 8 | Monthly reporting: Gross/Net Fraud; Fraud to Sales ; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O no payments, Skip/Trace <90MOB; Fraud savings, Investigation, Recoveries. | 2.18 | 0.30 | 0.75 | 0.65 | 3.88 |
| 9 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. | 2.14 | 0.50 | 0.75 | 0.45 | 3.84 |
| 10 | Monthly reports including follow-up action Items. | 2.33 | 0.50 | 0.45 | 0.55 | 3.83 |
| 11 | Key underwriting and transaction data tracked and used for fraud analysis. | 2.21 | 0.30 | 0.75 | 0.45 | 3.71 |
| 12 | Fraud Prevention/Detection/ Losses broken down by portfolio. | 2.10 | 0.50 | 0.45 | 0.55 | 3.60 |
| 13 | Variance analysis and development of control charts. | 2.03 | 0.50 | 0.45 | 0.45 | 3.43 |
| Section 8: Operational Efficiency | | | | | | 3.87 |
| 1 | Fraud Manager should have the awareness of fraud prevention and update the knowledge and skills especially for new fraud. | 2.78 | 0.50 | 0.75 | 0.55 | 4.58 |
| 2 | Data leakage from both paper-based and electronic-based should be controlled. | 2.44 | 0.50 | 0.75 | 0.65 | 4.34 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| 3 | Centrally located underwriting with documented check list of loans should be in place. | 2.63 | 0.50 | 0.75 | 0.45 | 4.33 |
| 4 | Formalized write-off police and procedure should be in place. | 2.51 | 0.50 | 0.75 | 0.55 | 4.31 |
| 5 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. | 2.44 | 0.50 | 0.75 | 0.55 | 4.24 |
| 6 | Random checks for underwriting process compliance should be performed. | 2.44 | 0.50 | 0.75 | 0.55 | 4.24 |
| 7 | Fraud prevention awareness should be raised and communicated regularly in the management level. | 2.44 | 0.50 | 0.75 | 0.55 | 4.24 |
| 8 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. | 2.33 | 0.50 | 0.75 | 0.65 | 4.23 |
| 9 | Fraud training programs should be conducted for Underwriting staff. | 2.33 | 0.50 | 0.75 | 0.65 | 4.23 |
| 10 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. | 2.40 | 0.50 | 0.75 | 0.55 | 4.20 |
| 11 | Well publicize whistle blower program should be one of channels to report fraud case at anytime. Moreover, a case management process to deal with the reported issues should be developed. | 2.40 | 0.50 | 0.75 | 0.55 | 4.20 |
| 12 | Fraud analyst should analyze fraud losses and review rule sets in fraud detection tools on an ongoing basis. | 2.36 | 0.50 | 0.75 | 0.55 | 4.16 |
| 13 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. | 2.25 | 0.50 | 0.75 | 0.55 | 4.05 |
| 14 | 100% review of high risk application or accounts should be conducted. For example, - 3PD or 2PD with no customer contact - Accounts that are potentially "Skip" accounts < | 2.21 | 0.50 | 0.75 | 0.55 | 4.01 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| | 210 days on book - Accounts where mail has been returned from the outset of the account opening. | | | | | |
| 15 | Operating procedures should be in place and Fraud Case Management should be deployed to alert fraudulent activities to Fraud team and Internal Audit. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 16 | Formalized fraud policy and procedure should be developed. | 2.36 | 0.30 | 0.75 | 0.55 | 3.96 |
| 17 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. | 2.21 | 0.30 | 0.75 | 0.65 | 3.91 |
| 18 | Involvement/sign off in CRP and new product innovations (NPI) process. | 2.10 | 0.50 | 0.75 | 0.55 | 3.90 |
| 19 | Code of conduct should include clear definition of fraud. | 2.25 | 0.30 | 0.75 | 0.55 | 3.85 |
| 20 | Fraud Coordinator should be assigned to coordinate between Fraud Risk Manager and ISM. Moreover, regular meeting between these two groups should be arranged to ensure open communication and close gaps. | 2.33 | 0.30 | 0.75 | 0.45 | 3.83 |
| 21 | Conducting the review by Internal Audit or independent 3rd party should be in place. | 2.36 | 0.30 | 0.75 | 0.35 | 3.76 |
| 22 | Fraud detection methods should be tailored to needs of individual portfolio. | 2.10 | 0.50 | 0.45 | 0.45 | 3.50 |
| 23 | The members of the Fraud team should consist of staff from Operations and Analytics. | 2.06 | 0.50 | 0.45 | 0.45 | 3.46 |
| 24 | The procedure for fraud alert process across industry peers should be developed. | 1.88 | 0.50 | 0.45 | 0.55 | 3.38 |
| 25 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. | 1.84 | 0.30 | 0.75 | 0.45 | 3.34 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------------------------------------|---|------|----------|------|------|-------------|
| 26 | Bad debt written off that is collected from customers in later period should be controlled. | 1.91 | 0.30 | 0.45 | 0.45 | 3.11 |
| 27 | Fraud awareness training should be provided to employees at least every six months. | 1.73 | 0.30 | 0.45 | 0.55 | 3.03 |
| 28 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. | 1.80 | 0.10 | 0.75 | 0.25 | 2.90 |
| 29 | Employee's KPIs should be established based on the risk associated with their tasks. | 1.50 | 0.30 | 0.45 | 0.55 | 2.80 |
| Section 9: Fraud technology | | | | | | 3.34 |
| 1 | Fraud technology should be deployed to combat internal fraud. | 2.29 | 0.50 | 0.75 | 0.55 | 4.09 |
| 2 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. | 2.18 | 0.50 | 0.75 | 0.65 | 4.08 |
| 3 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week. | 2.21 | 0.50 | 0.75 | 0.5 | 3.96 |
| 4 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. | 2.51 | 0.50 | 0.45 | 0.5 | 3.96 |
| 5 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. | 2.36 | 0.30 | 0.75 | 0.55 | 3.96 |
| 6 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. | 2.44 | 0.50 | 0.45 | 0.5 | 3.89 |
| 7 | Banks should implement case management tool with workflow capability. | 2.40 | 0.50 | 0.45 | 0.5 | 3.85 |
| 8 | Banks should implement pre-built software specifically for fraud detection technology. | 2.36 | 0.50 | 0.45 | 0.5 | 3.81 |
| 9 | Fraud technology should be deployed to combat external fraud. | 2.29 | 0.30 | 0.75 | 0.4 | 3.74 |
| 10 | Fraud technology should be compatible with existing core banking system. | 2.33 | 0.30 | 0.45 | 0.6 | 3.68 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| 11 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. | 2.18 | 0.30 | 0.75 | 0.35 | 3.58 |
| 12 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. | 1.99 | 0.30 | 0.75 | 0.5 | 3.54 |
| 13 | Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management. | 1.84 | 0.50 | 0.75 | 0.45 | 3.54 |
| 14 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. | 1.91 | 0.30 | 0.75 | 0.55 | 3.51 |
| 15 | Banks should update fraud detection techniques regularly, at least once a month. | 2.36 | 0.30 | 0.45 | 0.35 | 3.46 |
| 16 | Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. | 1.84 | 0.30 | 0.75 | 0.45 | 3.34 |
| 17 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. | 1.88 | 0.50 | 0.45 | 0.5 | 3.33 |
| 18 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. | 1.91 | 0.30 | 0.45 | 0.65 | 3.31 |
| 19 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. | 1.99 | 0.50 | 0.45 | 0.35 | 3.29 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| 20 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. | 1.54 | 0.50 | 0.75 | 0.5 | 3.29 |
| 21 | Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide faster and efficient support. | 2.03 | 0.30 | 0.45 | 0.5 | 3.28 |
| 22 | Fraud detection solution should process efficiently and respond back within targeted period. | 1.91 | 0.30 | 0.45 | 0.6 | 3.26 |
| 23 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. | 2.14 | 0.30 | 0.45 | 0.35 | 3.24 |
| 24 | Fraud technology should allows banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. | 1.88 | 0.50 | 0.45 | 0.4 | 3.23 |
| 25 | Fraud technology should consistently detect the staff's bank accounts and relevant people, analyze and alert the responsible people in case of any unusual transactions or suspicious behaviour. | 1.76 | 0.50 | 0.45 | 0.4 | 3.11 |
| 26 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. | 1.39 | 0.50 | 0.75 | 0.45 | 3.09 |
| 27 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. | 1.54 | 0.50 | 0.45 | 0.4 | 2.89 |
| 28 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. | 1.35 | 0.30 | 0.45 | 0.5 | 2.60 |
| 29 | The pre-built data model should be created for the bank's existing systems. | 1.69 | 0.30 | 0 | 0.45 | 2.44 |
| 30 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it | 1.31 | 0.50 | 0 | 0.3 | 2.11 |

| Rank | Revised description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|-----|------|-------------|
| | should support Thai language correctly. | | | | | |
| 31 | False positives created from the current technology should be reduced due to poor data quality. | 0.86 | 0.30 | 0 | 0.65 | 1.81 |

Sales Finance

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| Section 1: Know Your Customer (KYC) | | | | | | 3.65 |
| 1 | Underwriting Policy noting : ID verification procedure , predefined acceptable documents : ID verification procedure for merchant, : employment/income verification procedure : address verification procedure : phone verification procedure, e.g. no third party phones for 0% down payment : weighted bureau data | 2.70 | 0.50 | 0.75 | 0.75 | 4.70 |
| 2 | Validated address/phone number through public databases | 2.70 | 0.50 | 0.75 | 0.55 | 4.50 |
| 3 | Conforms to CRP (Credit Review Point) as signed off | 2.70 | 0.30 | 0.75 | 0.65 | 4.40 |
| 4 | High value Fraud alerts to other portfolio's at country level | 2.70 | 0.30 | 0.75 | 0.6 | 4.35 |
| 5 | Policy around Foreign Nationals | 2.25 | 0.50 | 0.75 | 0.55 | 4.05 |
| 6 | Approved policy limiting no. of loans to same family/same address | 2.40 | 0.50 | 0.75 | 0.4 | 4.05 |
| 7 | Fraud Blacklisting Capability | 2.25 | 0.30 | 0.75 | 0.65 | 3.95 |
| 8 | Ability for system to capture underwriting data (create relevant Exception reports as required) | 2.25 | 0.30 | 0.75 | 0.65 | 3.95 |
| 9 | Approved methodology for high Risk designation using historical data and current fraud trends | 2.40 | 0.30 | 0.45 | 0.65 | 3.80 |
| 10 | De-Dupe process (approved and declined apps) | 2.25 | 0.30 | 0.75 | 0.5 | 3.80 |
| 11 | Use of subjective negative codes from point of sale merchants | 2.25 | 0.30 | 0.75 | 0.5 | 3.80 |
| 12 | Centrally located underwriting, segregation between Sales and Underwriting Teams | 1.95 | 0.30 | 0.75 | 0.65 | 3.65 |
| 13 | No 2nd deal to be approved before 1st loan payment cleared. | 2.25 | 0.30 | 0.75 | 0.25 | 3.55 |
| 14 | Utilize high risk profiles for additional targeting | 1.50 | 0.30 | 0.75 | 0.55 | 3.10 |
| 15 | Install KYC tool where sufficient applications available | 1.50 | 0.30 | 0.75 | 0.55 | 3.10 |
| 16 | Install Fraud Scorecard where sufficient data available | 1.50 | 0.30 | 0.75 | 0.25 | 2.80 |
| 17 | If business operates via Intermediaries then must have documented process to audit KYC checks conducted by intermediary | 1.50 | 0.50 | 0 | 0.6 | 2.60 |
| 18 | Remote Channel - Internet Apps - Capture relevant session data (i.e. geo-location data/ IP address or other PC device ID) | 0.75 | 0.50 | 0 | 0.35 | 1.60 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|-----|------|-------------|
| | identify 'high risk accounts using these variables | | | | | |
| Section 2: Know Your Intermediary (KYI) using the KYI Framework | | | | | | 1.87 |
| 1 | Monthly Reporting on Intermediaries using performance triggers as review point i.e. Approval rate, W/O's, 3PD, Sales volume, delinquency, TTY, Fraud Loss. | 1.50 | 0.30 | 0 | 0.55 | 2.35 |
| 2 | Grade Intermediaries depending on performance. Process should 'Close the Loop' back to Sales team. | 1.50 | 0.30 | 0 | 0.55 | 2.35 |
| 3 | Develop Procedures for Additional Intermediary reviews. These should be incorporated into ongoing audit process. | 1.50 | 0.30 | 0 | 0.55 | 2.35 |
| 4 | Segment and Monitor by underwriter and/or Sales representative | 1.20 | 0.50 | 0 | 0.65 | 2.35 |
| 5 | Blacklist for Intermediaries. If Intermediary offers more than one product blacklisting should occur across all products and all intermediary groups.. Checks that if Intermediary terminated then terminated across all intermediary listings. | 1.50 | 0.30 | 0 | 0.5 | 2.30 |
| 6 | Payment to Intermediary after receipt of full documentation | 1.50 | 0.30 | 0 | 0.35 | 2.15 |
| 7 | Intermediaries have PI Insurance to cover Intermediary fraud | 1.50 | 0.30 | 0 | 0.25 | 2.05 |
| 8 | Monthly grading process must provide for closure of intermediaries depending on Performance | 0.75 | 0.30 | 0 | 0.6 | 1.65 |
| 9 | Intermediary Fraud - Included in contract with Intermediary is reimbursement for Internal Fraud. Or encourage Intermediary to take out insurance for internal fraud. | 0.75 | 0.30 | 0 | 0.5 | 1.55 |
| 10 | Robust Intermediary accreditation process – See Compliance guidelines | 0.45 | 0.50 | 0 | 0.6 | 1.55 |
| 11 | Perform site visitation prior to accreditation of broker | 0.75 | 0.30 | 0 | 0.45 | 1.50 |
| 12 | Bank holds cash deposit from merchant and is able to claw back this amount in case of merchant fraud | 0.75 | 0.30 | 0 | 0.45 | 1.50 |
| 13 | Credit of the intermediary or its financial health checks should be obtained and review as an annual basis. | 0.75 | 0.30 | 0 | 0.45 | 1.50 |
| 14 | Sub-Dealers. If sub-dealers are used then there should be proper contracting, monitoring processes and visibility around payments and monthly reporting at sub-dealer level | 0.75 | 0.30 | 0 | 0.4 | 1.45 |
| 15 | KYI tool installed - i.e. Actimize | 0.75 | 0.30 | 0 | 0.4 | 1.45 |
| Section 3: Asset Verification | | | | | | 1.62 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| 1 | Independent Asset validation process - valuation checked through independent database | 0.75 | 0.30 | 0 | 0.65 | 1.70 |
| 2 | Provide Plan for ability to identify 'at risk' accounts where asset may be on sold without finalizing settlement | 0.75 | 0.30 | 0 | 0.65 | 1.70 |
| 3 | Process that allows clear title registration over asset within a set time frame | 0.75 | 0.30 | 0 | 0.55 | 1.60 |
| 4 | If asset is not registered prior to disbursement then audit to ensure asset is secured within prescribed time frame | 0.75 | 0.30 | 0 | 0.55 | 1.60 |
| 5 | Prevent/monitor for forward sale of asset by customer | 0.75 | 0.30 | 0 | 0.55 | 1.60 |
| 6 | Clearly defined asset type that will be eligible for loans, Caps on extra's as defined by policy | 0.75 | 0.30 | 0 | 0.45 | 1.50 |
| Section 4: Revolving Fund - Re draw ability | | | | | | 2.85 |
| 1 | Account Takeover Controls - Ability to monitor for : Address change followed by card/PIN reissue : Activity on inactive accounts : Address change requests on lost/stolen cards | 2.40 | 0.50 | 0.75 | 0.4 | 4.05 |
| 2 | Authorization Controls : Adaptive controls for high risk transaction segmentation : Adaptive controls specific to high risk cash transactions | 2.40 | 0.50 | 0.75 | 0.3 | 3.95 |
| 3 | Card Mailing Controls: : Dead card mailing : IVR or voice support activation : Returned Card Procedures : Card activation on new and reissued cards : Mail disguise (Plain white envelopes) or Mail mixing strategy i.e. mixture of mail houses and cards sent over a period of time | 2.25 | 0.50 | 0.75 | 0.3 | 3.80 |
| 4 | BIN attacks : Track unissued BIN ranges or unissued card no's : When issuing large no's of cards in same BIN range ensure they have a range of expiry dates : Investigate auth or clearing requests that contain un-issued card no's or invalid expiry dates | 2.25 | 0.50 | 0.75 | 0.3 | 3.80 |
| 5 | Falcon or Aristion installation - high risk strategies developed including ant-counterfeit and cross border strategies | 2.25 | 0.30 | 0.75 | 0.3 | 3.60 |
| 6 | Review for - large \$ payments | 2.25 | 0.30 | 0.75 | 0.25 | 3.55 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|-----------------------------------|---|------|----------|------|------|-------------|
| | - multiple # of payments in short time frame with large \$ value total | | | | | |
| 7 | Payments against original documents | 2.25 | 0.30 | 0.75 | 0.25 | 3.55 |
| 8 | Create 'high risk' re -payment model for suspect accounts or credit bust-outs | 2.25 | 0.30 | 0.75 | 0.25 | 3.55 |
| 9 | Card Mailing Controls : IVR Failure tracking : Tiered verification strategies : Outbound deliver verification calls | 1.95 | 0.50 | 0.75 | 0.25 | 3.45 |
| 10 | Direct Debit repayments set up from commencement of loan | 1.95 | 0.30 | 0.75 | 0.25 | 3.25 |
| 11 | Process where Open to Buy is only released on cleared funds | 1.50 | 0.30 | 0.75 | 0.25 | 2.80 |
| 12 | Disbursement to customer account. Ability to match customer name to bank account no. | 1.50 | 0.30 | 0.75 | 0.25 | 2.80 |
| 13 | Large value reviews/Velocity Checking process for identifying high risk transactions as part of the revolve capability of the product | 1.50 | 0.30 | 0.75 | 0.25 | 2.80 |
| 14 | Remote Channel - Brand Domain Protection Anti-phishing take-down ability | 1.50 | 0.50 | 0 | 0.25 | 2.25 |
| 15 | Remote Channel - Internet /e-business transaction monitoring : Adaptive Authentication in Host system : Geo-location Analysis | 1.50 | 0.50 | 0 | 0.25 | 2.25 |
| 16 | Implement MasterCard Secure Code or Verified by Visa | 1.50 | 0.30 | 0 | 0.25 | 2.05 |
| 17 | Temporary Shopping Cards : Must be issued for a specified short period of time i.e. 2 weeks : Must only be issued for in store new accounts | 1.50 | 0.30 | 0 | 0.15 | 1.95 |
| 18 | Remote Channel - Card Not Present Authentication MasterCard 3D Secure Code Verified by Visa | 1.20 | 0.50 | 0 | 0.25 | 1.95 |
| 19 | Common Point of Compromise tracking | 1.20 | 0.30 | 0 | 0.25 | 1.75 |
| 20 | Chargeback Tracking | 0.75 | 0.30 | 0 | 0.25 | 1.30 |
| 21 | Process that allows early identification of payments that do not have cleared funds i.e. dishonored cheque process | 0.75 | 0.30 | 0 | 0.25 | 1.30 |
| Section 5: Know Your Staff | | | | | | 3.57 |
| 1 | ISM Capability with Feedback loop to Prevention | 2.70 | 0.30 | 0.75 | 0.55 | 4.30 |
| 2 | IT Security where system access is dictated by role | 2.40 | 0.50 | 0.75 | 0.55 | 4.20 |
| 3 | Whistle blowing and "Zero tolerance" policy documented and communicated at least annually | 2.25 | 0.50 | 0.75 | 0.55 | 4.05 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|--|------|----------|------|------|-------------|
| 4 | Separate approval process and review process for Staff accounts | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 5 | Operations Policy that provides guidelines around Employee accounts. Policy should state that employees should not action or maintain their own (customer) account, nor action or maintain a related parties (customer) account. | 2.25 | 0.30 | 0.75 | 0.45 | 3.75 |
| 6 | Background Employment Screening (See HR guidelines & Also check financial status of employees on an annual basis to ensure they are not in a financial pressure) | 1.95 | 0.50 | 0.75 | 0.45 | 3.65 |
| 7 | Can employees access into other banks beyond the bank they are working for? | 1.95 | 0.30 | 0.45 | 0.45 | 3.15 |
| 8 | Installation of KYS tool - Intellinx/Footprint | 1.95 | 0.30 | 0.45 | 0.25 | 2.95 |
| 9 | Ability to identify staff accounts. | 1.65 | 0.30 | 0.45 | 0.45 | 2.85 |
| 10 | Review process for Branches and Staff receiving Sales bonus's - review at both Branch and individual staff member level | 1.65 | 0.30 | 0.45 | 0.35 | 2.75 |
| Section 6: 3rd Party Payments / Disbursements | | | | | | 3.31 |
| 1 | Payments directly to dealer or supplier, not to customer with proof that supplier is paid | 1.95 | 0.30 | 0.75 | 0.45 | 3.45 |
| 2 | Payments to dealers / suppliers against full documentation | 1.95 | 0.30 | 0.75 | 0.45 | 3.45 |
| 3 | Match bank payment details to staff bank accounts | 1.95 | 0.30 | 0.75 | 0.45 | 3.45 |
| 4 | Disbursement - Model no. of payments and \$ value and payee and review unusual patterns | 1.95 | 0.30 | 0.75 | 0.45 | 3.45 |
| 5 | Independent checking/confirmation when notified of changes to payment details of dealer / supplier | 1.95 | 0.30 | 0.75 | 0.35 | 3.35 |
| 6 | Review triggers for \$ payments by dealer / supplier type | 1.95 | 0.30 | 0.75 | 0.35 | 3.35 |
| 7 | Ability to identify multiple dealer / supplier payment details to same bank account | 1.95 | 0.30 | 0.75 | 0.25 | 3.25 |
| 8 | Bi-Annual Auditing Processes are in place where degree of conformance to standards (listed above) is measured and recorded | 1.65 | 0.30 | 0.45 | 0.35 | 2.75 |
| Section 7: Reporting | | | | | | 3.38 |
| 1 | Fraud cases reported to the bank's head quarter. The amount of reporting should be considered from the percentage of some benchmark for each bank, for example, capital. | 1.95 | 0.50 | 0.75 | 0.75 | 3.95 |
| 2 | Summary report of fraud investigation outlining process weaknesses and Close the Loop action items. The amount of figures should be considered from the percentage of benchmark | 1.95 | 0.50 | 0.75 | 0.55 | 3.75 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|--|---|------|----------|------|------|-------------|
| | for each bank, for example, capital, net asset, and net revenue. | | | | | |
| 3 | Monthly reports relevant to fraud trends and observations. | 1.95 | 0.30 | 0.75 | 0.65 | 3.65 |
| 4 | Fraud Prevention/Detection/ Losses analyzed and reported by process weakness. | 1.95 | 0.30 | 0.75 | 0.65 | 3.65 |
| 5 | Fraud type analysis that provide sufficient details about methods and causes of fraudulent activities. The results can be used to develop or revise fraud scorecard/credit rating. | 1.95 | 0.30 | 0.75 | 0.55 | 3.55 |
| 6 | Key underwriting and transaction data tracked and used for fraud analysis. | 1.95 | 0.30 | 0.75 | 0.55 | 3.55 |
| 7 | Employee's KPIs should be established based on the risk associated with their tasks. | 1.87 | 0.30 | 0.75 | 0.45 | 3.37 |
| 8 | Quarterly reporting that also covers new global standards i.e. fraud to W/O, Fraud to NI, Reporting that is tailored to most relevant metric that would show impact to bottom line for country portfolio. | 1.95 | 0.30 | 0.75 | 0.35 | 3.35 |
| 9 | Monthly reporting: Gross/Net Fraud; Fraud to Sales ; Fraud to Write off, Hidden Fraud Surrogates, 3PD, W/O no payments, Skip/Trace <90MOB; Fraud savings, Investigation, Recoveries. | 1.65 | 0.30 | 0.75 | 0.55 | 3.25 |
| 10 | Fraud Prevention/Detection/ Losses broken down by fraud type. | 1.65 | 0.30 | 0.45 | 0.65 | 3.05 |
| 11 | Monthly reports including follow-up action Items. | 1.65 | 0.30 | 0.45 | 0.65 | 3.05 |
| 12 | Fraud Prevention/Detection/ Losses broken down by portfolio. | 1.65 | 0.30 | 0.45 | 0.55 | 2.95 |
| 13 | Variance analysis and development of control charts. | 1.65 | 0.30 | 0.45 | 0.45 | 2.85 |
| Section 8: Operational Efficiency | | | | | | 3.78 |
| 1 | Fraud alert process across portfolio or mechanism to rapidly inform fraudulent activities to selected members of business units should be developed. | 2.70 | 0.30 | 0.75 | 0.55 | 4.30 |
| 2 | Fraud detection methods should be tailored to needs of individual portfolio. | 2.70 | 0.30 | 0.75 | 0.45 | 4.20 |
| 3 | Fraud Council meeting should be arranged regularly. The members should consist of senior management including CEO, CRO (Chief Risk Officer), COO (Chief Operating Officer) and Compliance Leader. | 2.25 | 0.50 | 0.75 | 0.65 | 4.15 |
| 4 | Fraud analyst should analyze fraud losses and review rule sets in fraud detection tools on an ongoing basis. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| 5 | Responsible staff should be assigned to maintain any fraud detection tools being deployed. In addition, on-going productivity reviews should be conducted. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 6 | Random checks for underwriting process compliance should be performed. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 7 | The procedure for fraud alert process across industry peers should be developed. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 8 | Monitoring unusual incidence of customer complaints from CCRP (Customer Complaints Resolution Process) database should be performed. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 9 | A policy should be developed to cover improper/unusual payment to the government as well as considering impact on bank's image from law and regulations. | 2.40 | 0.30 | 0.75 | 0.55 | 4.00 |
| 10 | Fraud Coordinator should be assigned to coordinate between Fraud Risk Manager and ISM. Moreover, regular meeting between these two groups should be arranged to ensure open communication and close gaps. | 2.40 | 0.30 | 0.75 | 0.45 | 3.90 |
| 11 | Fraud prevention awareness should be raised and communicated regularly in the management level. | 2.10 | 0.50 | 0.75 | 0.55 | 3.90 |
| 12 | Data leakage from both paper-based and electronic-based should be controlled. | 1.95 | 0.50 | 0.75 | 0.55 | 3.75 |
| 13 | Fraud training programs should be conducted for Underwriting staff. | 1.95 | 0.30 | 0.75 | 0.65 | 3.65 |
| 14 | Centrally located underwriting with documented check list of loans should be in place. | 2.10 | 0.30 | 0.75 | 0.45 | 3.60 |
| 15 | Bad debt written off that is collected from customers in later period should be controlled. | 2.10 | 0.30 | 0.75 | 0.45 | 3.60 |
| 16 | The members of the Fraud team should consist of staff from Operations and Analytics. | 1.95 | 0.50 | 0.75 | 0.35 | 3.55 |
| 17 | Risk Management Function should take responsibility from fraud losses. Moreover, the Fraud Coordinator should be appointed as a key liaison point with business units. | 1.65 | 0.50 | 0.75 | 0.65 | 3.55 |
| 18 | Code of conduct should include clear definition of fraud. | 1.95 | 0.30 | 0.75 | 0.55 | 3.55 |
| 19 | Involvement/sign off in CRP and new product innovations (NPI) process. | 1.95 | 0.30 | 0.75 | 0.45 | 3.45 |
| 20 | Formalized fraud policy and procedure should be developed. | 1.65 | 0.50 | 0.75 | 0.45 | 3.35 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------------------------------------|--|------|----------|------|------|-------------|
| 21 | Reward program or incentive should be provided to bank's staff or intermediaries who can prevent/detect fraud. | 2.10 | 0.30 | 0.45 | 0.35 | 3.20 |
| Section 9: Fraud Technology | | | | | | 3.10 |
| 1 | Suspicious activities/transactions or exception reports can be extracted from fraud technology and used for further investigation on a daily basis. | 1.95 | 0.50 | 0.75 | 0.45 | 3.65 |
| 2 | Fraud technology should have the ability to interface directly with the Anti-Money Laundering (AML) application. | 1.50 | 0.50 | 0.75 | 0.65 | 3.40 |
| 3 | Fraud technology should be compatible with existing core banking system. | 1.50 | 0.50 | 0.75 | 0.6 | 3.35 |
| 4 | Fraud detection solution should process efficiently and respond back within targeted period. | 1.50 | 0.50 | 0.75 | 0.6 | 3.35 |
| 5 | Fraud technology should enable the Fraud team or IT staff to maintain the configurations/rules. | 1.65 | 0.30 | 0.75 | 0.65 | 3.35 |
| 6 | Fraud/Internal audit team should have access to their dedicated hardware/server/database. | 1.50 | 0.50 | 0.75 | 0.55 | 3.30 |
| 7 | Banks should implement pre-built software specifically for fraud detection technology. | 1.50 | 0.50 | 0.75 | 0.5 | 3.25 |
| 8 | Banks should have a single platform and workflow tools that automatically execute analytics and data mining to detect unknown patterns. | 1.50 | 0.50 | 0.75 | 0.5 | 3.25 |
| 9 | Banks should implement case management tool with workflow capability. | 1.50 | 0.50 | 0.75 | 0.5 | 3.25 |
| 10 | Fraud technology should have the ability to detect the similarity of names and addresses, for example, Phonetic or Fuzzy logic. | 1.50 | 0.50 | 0.75 | 0.5 | 3.25 |
| 11 | Banks should update fraud detection techniques regularly, at least once a month. | 1.95 | 0.30 | 0.75 | 0.25 | 3.25 |
| 12 | Fraud solution should have the ability to screen data with internal watch lists, for example, bad debts, and political exposed people, etc. | 1.65 | 0.30 | 0.75 | 0.55 | 3.25 |
| 13 | Banks should develop common data model to capture data from different sources and further ease the burden of data extraction process with automated ETL (Extract, Transform, Load) tool. | 1.50 | 0.50 | 0.75 | 0.45 | 3.20 |
| 14 | False positives created from the current technology should be | 1.50 | 0.30 | 0.75 | 0.65 | 3.20 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|--|------|----------|------|------|-------------|
| | reduced due to poor data quality. | | | | | |
| 15 | Banks should own advance data analytical tool that can identify anomalies or suspicious activities. | 1.50 | 0.50 | 0.75 | 0.4 | 3.15 |
| 16 | Fraud technology should be deployed to combat external fraud. | 1.50 | 0.50 | 0.75 | 0.4 | 3.15 |
| 17 | Fraud technology should be deployed to combat internal fraud. | 1.50 | 0.50 | 0.75 | 0.4 | 3.15 |
| 18 | Fraud solution should have the ability to detect fraudulent transactions in real-time and 24 hours a day, 7 days a week. | 1.50 | 0.50 | 0.75 | 0.4 | 3.15 |
| 19 | Fraud technology should allows banks to integrate transactions from different sources/systems such as deposit system, loan origination system, etc. and process them to detect any potential fraud. | 1.50 | 0.50 | 0.75 | 0.4 | 3.15 |
| 20 | As a bank has multiple legacy applications that prevent the Fraud team from diligently consolidating data daily or weekly, the interfacing between fraud detection technology and other legacy systems should be one of the considerations. | 1.65 | 0.30 | 0.75 | 0.4 | 3.10 |
| 21 | Social Network Analysis should be used to detect and visualize fraud. In addition, it should be used to discover previously hidden relationships that are meaningful to the bank. | 1.50 | 0.50 | 0.75 | 0.3 | 3.05 |
| 22 | Multiple views of reporting/dashboard should be generated based on different roles and responsibilities. | 1.50 | 0.30 | 0.75 | 0.5 | 3.05 |
| 23 | Fraud technology should provide the features to calculate risk scores for any potential fraud concerns learnt from previous risk scores as well as adjust the scoring automatically. | 1.50 | 0.30 | 0.75 | 0.45 | 3.00 |
| 24 | Fraud technology should have the ability to prioritize each fraud case according to risk scores and notify suspicious activities to the management. | 1.50 | 0.30 | 0.75 | 0.45 | 3.00 |
| 25 | Fraud detection solution should enable users to design and generate a report template, which can be used by different groups of users. Moreover, it should allow users to generate a report from data being stored in risk management system through the Microsoft Office tools, such as Word, Excel and PowerPoint. | 1.65 | 0.30 | 0.75 | 0.25 | 2.95 |
| 26 | Banks should leverage Business Intelligent (BI) and other relationship database/data warehouse to enhance the ability of money laundering detection. | 1.50 | 0.30 | 0.75 | 0.4 | 2.95 |
| 27 | Fraud technology should be supported by a vendor representative/service provider which exists in Thailand to provide | 1.20 | 0.30 | 0.75 | 0.5 | 2.75 |

| Rank | Description | Bank | Non-Bank | FMC | PwC | Total score |
|------|---|------|----------|------|------|-------------|
| | faster and efficient support. | | | | | |
| 28 | Banks should develop home-grown fraud detection solutions and routines using data analysis software such as ACL, IDEA, etc. | 1.20 | 0.30 | 0.75 | 0.5 | 2.75 |
| 29 | The pre-built data model should be created for the bank's existing systems. | 0.75 | 0.30 | 0.75 | 0.45 | 2.25 |
| 30 | Fraud technology should be designed on web-based or client/server architecture which is compatible to the Internet Explorer. Moreover, it should support Thai language correctly. | 0.90 | 0.30 | 0.45 | 0.35 | 2.00 |