Taxonomy of Fraud in Microfinance

A joint collaboration of Fraud Doctor LLC, OXUS Afghanistan, Microfinance Investment Support Facility for Afghanistan (MISFA), Association of Certified Fraud Examiners (ACFE), & Italian Support to Afghan Microfinance & Enterprises (ISAME).

November 2015

Acknowledgements

The development of the Taxonomy of Fraud in Microfinance was coordinated by Fraud Doctor LLC, OXUS Afghanistan of OXUS Development Network, Microfinance Investment Support Facility for Afghanistan (MISFA), and the Association of Certified Fraud Examiners (ACFE). Funding for this project was provided by a grant from the Italian Development Cooperation, specifically from the Italian Support to Afghan Microfinance & Enterprises (ISAME) project given to OXUS Afghanistan as facilitated through MISFA.

This report was prepared by Alexis C. Bell of Fraud Doctor LLC, with significant input from the *Taxonomy of Fraud in Microfinance* working group.

Working Group Members

- Alexis C. Bell, Managing Member, Fraud Doctor LLC
- Mohammad Jawad Safari, Head of Legal, OXUS Afghanistan
- Payenda Wafa, Audit Manager, OXUS Afghanistan
- Iraj Sayedi, Risk Manager, OXUS Afghanistan
- Edouard Sers, Head of Internal Audit & Risk, OXUS Development Network
- Shahzad Nisar, Deputy Director of Monitoring & Supervision Dept., MISFA
- Mirwais Waak, Senior Technical Support Officer, MISFA
- John Warren, VP & General Counsel, ACFE
- Andi McNeal, Director of Research, ACFE

Contact Information for Participating Organizations

- Fraud Doctor LLC: http://www.fraud-doctor.com
- OXUS Afghanistan: http://www.oxusnetwork.org/en/our-microfinance-institutions/oxus-afghanistan
- OXUS Development Network: http://www.oxusnetwork.org/en/about-us/management-team
- MISFA: http://www.misfa.org.af/
- ACFE: http://www.acfe.com/
- Italian Development Cooperation: http://www.coopitafghanistan.org/

Table of Contents

Background

One of the challenges we face in the antifraud industry is the lack of congruity between various thought leaders in how we define fraud and its many schemes. Each industry group or academic expert added great value to the advancement of the antifraud field. However, while every new distinction created a little more clarity, they all seemed to be inputs into a larger equation of the dynamic nature of what we face on a daily basis. In an effort to create a standardized fraud classification system that would apply across all fraud schemes, the *Framework for a Taxonomy of Fraud* was published by the Stanford Center on Longevity in July of 2015. It really was the first time a coding scheme was attempted that would allow for the vast universe of fraud schemes whether it be against an individual or an organization, from an insider threat such as from occupational fraud, against the public or private sector, or even industry specific fraud schemes.

The ability to have a common language and classification system across the fraud landscape affords us the opportunity to consistently measure fraud events so that we can begin to glean important information from more sophisticated data analysis. Having everyone on the same page gives us more data to analyze since the criteria for the inputs are alike when reporting fraud events. Being able to compare trends for the creation of industry & geographic baselines allows for the determination of risk appetite, tolerance levels (+/- %), key risk indicators (KRIs), identification of anomalies, and the development of predefined management actions and communication strategy in response to exception reporting. Organizations can now begin to shift from a purely reactionary response to a proactive model where prevention is the focus. The taxonomy of fraud is the first step in that process.

In addition to improvements in data analysis, the taxonomy provides advancement in the investigative component of an antifraud program. In general, as an investigator, if you know what scheme is likely involved, you know which people to interview based on who had access to those assets, you know what questions to ask, what data to analyze, the tests to run against that data, which documents to review, and the rest just falls into place. The scheme is the driving force behind what elements are required in terms of evidence to substantiate or refute allegations of fraud in court. That determines what must be addressed in the investigative report. It also provides a backdrop for training design related to investigators as well as fraud awareness training for business units (employees), clients and suppliers. It even affects the reporting mechanisms for suspicion of fraud.

This report is a collaborative effort to create and define the taxonomy for fraud related to the microfinance industry. It is our hope that it will be the springboard for the industry to foster collaboration in antifraud efforts and of global analysis of aggregate data so that together we can take a stand against fraud.

Prerequisite Reading

The taxonomy of fraud in microfinance concepts and structure are based on the following report published in July:

Stanford Center on Longevity. (2015). *Framework for a Taxonomy of Fraud*. Stanford, California: Stanford University, Financial Fraud Research Center of the Stanford Center on Longevity. Retrieved 22 July 2015, from: http://longevity3.stanford.edu /framework-for-a-taxonomy-of-fraud/

Applicability

All organizations are at risk for fraud schemes where an employee uses their job to facilitate the fraud. These kinds of schemes are known as "Occupational Fraud Schemes" and are defined by the Association of Certified Fraud Examiners (2012, p. 6) as:

> *The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.*

The Association of Certified Fraud Examiners (ACFE) places occupational fraud into three primary categories: (1) Asset Misappropriation, (2) Corruption, and (3) Fraudulent Statements.

The only schemes which could be considered excluded are those dependent on functional areas not currently within the operations of the MFI (Microfinance Institution) such as manufacturing. While occupational fraud applies to all companies regardless of the industry or geographic location, organizations are also at risk for industry specific fraud as well as external threats such as cybercrime and infiltration by organized crime syndicates.

Geographic location can increase the risk for fraud; especially given the countries in which MFIs operate. According to the *2008/2009 Global Fraud Report* (Kroll, p. 7), "Fraud is most prevalent in less developed economies… [N]otably those in the Middle East and Africa – have experienced much more [fraud]." For example, Afghanistan ranks number one in the Corruption Perceptions Index (Transparency International, 2013) alongside both Somalia and North Korea. Additionally, gangs and other forms of organized crime operate in the same countries in which many MFIs have a presence. While gang activity is typically controlled by and concentrated in large metropolis areas, they have a reach in even small, remote villages. Operations in Latin America and Eurasia are particularly vulnerable to the influences of organized crime.

In conclusion, the fraud schemes listed in the following section(s) [1] apply to MFIs and all of their subsidiaries. The only schemes excluded are those dependent on functional areas that are not currently part of the MFI's operations [2]. Certain factors such as geographic location can increase the level of risk, but the inherent risk still exists for all non-excluded fraud schemes.

Approach

The *Framework for a Taxonomy of Fraud* (July 2015, p. 7) defined fraud as, "*Intentionally and knowingly deceiving the victim by misrepresenting, concealing, or omitting facts about promised goods, services, or other benefits and consequences that are nonexistent, unnecessary, never intended to be provided, or deliberately distorted for the purpose of monetary gain.*" However, given that fraud committed against an organization can include schemes that are broader than the definition used or where the fraudster does not directly benefit monetarily, the *Black's Law Dictionary* (2004) definition of fraud was used as a more encompassing definition, "*A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.*"

In addition, while the *Framework for a Taxonomy of Fraud* (July 2015) specifically excluded identity theft as a scheme, we included it as it is an essential scheme committed against organizations in microfinance. By including it within the

[1] This is not an all-inclusive list of fraud schemes. For example, there are a host of cybercrimes not listed which pose a fraud risk to MFIs such as data breech, account takeovers, malware, and website defacing to just name a few. Additionally, with each new channel introduced into the product line of the MFI new industry specific fraud schemes unique to that channel become risks as well.

[2] Excluded fraud schemes which are dependent on functional areas that are not part of the MFI's operations have been included in the fraud scheme(s) listing for two reasons: (1) In the event the MFI decides to incorporate that functional area into operations in the future, and (2) The potential applicability to fraud committed against the MFI by a supplier, vendor, client, or other external party that does have the functional area as part of their operations.

taxonomy the specific risk is highlighted so MFIs (microfinance institutions) can begin to put mechanisms in place to mitigate the risk for identity theft.

Within the taxonomy, the first question asked when attempting to classify a fraud scheme is in Level 1: Who is the target? Is the target (victim) of the fraud an individual or an organization? The *Framework for a Taxonomy of Fraud* (July 2015, p. 9) focused primarily on fraud committed against an individual. As such, the distinctions for fraud committed against an organization were largely left unaddressed. In microfinance, the majority of the fraud schemes are committed against the organization. Therefore, we determined the organization (*category 2*) element of the taxonomy would be the main focus of the working group.

We determined that the schemes would typically fall into two scenarios. First, there are schemes commonly seen in microfinance that are also found in all organizations. We refer to those as "Core Fraud". We noted that these types of schemes were already defined and addressed by the Association of Certified Fraud Examiners (ACFE) in occupational fraud schemes committed by employees. According to the ACFE, occupational fraud is defined as, "*The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.*" Schemes already defined by occupational fraud were classified using the existing naming and definition convention established by the ACFE.

The second scenario involved fraud schemes that were industry specific. Although microfinance is an industry by itself, we found that the industry schemes affecting microfinance also applied to all financial institutions with lending practices. Therefore, we determined that the industry hierarchy and resulting nesting would be left at the higher more encompassing level of financial institution. This would allow for the later classification of other schemes noted in the larger banking industry. It would also be in line with the requirement of schemes being mutually exclusive from one another and reduce the potential for industry specific overlap.

The hierarchy and nesting of fraud schemes were only included as to seven levels in. While additional scheme names and definitions have been defined in other publications, for the purposes of this report, we only included up to seven levels.

In addition, although microfinance organizations like all other companies are at risk for hundreds if not thousands of different fraud schemes, the majority of the industry schemes center around the lending process. As such, we focused on the highest frequency fraud schemes and those happen to involve the lending process. It should be noted however, that while microfinance is not immune to issues involving InfoSec (information security) and cyber crime, we determined those types of fraud schemes warranted their own report. This paper does not incorporate cyber specific crimes. A more detailed classification on that topic should be addressed on a later date.

Each scheme can be coded to reflect additional attribute details. Attributes of method of advertising the fraud, purchase setting, and method of money transfer were all considered. However, the general incident tags did not provide a subset of detail for one common aspect; rather they were details of differing elements. For example, AF – affinity fraud is detail about the victim whereas PS – pyramid scheme, PZ – ponzi scheme, IG – impersonated government official, PD - pump & dump scheme, CS – continuity scam, OV – overpayment fraud, and CP – counterfeit payment instrument are fraud schemes and HM – health or medical related fraud is a specific industry. Therefore, the general incident tags were not used during this the coding of the microfinance schemes.

Lastly, the *Framework for a Taxonomy of Fraud* (July 2015, p. 40) classified Level 2 as either 2.1 governmental fraud or 2.2 non-governmental fraud. At first glance, this distinction seemed plausible. However, after going through the exercise of attempting to classify the organizational fraud schemes, we found that this grouping made it difficult to maintain the criteria of mutual exclusiveness. Therefore, it is suggested that Level 2 be updated to reflect the following:

- 2.1 Core Fraud: Fraud schemes that apply to all organizations regardless of the sector (public/private) or industry;
- 2.2 Governmental Fraud: Fraud committed against government agencies, programs, regulations, & society; and
- 2.3 Industry Fraud: Fraud schemes found only in certain industries.

This allows for the differentiation of schemes that apply to all organization regardless of the sector or industry, public (government) versus private (industry), and industry specific fraud schemes.

Example Scenario

A loan officer creates a fictitious (fake) client in the system. Counterfeit loan documents are created for the file to make it appear as if the fictitious client is a real person. Upon disbursement of the loan, the loan officer pockets (keeps) the money for himself.

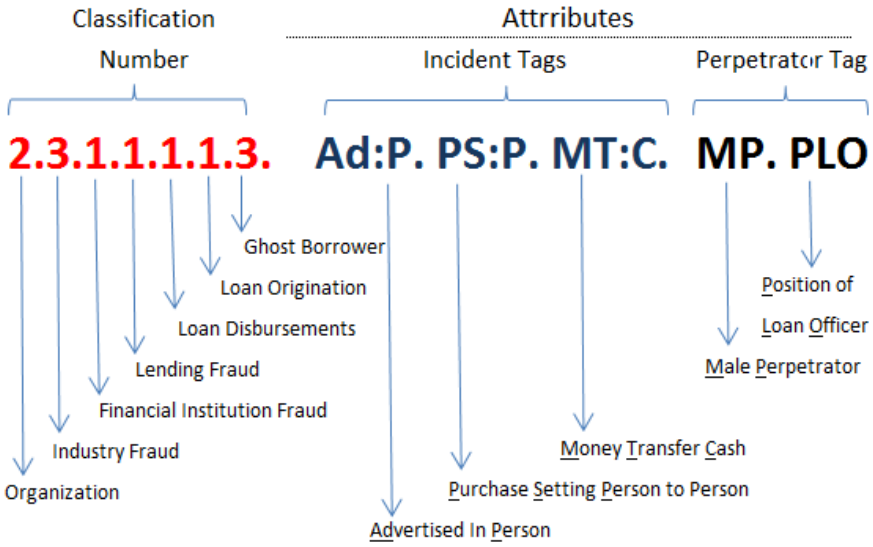
In this case, there are two fraud schemes. The primary scheme is **Ghost Borrower** where the classification is as follows:

Level 1: 2 Organization
Level 2: 2.3 Industry Fraud
Level 3: 2.3.1 Financial Institution Fraud
Level 4: 2.3.1.1 Lending Fraud
Level 5: 2.3.1.1.1 Loan Disbursements
Level 6: 2.3.1.1.1.1 Loan Origination
Level 7: 2.3.1.1.1.1.3 Ghost Borrower

The attributes in this scenario for the primary scheme of Ghost Borrower include the following:

Method of Advertising: Ad:P In Person
Purchase Setting: PS:P Person to Person
Method of Money Transfer: MT:C Cash
Victim Tags: n/a (apply only for fraud committed against an individual)
Perpetrator Tags: MP Male Perpetrator; PLO Position of Loan Officer

GHOST BORROWER



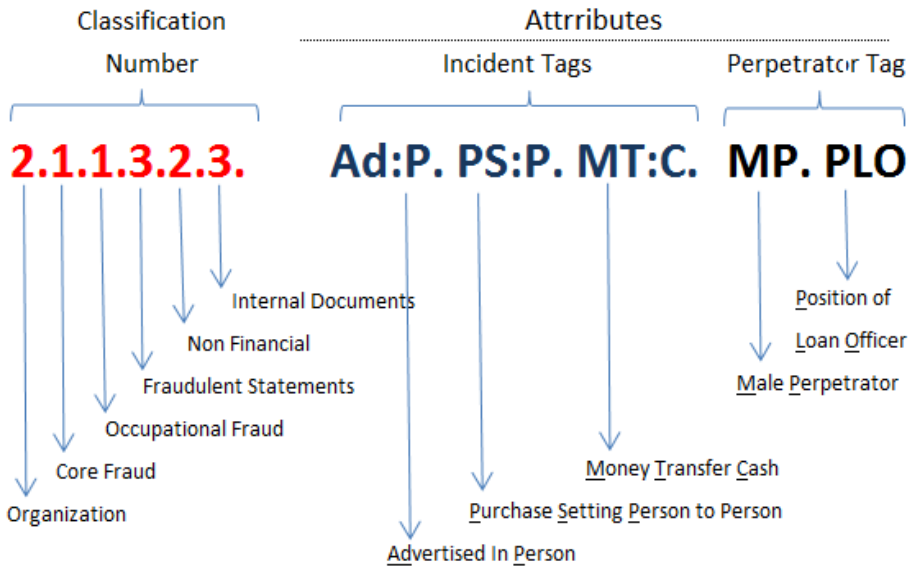
In addition, the secondary or supporting scheme [3] is counterfeit **Internal Documents** where the classification is as follows:

Level 1: 2 Organization
Level 2: 2.1 Core Fraud
Level 3: 2.1.1 Occupational Fraud
Level 4: 2.1.1.3 Fraudulent Statements
Level 5: 2.1.1.3.2 Non Financial
Level 6: 2.1.1.3.2.3 Internal Documents
Level 7: n/a

The attributes in this scenario for the supporting scheme of counterfeit Internal Documents are the same as with the primary scheme of Ghost Borrower and include the following:

Method of Advertising: Ad:P In Person
Purchase Setting: PS:P Person to Person
Method of Money Transfer: MT:C Cash
Victim Tags: n/a (apply only for fraud committed against an individual)
Perpetrator Tags: MP Male Perpetrator; PLO Position of Loan Officer

INTERNAL DOCUMENTS



[3] A secondary or supporting fraud scheme is one that is perpetrated so that the primary fraud scheme can be more successful. In this example, the counterfeit internal documents created for the fictitious client's loan file potentially aided the fraudster in lessoning the possibility of detection. A blank loan file would have raised more suspicion.

Classification Categories

(1) Individual Fraud

This refers to intentionally and knowingly deceiving the victim by misrepresenting, concealing, or omitting facts about promised goods, services, or other benefits and consequences that are nonexistent, unnecessary, never intended to be provided, or deliberately distorted for the purpose of monetary gain (Stanford, 2015). [4]

> *This would typically be seen in MFI (microfinance institution) instances when an employee commits a fraud against a client.*
>
> *Individual Fraud poses an opportunity for the MFI to educate their clients about the possibility of being cheated or scammed by both dishonest employees and nefarious outsiders (external threats). The MFI should consider communicating to the client that the company would never condone an employee stealing from them and provide a mechanism for the client to inform the MFI of potential wrongdoings such as a hotline or complaint box at the branch. Lastly, the MFI should consider including verbiage in their contracts with clients that address these topics and provisions should be explained during the disbursement phase of the loan award.*

1.1 Consumer Investment Fraud

NOTE: Does not specifically relate to MFI

1.2 Consumer Products & Services Fraud

This broad category covers all fraud related to the purchase of tangible goods and services. It also includes vacations and travel, house/apartment rentals, purchase of pets, concerts/performances, and other events or items the victim paid for but did not receive as promised. The category is further subdivided based on whether the fraud deals with a product, a service, or unauthorized billing. This broad category includes many fraud schemes, including bogus loans, worthless products, phony insurance, products paid and never received, unnecessary repairs, and many others (Stanford, 2015).

1.2.1 Worthless or Non-Existent Products – *the sub-schemes typically do not apply to MFI*

1.2.2 Worthless, Unnecessary, or Non-Existent Services -

> […] [5]
>
> 1.2.2.7 Fake Credit Lines & Loans - These scams are often targeted at people with bad credit or in need of a loan. … a victim is informed they qualify for a loan … but first must pay money up front. The victim pays the money, but no loan … is issued (Stanford, 2015).
>
> > 1.2.2.7.1 Fake Loans - Often called "advance fee loans," in this scam the consumer receives a phone call or is prompted to click on a link stating that the consumer qualifies for a loan and that the loan is not dependent on the consumer's credit history. Before the loan is issued, a fee must be paid and the consumer may be asked to provide personal identifying information. Consumers may be told that the fee is for a security deposit, loan processing, or other paperwork, but the lender's fee structures are not properly disclosed and the loan is never provided (Stanford, 2015).

1.3 Employment Fraud

NOTE: Does not specifically relate to MFI

[4] Fraud committed against an Individual is addressed by the original report *Framework for a Taxonomy of Fraud*. Further exploration as it specifically relates to microfinance should be addressed at a later time in greater detail.
[5] Other non-applicable schemes were not included, but can be reviewed in the original report *Framework for a Taxonomy of Fraud*.

1.4 Prize & Grant Fraud

NOTE: Does not specifically relate to MFI

1.5 Phantom Debt Collection Fraud

NOTE: Does not specifically relate to MFI

1.6 Charity Fraud

This category of fraud involves scam artists collecting money by posing as a genuine charity. There is no expected benefit or product/service resulting from the transaction. Instead, the expected outcome from the perspective of the victim is organized charitable giving. This category is sub-divided into bogus charitable organizations and crowdfunding for bogus causes depending on whether the fraudulent entity is supposedly a non-profit organization or an online crowdfunding account where individuals can donate money (Stanford, 2015).

1.6.1 Bogus Charitable Organization - A sub-type of charity fraud in which the fraudsters collect donations by pretending to be genuine non-profit organizations representing a variety of causes, from natural disaster relief to children's issues (Stanford, 2015).

Examples include: A fraudster contacts a community leader and tells him if the community leader can get the villagers to obtain loans at the MFI, the money should be given to the fraudster so he can then give the funds to a charitable organization in another country. In return, the fraudster promises to make all of the repayments to the MFI on behalf of the villagers (clients). The villagers would be considered as helping a worthy cause. This scam has been known to spread throughout multiple neighboring communities as the fraudster uses one community leader as a reference to another. In the end, the villagers give all of the loan disbursements to the fraudster who then escapes with the money. The villagers are left with a debt obligation and no influx of working capital into their business.

1.7 Relationship & Trust Fraud

NOTE: Does not specifically relate to MFI

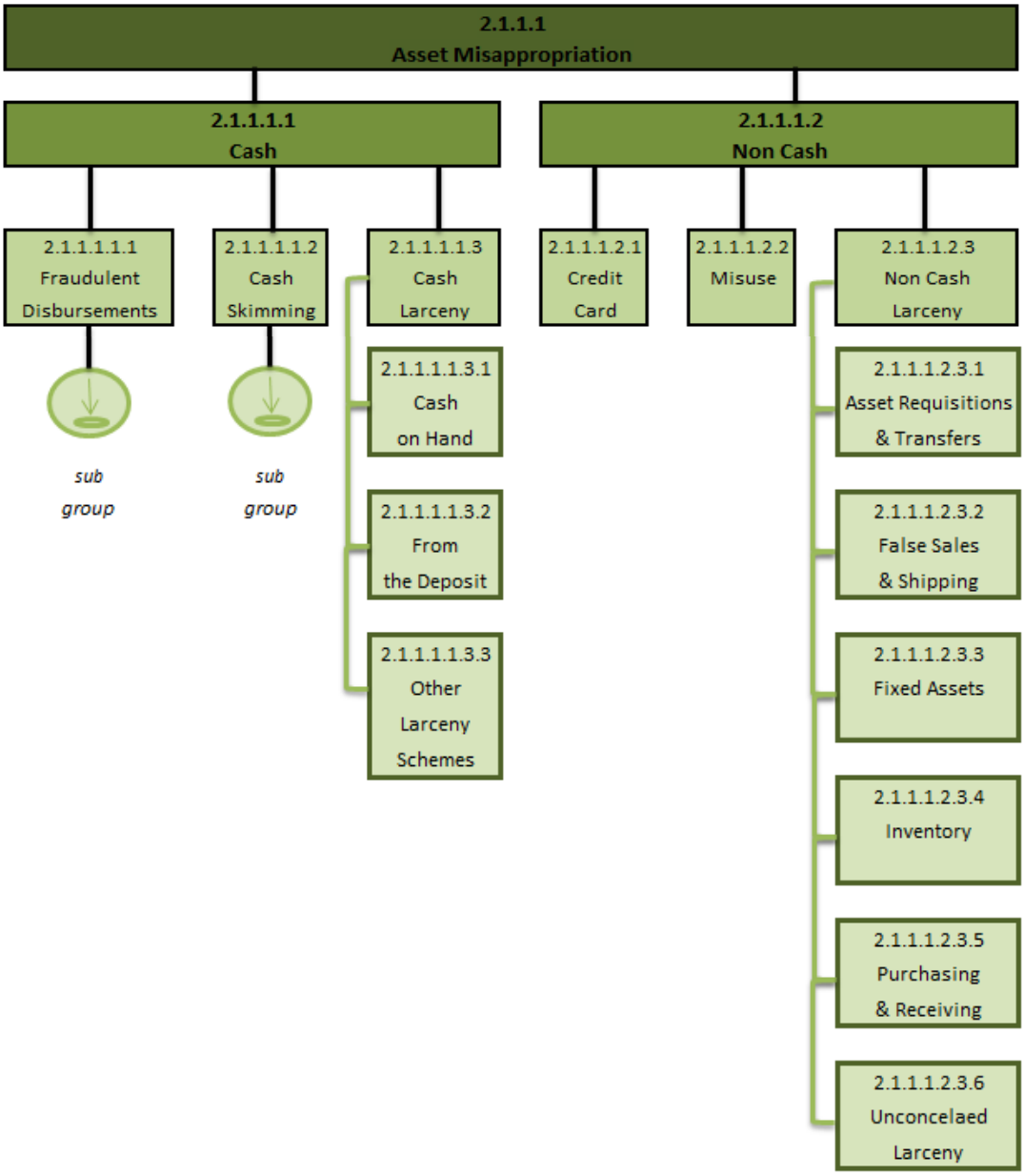
(2) Organizational Fraud

A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment where fraud is committed against an organization.

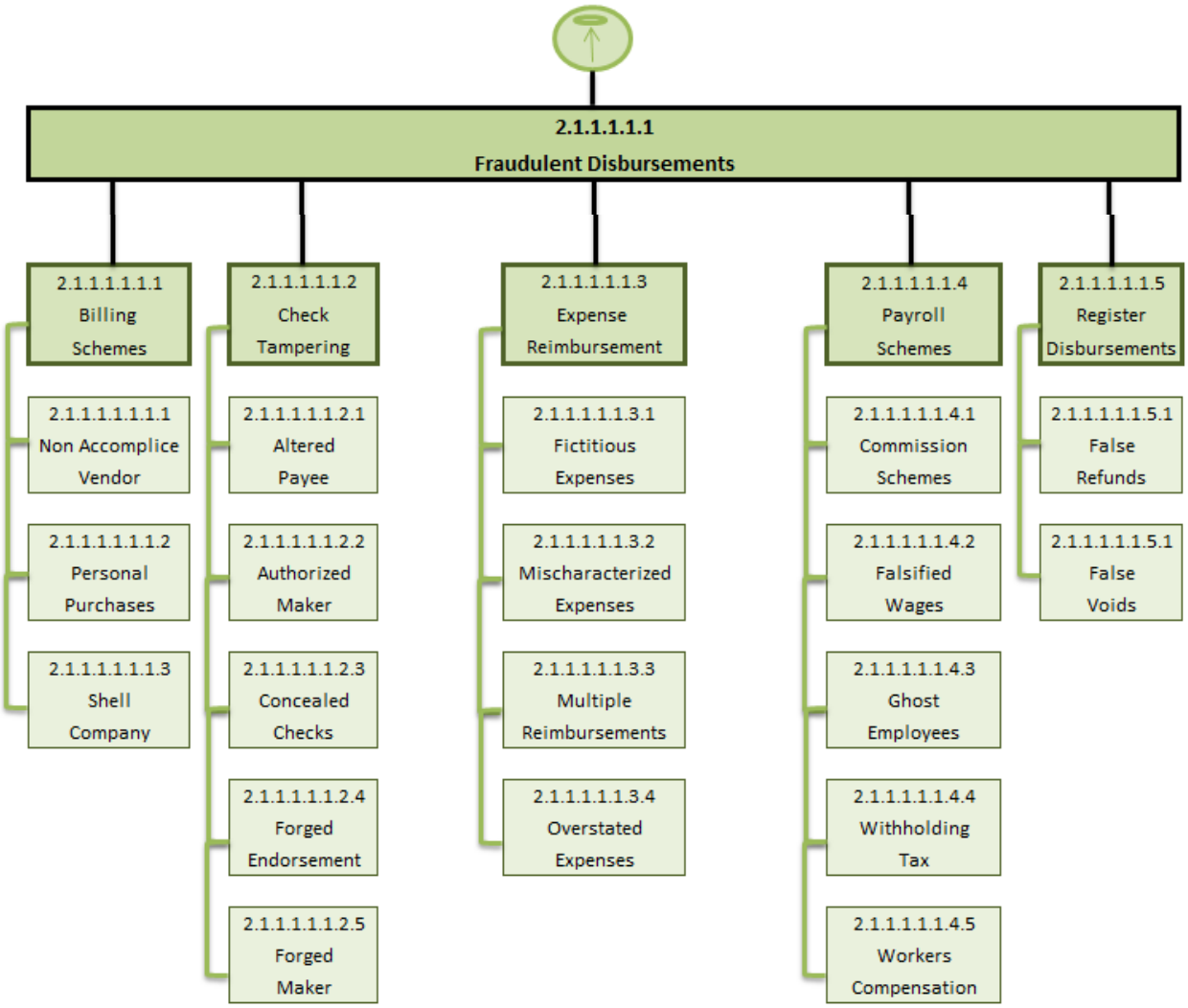
2.1 Core Fraud

Fraud schemes that apply to all organizations regardless of the sector (public/private) or industry.

2.1.1 Occupational Fraud - The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. [6]



[6] Not all of the Occupational Fraud schemes have been listed. Only the most common (highest frequency) schemes have been included in this report. They represent the starting point for MFIs to address when implementing mitigating controls. However, all of the schemes should be considered once that exercise has been completed.



2.1.1.1 Asset Misappropriation - Theft of assets.

Asset misappropriation schemes include those frauds in which a perpetrator employs trickery or deceit to steal or misuse an organization's resources. The distinguishing elements of asset misappropriation are that an organization's assets are taken through trickery or deceit, rather than by force.

2.1.1.1.1 Cash - Cash misappropriation involves the misuse or theft of an organization's cash.

2.1.1.1.1.1 Fraudulent Disbursements - Fraudulent disbursement schemes are those in which a distribution of funds is made from some company account in what appears to be a normal manner, but is actually fraudulent. The method for obtaining the funds may be the forging of a check, the submission of a false invoice, the doctoring of a time card, and so on. The key difference between fraudulent disbursement schemes and cash larceny schemes is in the former, the money is moved from the company in what appears to be a legitimate disbursement of funds (Singleton & Singleton, 2010).

2.1.1.1.1.1.1 Billing Schemes - Any scheme in which a person causes his or her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices or invoices for personal purchases. Billing schemes use the company's accounting system to steal funds by submitting bogus claims in one form or another (Singleton & Singleton, 2010).

2.1.1.1.1.1.2 Check Tampering - Check tampering is any scheme in which a person steals his or her employer's funds by intercepting, forging or altering a check drawn on one of the organization's bank accounts (Association of Certified Fraud Examiners, 2012).

Check tampering is unique among fraudulent disbursements because it is the one group of schemes in which the perpetrator physically prepares the fraudulent check (Wells, Principles of Fraud Examination, 2010).

Check tampering schemes depend on factors such as access to the company checkbook, access to bank statements, and the ability to forge signatures or alter other information on the face of the check (Wells, Principles of Fraud Examination, 2010).

2.1.1.1.1.1.3 Expense Reimbursement Schemes - Expense reimbursement schemes occur when employees make false claims for reimbursement of fictitious or inflated business expenses.

Expense reimbursements are usually paid by organizations in the following manner: An employee submits a report detailing an expense incurred for a business purpose, such as a business lunch with a client, airfare, or hotel bills associated with business travel.

In preparing the expense report, the employee usually must explain the business purpose for the expense as well as the time, date and location in which it was incurred. Attached to the report should be supporting documentation for the expense, typically a receipt. The report usually must be authorized by a supervisor in order for the expense to be reimbursed (Kranacher, Riley, & Wells, 2010).

2.1.1.1.1.1.4 Payroll Schemes - Payroll schemes occur when an employee fraudulently generates overcompensation on his or her behalf. These schemes are similar to billing schemes, in that the perpetrator generally produces some false document or otherwise makes a false claim for a distribution of funds by his employer. In payroll schemes, the false claim generally occurs when the fraudster falsifies payroll records, timekeeping records, or some other document concerned with the payroll function (Association of Certified Fraud Examiners, 2012).

Examples include: A commission scheme where a loan officer's delinquent loans are transferred to a supervisor. This makes PAR [7] look better than it should thereby making it possible for a loan officer to receive commission (incentives) more than they are entitled to.

2.1.1.1.1.1.5 Register Disbursements - Two basic fraudulent schemes take place at the register: false refunds and false voids (Albrecht, Albrecht, & Kimbleman, 2008).

Refunds and voided sales are transactions processed at the register when a customer returns an item of merchandise purchased from that store. The transaction entered on the register indicated the merchandise is being replaced in the store's inventory and the

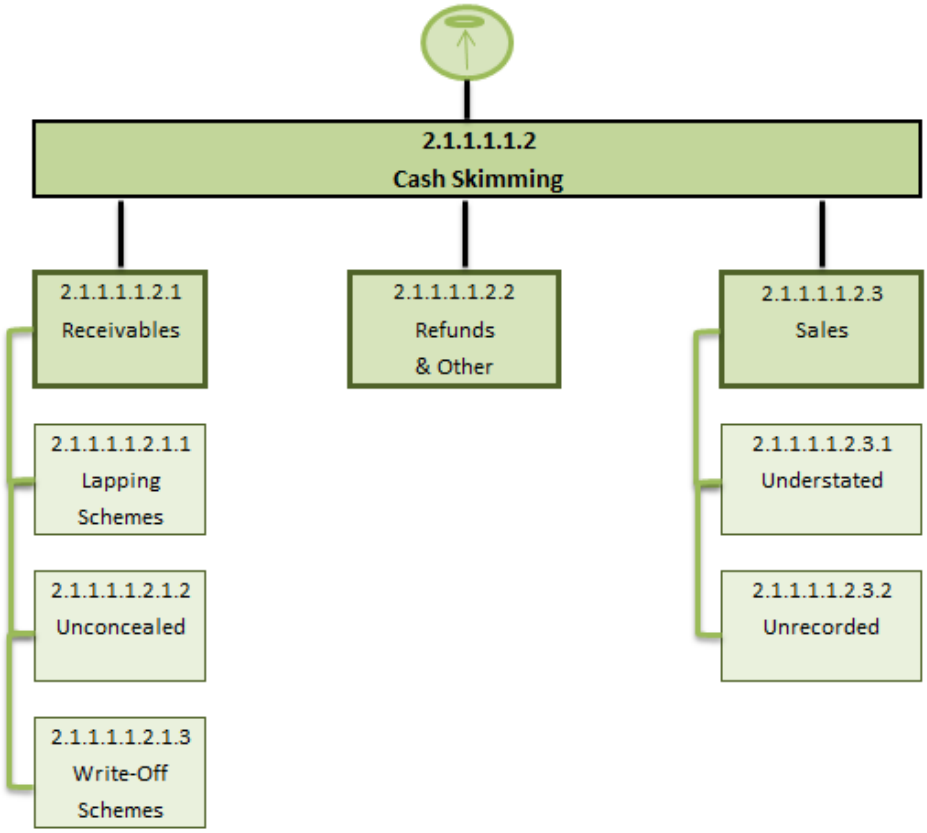
[7] Portfolio at Risk (PAR). See the Appendix for a compete definition.

purchase price is being returned to the customer. In other words, a refund or void shows a disbursement of money from the register as the customer gets his money back.

Fraudulent refunds and voids represent a class of occupational fraud that is a hybrid between cash theft and fraudulent disbursements. Since these schemes appear on the books as legitimate disbursements of funds from the cash register, they are classified as fraudulent disbursements. In practice, an employee physically removes cash from his cash register and absconds with it. In that respect, such schemes are very similar to cash larceny schemes (Association of Certified Fraud Examiners, 2012).

Skimming: *before recorded in the system.*

Larceny: *after recorded on the books.*



2.1.1.1.1.2 Cash Skimming - Skimming is the process by which cash is removed from the entity before it enters the accounting system. This is an "off-book scheme" because the receipt of the cash is never reported to the entity. This aspect of skimming schemes means they leave no direct audit trail. Consequently, it may be very difficult to detect that the money has been stolen.

Skimming can occur at any point where cash enters a business, so almost anyone who deals with the process of receiving cash may be in a position to skim money. This includes salespeople, tellers, waitpersons, and others who receive cash directly from customers (Association of Certified Fraud Examiners, 2012).

2.1.1.1.1.2.1 Receivables - Skimming receivables may be more difficult to conceal than skimming sales because receivables payments are expected. The victim company knows the customer owes money and is waiting for the payment. In a revenue skimming scheme where a sale goes unrecorded, it is as if the sale never existed. Receivables skimming, by contrast, may raise questions about missing payments (Wells, Corporate Fraud Handbook: Prevention and Detection, 2011).

Examples include: (See the Appendix for supplemental details)

- ***Lapping:*** *The loan officer takes a portion of an installment payment (repayment) and keeps it for himself, but uses another client's repayment to make up the difference for the first client.*
- ***Unconcealed:*** *The loan officer collects the installment payment (repayment) in the field and pockets (keeps) the cash.*
- ***Unconcealed:*** *The loan officer collects a partial installment payment (repayment) in the field and pockets (keeps) the cash.*
- ***Unconcealed:*** *The loan officer accepts the installment payment (repayment) from the client and a penalty amount, but does not enter the penalty into the system* [8] *and pockets (keeps) the penalty portion of the cash.*
- ***Write-Off:*** *an employee deliberately stalls recovery for loans so that loans are written-off after a threshold, e.g. 180-days past due.*

Skimming: *before recorded in the system.*

Larceny: *after recorded on the books.*

2.1.1.1.1.3 Cash Larceny - A cash larceny may be defined as the intentional taking of an employer's cash (the term cash includes both currency and checks) without the consent and against the will of the employer.

Cash larceny involves the theft of cash by employees after it has been recorded on the entity's books. For this reason it is easier to detect larceny than it is to detect skimming (Association of Certified Fraud Examiners, 2010).

Examples include:

- *The loan officer accepts the installment payment (repayment) from the client and a penalty amount, but reverses (waives) the penalty in the system* [9] *and pockets (keeps) the penalty portion of the cash.*

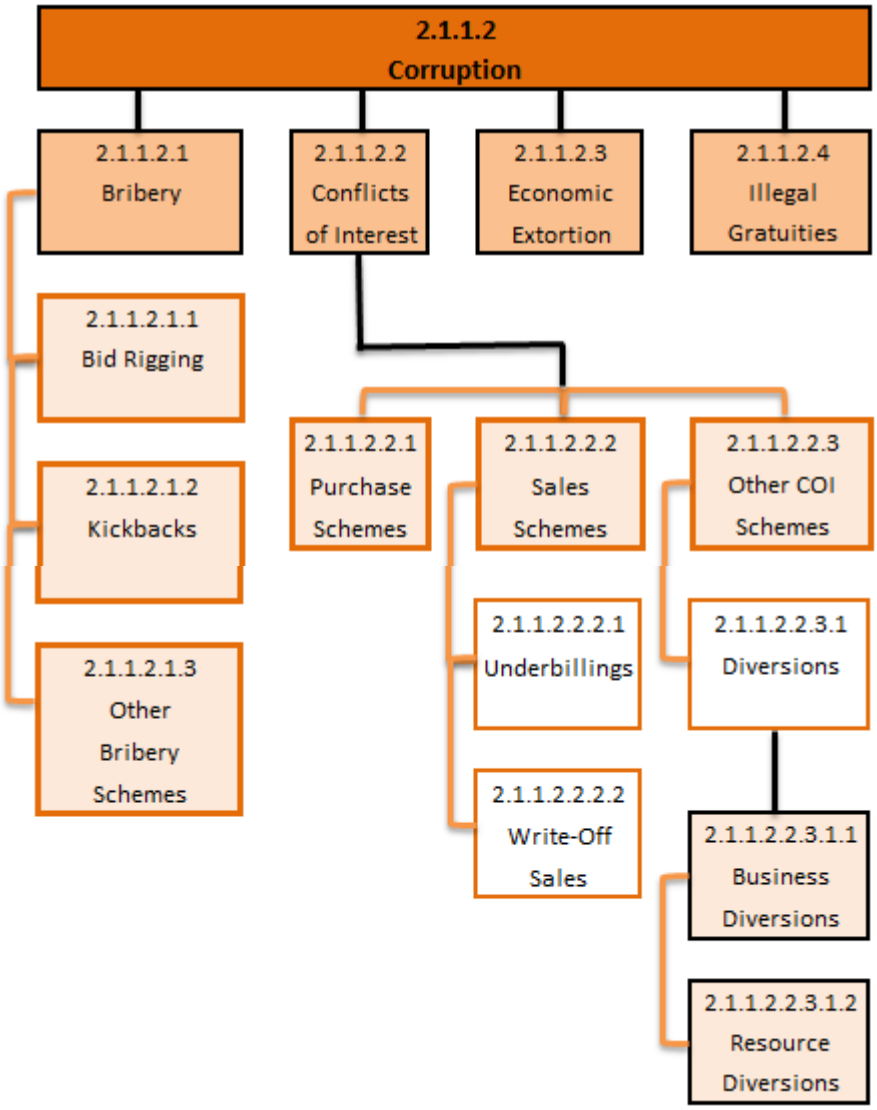
2.1.1.1.2 Non Cash - Employees target inventory, equipment, supplies, and other non-cash assets for theft in a number of ways. These schemes can range from stealing a box of pens to the theft of millions of United States Dollars' (USD) worth of company equipment.

2.1.1.2 Corruption - The misuse of power, office, or authority for private benefit—through bribery, extortion, influence peddling, nepotism, fraud, speed money or embezzlement.

2.1.1.2.1 Bribery – Bribery is the offering, giving, receiving, or soliciting anything of value to influence an official act or business decision (Wells, Principles of Fraud Examination, 2010).

The term official act means that traditional bribery statutes proscribe only payments made to influence the decisions of government agents or employees. Commercial bribery cases deal with the acceptance of under-the-table payments in return for the exercise of influence over a business transaction (Kranacher, Riley, & Wells, 2010).

[8] If a reversing entry or waiver is entered into the system for the penalty fee, then it is a larceny scheme and not a skimming scheme.
[9] If the books and records (system) are not manipulated to account for the reduced cash amount equal to the penalty fee, then it is a skimming scheme and not a larceny scheme.



2.1.1.2.1.1 Bid Rigging – Bid rigging schemes occur when an employee fraudulently assists a vendor in winning a contract through the competitive bidding process.

NOTE: See the Appendix for supplemental information.

2.1.1.2.1.2 Kickbacks – Kickbacks are undisclosed payments made by vendors to employees of purchasing companies. The purpose of a kickback is usually to enlist the corrupt employee in an overbilling scheme.

Kickbacks are classified as corruption schemes rather than asset misappropriations because they involve collusion between employees and vendors; in asset misappropriation, no outsiders are knowing participants (Kranacher, Riley, & Wells, 2010).

Examples includes: Kickback payments made by vendors and suppliers to an employee.

In a common type of kickback scheme, a vendor submits a fraudulent or inflated invoice to the victim company and an employee of that company helps make sure that a payment is made on the

false invoice. For his assistance, the employee/fraudster receives some form of payment from the vendor. This payment is the kickback (Kranacher, Riley, & Wells, 2010).

2.1.1.2.1.3 Other Bribery Schemes - Bribes are not always paid to employees to process phony invoices. In some circumstances outsiders seek other fraudulent assistance from employees of the victim company. In other cases, bribes come not from vendors who are trying to sell something to the victim company, but rather from potential purchasers [clients] who seek a lower price from the victim company (Kranacher, Riley, & Wells, 2010).

Examples includes: Kickback payments made to an employee prior to the loan disbursement by a client in order to process a loan faster than policy allows (due to verification processes) or one that the client would not otherwise be entitled to receive.

2.1.1.2.2 Conflicts of Interest – A conflict of interest is a situation that has the potential to undermine the impartiality of the person because of the possibility of a clash between the person's self-interest and professional or public interest (Kapka).

The vast majority of conflict of interest cases occur because the fraudster has an undisclosed economic interest in a transaction. But the fraudster's hidden interest is not necessarily economic. In some scenarios an employee acts in a manner detrimental to his company in order to provide a benefit to a friend or relative, even though the fraudster receives no financial benefit from the transaction himself.

In order to be classified as a conflict of interest scheme, the employee's interest in the transaction must be undisclosed. The crux of a conflict case is that the fraudster takes advantage of his employer; the victim organization is unaware that its employee has divided loyalties. If an employer knows of the employee's interest in a business deal or negotiation, there can be no conflict of interest, no matter how favorable the arrangement is for the employee (Association of Certified Fraud Examiners, 2010).

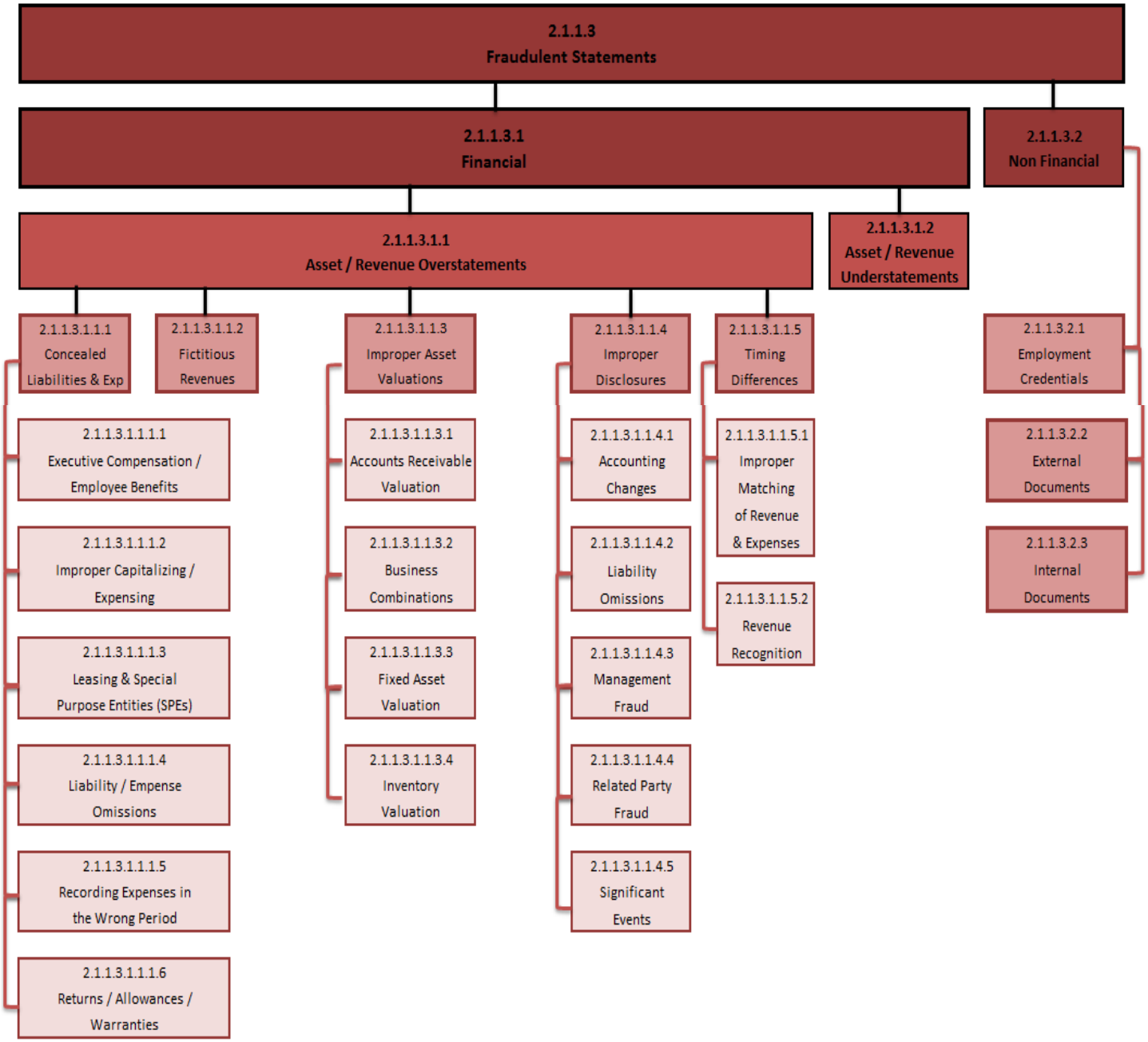
2.1.1.2.3 Economic Extortion - Economic extortion cases are the "Pay up or else…" corruption schemes; basically the flip side of bribery schemes. Instead of a vendor offering a payment to influence a decision, an employee demands that a vendor pay him in order to make a decision in that vendor's favor. If the vendor refuses to pay, he faces some harm such as loss of business with the extorter's company. In any situation where an employee might accept bribes to favor a particular company or person, the situation could be reversed to a point where the employee extorts money from a potential purchaser or supplier (Association of Certified Fraud Examiners, 2010).

Economic extortion also includes scenarios where an employee extorts another employee to force a certain action to occur that would be to the detriment of either the employee or the organization. It can also be committed by or against a client [10] to the detriment of another person or organization (Bell, 2013).

2.1.1.2.4 Illegal Gratuities - Illegal Gratuities are similar to bribery schemes except there is not necessarily an intent to influence a particular business decision before the fact. In the typical illegal gratuities scenario, a decision is made that happens to benefit a certain person or company. The party who benefited from the decision then gives a gift to the person who made the decision. The gift could be anything of value. An illegal gratuity does not require proof of an intent to influence.

At first glance, it may seem that illegal gratuities schemes are harmless as long as the business decisions in question are not influenced by the promise of payment. But most company ethics policies forbid employees from accepting unreported gifts from vendors. One reason is that illegal gratuities schemes can (and do) evolve into bribery schemes (Association of Certified Fraud Examiners, 2010).

[10] If economic extortion is committed against a client, then this would be **Individual** fraud and not Organizational fraud.



2.1.1.3 Fraudulent Statements - A statement related to a material fact and known to be untrue or made with reckless indifference as to its truth or falsity. A statement or representation may also be "false" or "fraudulent" when it constitutes a half truth, or effectively conceals a material fact.

2.1.1.3.1 Financial - Financial statement fraud is the deliberate misrepresentation of the financial condition of an enterprise accomplished through the intentional misstatement or omission of amounts or disclosures in the financial statements to deceive financial statement users. [11]

Financial statement fraud usually involves overstating assets, revenues, and profits and understating liabilities, expenses, and losses (Association of Certified Fraud Examiners, 2010).

[11] There are many different financial statement fraud schemes. While they are beyond the scope of this paper, they should be considered in more detail when evaluating fraud risk.

2.1.1.3.2 Non Financial - The falsification of documents other than financial reports.

2.1.1.3.2.1 Employment Credentials - Fake credentials fraud is closely related to counterfeit documents fraud and identity fraud. Scam artists use falsified documents to get jobs, obtain access to secure areas and apply for citizenship. Fraudsters have been known to falsify degrees from legitimate schools or they may just invent the school. They often will try to use names that closely resemble legitimate schools, but the actual degree comes from a false institution known as a diploma mill.

Other credentials also can be fraudulent. Documents that prove a membership in an association, or a professional designation can also be faked (Fake Credentials Fraud).

2.1.1.3.2.2 External Documents - Falsification of external documents may include: (Weaver, 2012)

- Publicly announced information that provides unsubstantiated favorable results.
- Falsifying external documents to suppliers and other stakeholders.

Examples include:

- *An employee providing external auditors or regulators with falsified documents.*
- *A loan officer providing a client with a counterfeit receipt.*

2.1.1.3.2.3 Internal Documents - Falsification of internal documents may include:

- Internal memorandums giving misleading information (Weaver, 2012).
- Creating a fictitious document including cash receipts [12], checks, expense reports, and time sheets (Office of Internal Audit & Ethics Liaison).
- Submitting false, incomplete or misleading information to decision makers influencing their decision in a manner in which they would not have otherwise made that decision had they been given true and accurate information (Bell, 2013).

Examples include: counterfeit documents created by a loan officer to falsely substantiate a loan disbursement.

2.1.2 External Perpetrator - Fraud committed by an external perpetrator.

2.2 Governmental Fraud

Fraud committed against government agencies, programs, regulations, and society.

2.2.1 Government Programs - Fraud exploiting government programs.

Examples include: Welfare fraud, Disability fraud, Medicare fraud, and Medicaid fraud.

2.2.2 Government Regulations - Fraud exploiting government regulations.

Examples include: immigration fraud, voting fraud, tax fraud, and stamp fraud.

[12] If this is created by an employee and the counterfeit cash receipt stays inside the company, then it is an Internal Document. However, if the cash receipt is given to an outside party such as a client, then it would be considered an External Document.

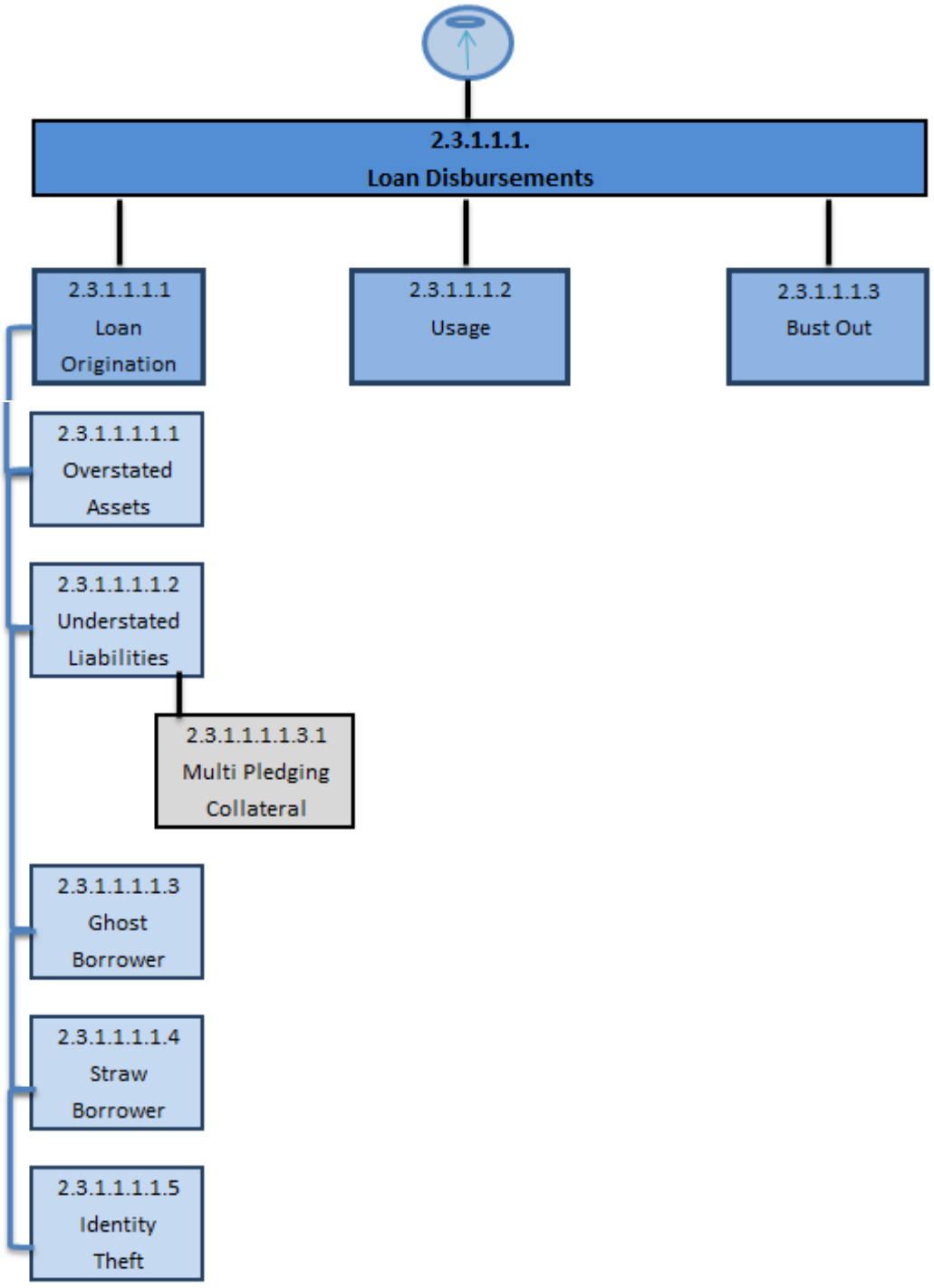
2.3 Industry Fraud

Fraud schemes found in only certain industries.

2.3.1 Financial Institution Fraud - Fraud schemes unique to financial institutions.

2.3.1.1 Lending Fraud - Fraud schemes unique to lending practices.

2.3.1.1.1 Loan Disbursements - Fraudulent loan disbursements whereby the lending process is manipulated.



2.3.1.1.1.1 Loan Origination - Misrepresentation of the financial records in order to obtain a loan for which the borrower would otherwise not be entitled to receive.

A supporting or secondary scheme for this typically involves counterfeit internal documents related to the loan origination process.

2.3.1.1.1.1.1 Overstated Assets - Overstating assets in order to obtain a loan for which the borrower would otherwise not be entitled to receive.

Examples include:

- *Falsifying income so as to make it appear inflated by supplying fictitious bank statements, earnings forms, tax return documents, using higher seasonal income to represent every month, and using one-time contract work to represent ongoing employment.*
- *Overstating the valuation of assets by recording inflated appraisals, fictitious revenues, fictitious receivables, manipulating timing differences (revenue recognition), incorrect or misleading disclosures, or by other means to inflate the cash flows from operations.*
- *The loan officer helps the client make fake title deeds in order to qualify for the loan.*

2.3.1.1.1.1.2 Understated Liabilities - Concealing debt obligations to artificially lower the debt-to-equity ratio to manipulate the loan award decision and receive a loan the borrower would otherwise not be entitled to receive.

Examples include:

- *Concealing liabilities and expenses.*
- *The loan officer disburses multiple loans [13] to the same business (client).*

  2.3.1.1.1.1.2.1 Multi Pledging Collateral - The loan collateral has already previously been pledged to another financial institution or creditor and not disclosed by the borrower and/or filed with the appropriate authorities.

  This is sometimes referred to as "shot gunning" or "silent second mortgages".

2.3.1.1.1.1.3 Ghost Borrower - Loan proceeds are received by someone who creates a fictitious borrower who does not exist, i.e. a fake identity.

Examples include:

- *Loan proceeds received by an employee instead of the borrower where a fictitious borrower is created who does not exist.*
- *Loan proceeds are shared by multiple employees instead of the borrower where a fictitious borrower is created who does not exist.*
- *A borrower creates a fictitious identity in order to receive a loan.*

This is sometimes referred to as "ghost client" or "ghost loan".

[13] If the same collateral was listed for all of the loans, then the fraud scheme is Multi Pledging Collateral.

2.3.1.1.1.1.4 Straw Borrower - Loans transferred to third-parties.

This scheme is typically also associated with usage fraud as it potentially violates contract law under the stated purpose provision.

Examples include:

- *A borrower who is no longer eligible to receive a loan entices a friend or family member with a good credit standing to apply for a loan and the proceeds are transferred to the original ineligible borrower.*
- *Loan proceeds that are shared between the client and another person [14] such as the guarantor.*
- *In group loans, the loans transferred by the borrower to another member within the same group.*

This is sometimes referred to as "on-lending".

2.3.1.1.1.1.5 Identity Theft - An individual's identity is stolen without their knowledge or consent in order for the fraudster to receive a loan.

Examples include:

- *All loan proceeds [15] received by an employee instead of the borrower where an actual borrower's identity is used to obtain additional loans, e.g. cycle 2+.*
- *A borrower impersonates (assumes the identity) a bonafide [16] individual without their knowledge or consent in order to receive a loan.*

2.3.1.1.1.2 Usage - Loan proceeds are used for other than the stated purpose.

This is a violation of contract law unless the contract expressly stipulates the funds can be used for any purpose.

Examples include:

- *The borrower takes out a loan for the purpose of utilizing it for their business and the borrower uses the funds instead to pay for personal expenses such as for a child's wedding or a television for the home.*
- *The client is issued another loan that still has a balance due and the disbursement from the second loan is used to pay off the balance of the first loan. This is sometimes referred to as "early closure".*
- *Money laundering where illegally obtained money has the appearance of having a legitimate origin.*

2.3.1.1.1.3 Bust Out - A bust out scheme occurs when there was never an intention by the borrower to make the underlying loan payments. The borrower disappears from the address registered with the financial institution primarily for the purposes of defaulting on the loan and/or to avoid prosecution and typically occurs before the first installment is due.

This is sometimes referred to as "Client Escape".

[14] Loans shared between the client and an employee constitute an Other Bribery Scheme under Corruption.
[15] If only partial proceeds are given to the employee, then it would be considered a primary identity theft scheme for the borrower and a supporting kickback (corruption) scheme for the amount given to the employee.
[16] Authentic or real person as opposed to a fictitious (fake) or made-up identity.

Attributes

The following attributes can be utilized for reporting more detailed information about fraud events which can further enhance the analysis capabilities. [17]

Incident Tags

Method of Advertising the Fraud: How was the fraud advertised or promoted to victims? Where did the victim first learn about it?

Ad:IE - Internet, email
Ad:TX - Text, direct message
Ad:DM - Direct mail
Ad:TVR - TV or radio
Ad:T - Telemarketing
Ad:P - In person

Purchase Setting: In what setting was the fraudulent purchase made?

PS:I - Computer via Internet
PS:M - Mail
PS:T - Telephone
PS:S - Store (brick and mortar) *NOTE: In MFI this would be the branch.*
PS:P - Person to person

Method of Money Transfer: How did the money move from the possession of the victim to the possession of the perpetrator?

MT:CC - Credit card
MT:DC - Debit/ATM card
MT:C - Cash
MT:PC - Personal check
MT:M - Mobile/online payment application (e.g., Apple Pay, Square, Venmo, Google Wallet)
MT:MO - Money order
MT:W - Wire funds (e.g., Western Union, Money Gram, or bank)
MT:T - Telephone account
MT:PP - Prepaid card (e.g., Green Dot, Vanilla card, Bluebird, Walmart MoneyCard)
MT:B – Bitcoin

Dollar loss categories: Dollar loss categories indicate how much money the victim lost in the fraudulent transaction (if known).

Consideration should be given to tracking exposure, fraud amount and loss amount for each fraud event. For more information, see "Reporting Fraud Calculations" at http://fraud-doctor.com/2013/02/25/reporting-fraud-calculations/

[17] Unless otherwise noted, each of the attributes were from the *Framework for a Taxonomy for Fraud* (Stanford, 2015, pp.35-37) verbatim.

Duration of incident: If the victim lost money over a period of time involving a series of transactions, duration categories indicate how long the fraudulent incident lasted. *Consideration should be given to a meaningful grouping of time (days, months) that if captured (tracked) would provide insight into the fraud events.*

Victim Tags

MV - Male Victim: The victim of the fraud was male.
FV - Female Victim: The victim of the fraud was female.
EV - Elder Victim: The victim of the fraud was age 65 or over. This tag identifies a type of fraud with particular policy relevance.
VV - Veteran Victim: The victim of the fraud was a veteran. This tag identifies a type of fraud with high policy relevance.
CIV - Cognitively Impaired Victim: The victim of the fraud was cognitively impaired. This tag identifies a type of fraud with high policy relevance.
RV - Repeat Victim: The individual has been victimized in the past by the same or a different type of fraud.
RA - The victim reported the fraud to authorities.

Perpetrator Tags

MP - Male Perpetrator: The perpetrator of the fraud was male.
FP - Female Perpetrator: The perpetrator of the fraud was female.
IP - Intimate Partner Perpetrator: The perpetrator of the fraud was an intimate partner of the victim, including boyfriend/girlfriend, former and current spouse.
FP - Family member Perpetrator: The perpetrator of the fraud was a family member of the victim, such as a child, parent, spouse, or other relative.
CP - Caregiver Perpetrator: The perpetrator of the fraud was the victim's caregiver.

The *Taxonomy of Fraud in Microfinance* working group suggests adding an additional grouping to the perpetrator tags that capture the position of the employee if fraud is committed by an insider. Others can be added as new positions are created within the MFIs as long as the designation code is unique.

PLO – Loan Officer: The position of the perpetrator of the fraud was loan officer.
PCS – Credit Supervisor: The position of the perpetrator of the fraud was credit supervisor.
PBM – Branch Manager: The position of the perpetrator of the fraud was branch manager.
PRM – Regional Manager: The position of the perpetrator of the fraud was regional manager.

PA – **Auditor**: The position of the perpetrator of the fraud was audit officer.
PAM – **Audit Manager**: The position of the perpetrator of the fraud was audit manager.
PR – **Risk Officer**: The position of the perpetrator of the fraud was risk officer.
PMR – **Manager of Risk**: The position of the perpetrator of the fraud was manager of risk.
PIC – **Internal Controls**: The position of the perpetrator of the fraud was internal controls.
PICM – **Internal Controls Manager**: The position of the perpetrator of the fraud was internal controls manager.
PS – **Security**: The position of the perpetrator of the fraud was security officer.
PSM – **Security Manager**: The position of the perpetrator of the fraud was security manager.

PHR – **Human Resources**: The position of the perpetrator of the fraud was HR officer.
PHRM – **Human Resources Manager**: The position of the perpetrator of the fraud was HR manager
PAm – **Administration**: The position of the perpetrator of the fraud was administration officer.
PAmM – **Administration Manager**: The position of the perpetrator of the fraud was admin manager.
PIT – **I.T.**: The position of the perpetrator of the fraud was I.T. officer.

PITM – **I.T. Manager**: The position of the perpetrator of the fraud was I.T. manager.
PMM – **Marketing Manager**: The position of the perpetrator of the fraud was marketing manager.
PF – **Finance**: The position of the perpetrator of the fraud was finance officer.
PA – **Accountant**: The position of the perpetrator of the fraud was accountant.
PC – **Controller**: The position of the perpetrator of the fraud was controller.
PL – **Legal**: The position of the perpetrator of the fraud was attorney or legal staff.
PHL – **Head of Legal**: The position of the perpetrator of the fraud was head of legal.

PCFO – **Chief Financial Officer**: The position of the perpetrator of the fraud was CFO.
PCOO – **Chief Operations Officer**: The position of the perpetrator of the fraud was COO.
PCEO – **Chief Executive Officer**: The position of the perpetrator of the fraud was CEO.

Appendix 1 – Portfolio at Risk (PAR)

Definition

Portfolio at risk is the value of all loans outstanding that have one or more installments of principal past due more than a certain number of days. This item includes the entire unpaid principal balance, including both past-due and future installments, but not accrued interest. Portfolio at risk (PAR) is usually divided into categories according to the amount of time passed since the first missing principal installment.

PAR Ratio

PAR Ratio is the most accepted measure of portfolio quality. PAR ratio is calculated as the outstanding amount of all loans (both individual and group loans) that have one or more installments of principal past due by a certain number of days, divided by gross loan portfolio. The numerator of the PAR ratio includes the entire unpaid principal balance of the loan, including both past-due and future installments, but not accrued interest. The numerator is not limited to the delinquent portion of the loan.

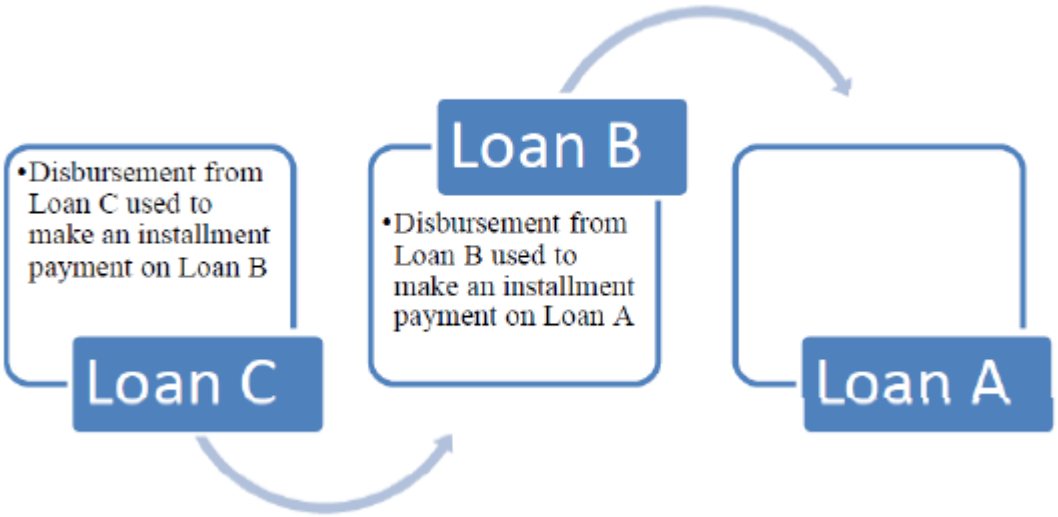
Appendix 2 –Skimming Receivables Supplement

Skimming receivables may be more difficult to conceal than skimming sales because receivables payments are expected. The victim company knows the customer owes money and is waiting for the payment. In a revenue skimming scheme where a sale goes unrecorded, it is as if the sale never existed. Receivables skimming, by contrast, may raise questions about missing payments (Wells, Corporate Fraud Handbook: Prevention and Detection, 2011).

Lapping - Lapping is the crediting of one account through the abstraction of money from another account. Suppose a company has three customers: A, B and C. When A's payment is received, the fraudster takes it instead of posting it to A's account. Customer A expects that her account will be credited with the payment she has made, but this payment actually has been stolen. When B's check arrives, the fraudster takes this money and posts it to A's account. Payments now appear to be up to date on A's account, but B's account is short. When C's payment is received, the perpetrator applies it to B's account.

Examples include:

- *The loan officer takes a portion of an installment payment (repayment) and keeps it for himself, but uses another client's repayment to make up the difference for the first client.*



This process continues indefinitely until one of three things happens: (1) someone discovers the scheme, (2) restitution is made to the accounts, or (3) some concealing entry is made to adjust the accounts receivable balances.

Because lapping schemes can become very intricate, fraudsters sometimes keep a second set of books on hand detailing the true nature of the payments received. The second set of records helps perpetrators keep track of what funds they have stolen and what accounts need to be credited to conceal the fraud (Wells, Corporate Fraud Handbook: Prevention and Detection, 2011).

Unconcelaed - This is a scheme in which an employee skims receivables without attempting to conceal it in the books and records.

Examples include:

- *The loan officer collects the installment payment (repayment) in the field and pockets (keeps) the cash.*
- *The loan officer collects a partial installment payment (repayment) in the field and pockets (keeps) the cash.*
- *The loan officer accepts the installment payment (repayment) from the client and a penalty amount, but does not enter the penalty into the system [18] and pockets (keeps) the penalty portion of the cash.*

Write-Offs - Some employees cover their skimming by posting entries to contra revenue accounts such as "discounts and allowances". If, for instance, an employee intercepts a USD $1,000 payment, he would create a USD $1,000 "discount" on the account to compensate for the missing money. Another account that might be used in this type of concealment is the bad debts expense account (Wells, Corporate Fraud Handbook: Prevention and Detection, 2011).

Examples include:

- *An employee deliberately stalls recovery for loans so that loans are written-off after a threshold, e.g. 180-days past due*

[18] If a reversing entry or waiver is entered into the system for the penalty fee, then it is a larceny scheme and not a skimming scheme.

Appendix 3 – Bid Rigging Supplement

Bid rigging schemes occur when an employee fraudulently assists a vendor in winning a contract through the competitive bidding process. The typical fraud in the need recognition phase of the contract negotiation is a conspiracy between the buyer and contractor where an employee of the buyer receives something of value and in return recognizes a "need" for a particular product or service. The result of such a scheme is that the victim organization purchases unnecessary goods or services from a supplier at the direction of the corrupt employee.

The other type of pre-solicitation fraud is a **specification scheme**. Specifications are prepared to assist vendors in the budding process, telling them what they are required to do and providing a firm basis for making and accepting bids. In some cases the vendor pays off an employee of the buyer who is involved in preparing specifications for the contract. In return, the employee tailors the specifications to accommodate that vendor's capabilities so that the contractor is effectively assured of winning the contract.

Another form of specifications fraud is **bid splitting**. Government and other entities are often required to solicit bids on projects over a certain dollar amount. In order to avoid this requirement, employees might break a large project up into several small projects that fall below the mandatory bidding level. Once the contract is split, the employee can award some or all of the component parts to a contractor with whom he is conspiring.

A less egregious but nevertheless unfair form of bid-rigging occurs when a vendor pays an employee of the buyer for the right to see the specifications earlier than his competitors.

In the solicitation phase of the competitive bidding process, fraudsters attempt to influence the selection of a contractor by restricting the pool of competitors from whom bids are sought. In other words, a corrupt vendor pays an employee of the purchasing company to ensure that one or more of the vendor's competitors do not get to bid on the contract.

Bid pooling is a process by which several bidders conspire to split up contracts and ensure that each gets a certain amount of work. Instead of submitting confidential bids, the vendors discuss what their bids will be so they can guarantee that each vendor will win a share of the purchasing company's business. Furthermore, since they plan their bids ahead of time, then vendors can conspire to raise their prices.

Another way to eliminate competition in the solicitation phase of the selection process is to solicit bids from **fictitious suppliers**. This gives the appearance of a competitive bidding situation, when in fact only one real supplier bids on the job. Furthermore, the real contractor can hike up his prices, since the other bids are fraudulent and sure to be higher than his own.

In some cases, competition for a contract can be limited by severely restricting the time for submitting bids. Certain suppliers are given advanced notice of contracts before bids are solicited. These suppliers are therefore able to begin preparing their bids ahead of time.

Bribed purchasing officials can also restrict competition for their coconspirators by soliciting bids in obscure publications where other vendors are unlikely to see them. Some schemes have also involved the publication of bid solicitations during holiday periods when those suppliers not "in the know" are unlikely to be looking for potential contracts.

In more blatant cases, the bids of outsiders are accepted but are "lost" or improperly disqualified by the corrupt employee of the purchaser. In the actual submission phase of the process, where bids are proffered to the buyer, several schemes may be used to win a contract for a particular supplier. The principal offense tends to be abuse of the sealed bid process. Competitive bids are confidential; they are, of course, supposed to remain sealed until a specific date at which all bids are opened and reviewed by the purchasing company. Other reasons to bribe employees of the purchaser include ensuring receipt of a late bid, or falsify the bid log, to extend the bid opening date, and to control bid openings (Association of Certified Fraud Examiners, 2010).

References

Albrecht, W. S., Albrecht, C. C., & Kimbleman, M. F. (2008). *Fraud Examination.* Stamford, CT, United States: South-Western College Pub.

Asset Recovery Associates LLC. (2012). *Fraud Schemes.* Retrieved from http://www.assetrecoverystl.com/wp-content/uploads/2012/07/Fraud-Schemes.pdf

Association of Certified Fraud Examiners. (2008). *The Corporate Con: Internal Fraud and The Auditor.* Austin, Texas, United States. Retrieved from http://www.acfe.com/uploadedFiles /Shared_Content/Products/Self-Study_CPE/corporate-con-2008-excerpt.pdf

Association of Certified Fraud Examiners. (2010). *International Fraud Examiners Manual*. Austin, Texas, United States.

Association of Certified Fraud Examiners. (2011). *Introduction to Fraud Examination.* Austin, Texas, United States. Retrieved from ttp://www.acfe.com/uploadedFiles/Shared_Content/Products /Self-Study_CPE/intro-to-fraud-exam-2011-extract.pdf

Association of Certified Fraud Examiners. (2012). *Other People's Money: The Basics of Asset Misappropriation.* Austin, Texas, United States.

Association of Certified Fraud Examiners. (2012). *Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study*. Austin, Texas, United States.

Bhatnagar, S. (n.d.). *Building Trust through E-Government: Leadership and Managerial Issues.* United Nations Public Administration Network. Retrieved 12 August 2013, from http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan025871.pdf

Bell, A. (2009/2013). *Occupational Fraud Schemes {Microfinance}* [Chart]. Fraud Doctor. Charlotte, North Carolina, United States. Retrieved from http://www.fraud-doctor.com

Bell, A. (2010). *Mortgage Fraud and the Illegal Property Flipping Scheme: A Case Study of United States v. Quintero-Lopez*. Charlotte, North Carolina, United States: CreateSpace.

Crawford, P. J., & Fredericks, E. H. (2010). *Special Purpose Entities.* Graziadio Business Review. Retrieved from http://gbr.pepperdine.edu/2010/08/special-purpose-entities/

Denis, D. J., Hanouna, P., & Sarin, A. (2005). *Is there a dark side to incentive compensation?*

Fake Credentials Fraud. (n.d.). Fraud Squad TV. Retrieved August 23rd, 2013, from http://www.fraudsquadtv.com/docs/Fake_Credentials_Fraud.php

Fraud. (2004). In Bryan A. Garner (Ed.), *Black's Law Dictionary* (8th ed.). Eagan, Minnesota, United States: West Group.

Gao, L., & Srivastava, R. P. (2011). The Anatomy of Management Fraud Schemes: Analyses and Implications. *Indian Accounting Review*, 1-23.

Greene, C. L. (n.d.). *Employee Frauds: Payroll*. Mc Govern & Greene LLP. Retrieved from http://www.mcgoverngreene.com/archives/archive_articles/Craig_Greene_Archives /Focus-Employee_Frauds-Payroll.html

Joshi, M. S. (2005). *Occupational Frauds and Money Laundering.* Mumbai, India: Snow White Publications.

Kapka, K. W. (n.d.). *Conflicts of Interest.* University of Texas at Tyler. Retrieved 12 August 2013, from http://www2.uttyler.edu/ohr/ConflictsofInterest2009METraining.pptx

Ketling, W. (n.d.). *Occupational Fraud: Asset Misappropriation, Skimming and Cash Larceny.* Retrieved from http://www.sbmonthly.com/?p=2518

Kovacich, G. L. (2007). *Fighting Fraud: How to Establish and Manage an Anti-Fraud Program.* Oxford, United Kingdom: Butterworth Heinemann.

Kranacher, M. J., Albrecht, S., & Albrecht, C. (2008). *Asset Misappropriation Research White Paper for The Institute for Fraud Prevention.*

Kranacher, M. J., Riley, R., & Wells, J. T. (2010). *Forensic Accounting and Fraud Examination.* Hoboken, NJ, United States: John Wiley & Sons.

Kroll. (2008/2009). *Global Fraud Report*. Economic Intelligence Unit. New York, New York, United States: Marsh & McLennan Companies, Inc (NYSE: MMC).

Lectric Law Library, The. (n.d.). Retrieved May 2013, from http://www.lectlaw.com/def/f016.htm

Office of Internal Audit & Ethics Liaison. (n.d.). Northwestern State University of Louisiana. Retrieved May 2013, from http://internalaudit.nsula.edu/fraud-awareness/

Rittenberg, E. L., Johnstone, K. M., & Gramling, A. A. (2009). *Auditing: A Business Risk Approach.* Stamford, CT, United States: Cengage Learning.

Rittenberg, E. L., Mohnstone, K., & Gramling, A. A. (2009). *Auditing: A Business Risk Approach.* Stamford, CT, United States: South-Western College Pub.

Singleton, T. W., & Singleton, A. J. (2010). *Fraud Auditing and Forensic Accounting.* Hoboken, New Jersey, United States: John Wiley & Sons.

Stanford Center on Longevity. (2015). *Framework for a Taxonomy of Fraud.* Stanford, California: Stanford University, Financial Fraud Research Center of the Stanford Center on Longevity. Retrieved 22 July 2015, from: http://longevity3.stanford.edu /framework-for-a-taxonomy-of-fraud/

Thornton, G. (n.d.). *The Forensic and Investigative Services Practice.* London, United Kingdom.

Transparency International. (2013). *Global Corruption Barometer 2013*. Berlin, Germany. Retrieved from http://www.transparency.org/whatwedo/pub/global_corruption_barometer_2013

Weaver. (2012). *Fraud Prevention: Recognizing the prevalence of Fraud and the importance of Prevention*, (p. 65).

Wells, J. T. (2007). *Corporate Fraud Handbook: Prevention and Detection.* Hoboken, New Jersey, United States: John Wiley & Sons.

Wells, J. T. (2010). *Principles of Fraud Examination.* Hoboken, New Jersey, United States: Wiley.

Wells, J. T. (2011). *Corporate Fraud Handbook: Prevention and Detection.* Hoboken, NJ, United States: John Wiley & Sons.

What is Fraud? (n.d.). Association of Certified Fraud Examiners. Austin, Texas, United States. Retrieved from http://www.acfe.com/fraud-101.aspx