The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management.

Wesley Kenneth Wilhelm
Manager, Strategic Planning
Fair Isaac Company

Abstract

Fraud losses impact every business. Caveat Emptor, let the buyer beware, tells half the story; Caveat Venditor, let the seller beware, tells the rest. Fraud costs are passed on to society through increased customer inconvenience, opportunity costs, unnecessarily high prices, and criminal activities funded by the fraudulent gains. In short, fraud is rampant. This study developed a theoretical framework for the Fraud Management Lifecycle, examined numerous significant lifecycle stage interactions, and evaluated the lifecycle in five industries with significant economic crime.

The Fraud Management Lifecycle is dynamic, evolving, and adaptive. The eight stages are: Deterrence, Prevention, Detection, Mitigation, Analysis, Policy, Investigation, and Prosecution. Effective fraud management requires a balance in the competing and complementary actions within the Fraud Management Lifecycle.

Introduction

Fraud losses continue to impact virtually every business enterprise. Caveat Emptor, let the buyer beware, tells only half the story. The other half is told by Caveat Venditor, let the seller beware. The costs of fraud are passed on to society in the form of increased customer inconvenience, opportunity costs, unnecessarily high prices for goods and services, and criminal activities funded by the fraudulent gains. But what if there existed a Fraud Management Lifecycle that when managed effectively, with successfully balanced components, would significantly reduce the losses and societal costs associated with fraud? This study developed a theoretical framework for the Fraud Management Lifecycle and tested it with empirical research.

Despite significant advances in fraud detection technologies, fraud losses continue to pose a significant problem to many industries, including telecommunications, banking and finance, insurance, health care, Internet merchants, brokerage and securities, and many others. The statistics that follow are but a few examples of the magnitude of the problem.

Insurance:

"In the United States, about $67 billion is lost every year to fraudulent claim." (Federal Bureau of Investigation [FBI], 2003).

Telecommunications:

"The $1.5 trillion phone industry loses approximately 10% to fraud, that is $150 billion at current estimates" (Mena, 2003).

Bank Fraud:

"For the period of April 1, 1996 through September 30, 2002, the FBI received 207,051 Suspicious Activity Reports (SARs) for criminal activity related to check fraud, check kiting, counterfeit checks, and counterfeit negotiable instruments. These fraudulent activities accounted for 47 percent of the 436,655 SARs filed by U.S. financial institutions (excluding Bank Secrecy Act violations), and equaled approximately $7 billion in losses" (U.S. Department of Justice [DOJ], 2002). Though illustrative, it must be noted that the SAR data amounts reported are total exposure and not net losses. They are, however, indicative of the continuing problem due to historically low loss recovery and restitution rates.

Money Laundering:

"United States Treasury officials estimate that as much as $300 billion is laundered annually, worldwide, with from $40 billion to $80 billion of this originating from drug profits made in the United States" (Mena, 2003).

Internet:

"According to Meridien Research, without any technological investments in fraud detection and prevention, worldwide credit card fraud [the Internet component] will represent $15.5 billion in losses [annually] by 2005. However, if merchants adopt data mining technology now to help screen credit-card orders prior to processing, the widespread use of this technology is predicted to cut overall losses by two thirds to $5.7 billion in 2005" (Mena, 2003).

Credit Card:

The numbers from the Nilson report indicate that issuer credit card fraud losses run approximately 1 billion dollars annually. This list does not even include debit card fraud, brokerage fraud, fraud at casinos, health care fraud, and other miscellaneous fraud types such as bankruptcy fraud where it is estimated that "…in 1995 alone, almost 250 fraudulent bankruptcies were filed every day" (FBI, 2003). Just these limited components aggregate to approximately 265 billion dollars annually flowing to fund other more damaging illegal activities. As

Senator Everett Dirksen so aptly said, “A billion here a trillion there; the first thing you know, you’re talking about real money.”

Industry	Annual Losses	Running Total
Insurance Fraud	67 billion	67 billion
Telecommunications Fraud	150 billion	217 billion
Bank Fraud	1.2 billion	218.2 billion
Money Laundering	40 billion	258.2 billion
Internet fraud	5.7 billion	263.9 billion
Credit Card Fraud	1 billion	264.9 billion
Grand Total	**264.9 billion**	264.9 billion

Figure 1. Cross Industry Fraud Losses and Money Laundering estimates.

Fraud losses are frequently part of an economic externality. An economic externality is present when one business takes actions or refrains from acting and, as a result, passes on, imposes, or facilitates costs upon another business. An example from the internal fraud perspective would be when a financial institution decides not to facilitate law enforcement’s arrest and prosecution of a staff member who stole from them. As a result of their decisions, the ex-staff member may very well obtain employment at another financial institution and commit the same crime again. This situation is quite aptly described by the following “While fraud does exist in retail originations, it is typically related to a particular loan officer and is more often than not quickly discovered. The employee is usually terminated from his [or her] position and moves on to a new company until the same thing happens all over” (Prieston and Dreyer, 2001). Generally, since the costs of the decision are external to their business and are not illegal, it is accepted in the business community that there is limited reason to be concerned with the spillover or externality impacts of their fraud prevention actions or inaction upon other entities and society.

An example may prove illustrative. In a case on which the author worked, a telecommunications company with excessive credit card fraud losses was faced with several types of fraud. One was that some employees, frequently, but not exclusively call center staff, were taking customer demographic and payment information and using it to purchase goods and services from other card-not-present merchants. There was reason to suspect that some of them may have been initiating the first steps of identity theft and identity fraud to obtain payment cards and checks in the customer’s name. The telecommunications company was faced with an all too common decision regarding an economic externality. Although the company found cause to terminate the employee in question for exploiting his access to privileged customer information, it declined to invest in a system to proactively detect and prevent this type of behavior. The fraud being perpetrated by its employees and contract employees did not result in losses to the telecommunications company. The losses and other negative impacts of the

fraud were borne by other participants in the payment system, by their customers, and by society as a whole. Although the decision process was difficult, it was decided to focus only on and fix the fraudulent practices that were resulting in direct losses to the telecommunications company. The author would submit that it is reasonable to argue that by not acting, the company made a decision to continue facilitating that type of fraud.

It is precisely this type of externality in the banking arena that was addressed by the Department of the Treasury and the Federal Reserve when they published their "Interagency Guidelines Establishing Standards for Safeguarding Customer Information." The guidelines were created and distributed in order to comply with a requirement in § 501(b) of the Gramm-Leach-Bliley Act. In the Act "Congress directed the Agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer" (U.S. Department of the Treasury, Office of the Comptroller of the Currency et. al. [DOT], 2003). "Among other things, the Security Guidelines direct financial institutions to: (1) identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and (3) assess the sufficiency of policies and procedures, customer information systems, and other arrangements in place to control risks" (DOT, 2003).

Notably and regrettably absent from the interagency guidelines are any requirements to proactively monitor and profile employee activity with predictive statistical models in order to ensure the early detection and fast correction of these types of cases. Also absent from the guidelines is a secondary and delayed form of this kind of monitoring known as footprint review. Footprint reviews compare accounts with confirmed fraud cases against those employees who viewed or maintained the account information prior to the onset of the fraudulent activity. The guidelines correctly address deterrence and prevention stages of the Fraud Management Lifecycle, but they clearly fall short of adequately addressing detection and mitigation activities. Previous employee dishonesty in the financial industry surely constitutes a reasonable anticipation of future employee dishonesty. In other words, financial institutions should be able to foresee that cases of employee dishonesty will occur.

Another example of economic externality involves an Internet travel agent with whom this author had the pleasure of working in October 2001. It seemed that their web site was being used fraudulently to book air travel. Their chief legal officer indicated that it was not their place to fix society's problems; they just

needed to reduce their losses to a tolerable "cost of doing business." This same company utilized a processing system that displayed their customers' travel and payment information in such a way that employees could access it and use it to facilitate illegal activity. However, since the losses resulting from this activity were external to the travel company, the processing company, and the call center company, it was deemed "not worth our investment" to remedy the situation.

In fact, many companies subscribe to the philosophy of fraud prevention as a "competitive advantage" where they gauge part of their success by how much fraud they can push off on their competitors. This can be described as a "not in my backyard" approach. These companies typically are unwilling to discuss or share their fraud management methods with their competitors. The ability to quickly analyze fraud losses and implement prevention and detection policies increases the difficulty for the fraudsters, as they must defeat the new strategies put in place. Fast action can make fraudsters go elsewhere. This forced migration is a core component for those companies which treat fraud management as a competitive advantage. Their focus is one of implementing strategies before their competitors, so the fraudsters will go to their competitors to commit the fraud.

This approach to fraud management frequently results in isolation and a failure to maintain the required speed of adaptation. It is, however, still present in a significant number of industries. As the Internet began to emerge as a commercial delivery channel in the late 1990's, many Internet based merchants, thinking that they were unique, relied upon their own "proprietary heuristics." These companies would not consider working with their peers or fraud management professionals from other industries because they were "unique." This philosophy is by no means limited to the merchant and issuer segments of the credit card industry. It is present to a certain extent in telecommunications, bankcard, insurance, and other industries as well, and contributes to an overall increase in losses and missed opportunities.

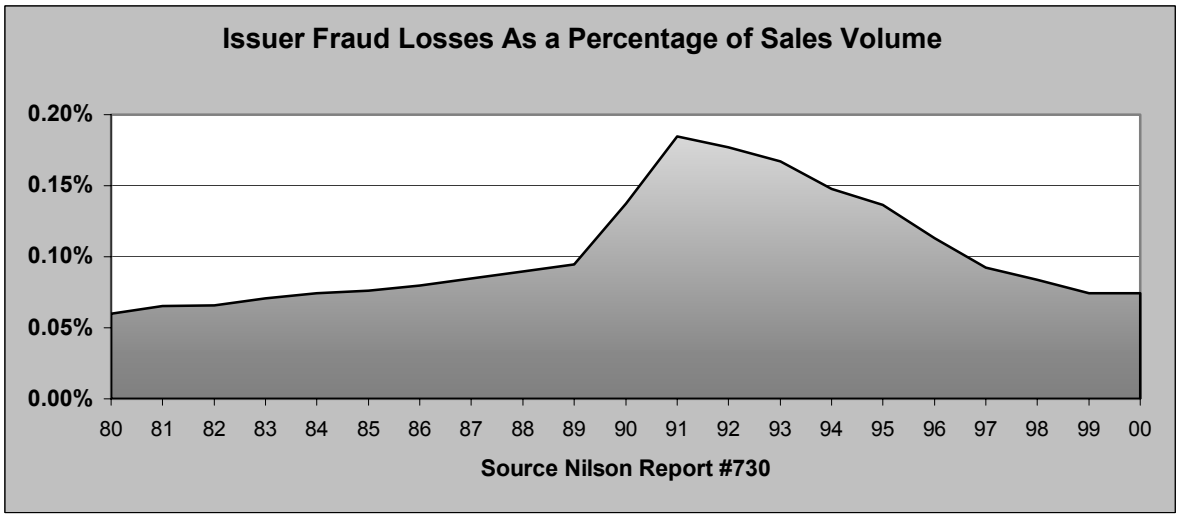

Figure 2. The Nilson Report #730. Credit Card Fraud Losses as a percentage of Sales Volume 1980 through 2000.

MasterCard and Visa, the major card associations which usually track and report fraud losses as a percentage of sales volume or loan amounts outstanding, have frequently responded to fraud inquiries with the approach that losses are under control and are running a few pennies of every hundred dollars processed through the system. Currently the numbers are around eight cents per hundred or eight basis points. The graphs in Figures 2 and 3 represent the value of fraud, as a percentage of sales volume and loan outstandings respectively, over the twenty year time period from 1980 to 2000.

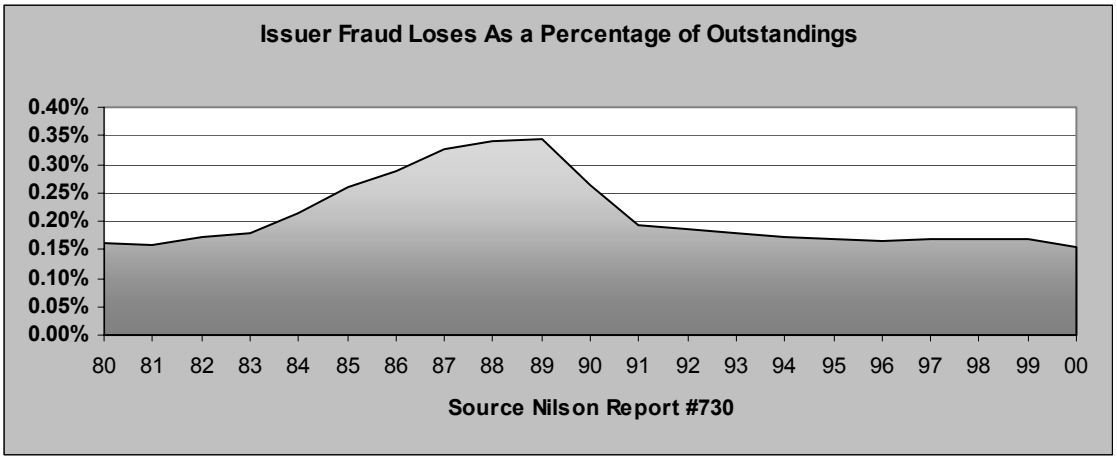

Figure 3. The Nilson Report #730. Credit Card Fraud Losses as a percentage of Outstandings 1980 through 2000.

The graphs for fraud losses to sales and fraud losses to outstandings both show a spike in fraud losses and then a leveling out to a historical equilibrium. This equilibrium, it can be argued, is the level at which the associations are

comfortable with the "fraud prevention business case" and the resulting externality spillover. However, the real dollars lost during the same time period show quite a different picture of the losses and the external impact. It is also important to take into consideration that these are issuer losses and that the merchant losses due to charge backs or acquirer losses are not represented. Similarly, these numbers do not include the fraud losses experienced by American Express, Discover, retailer-issued private label, and JCB cards, because they are not reported.

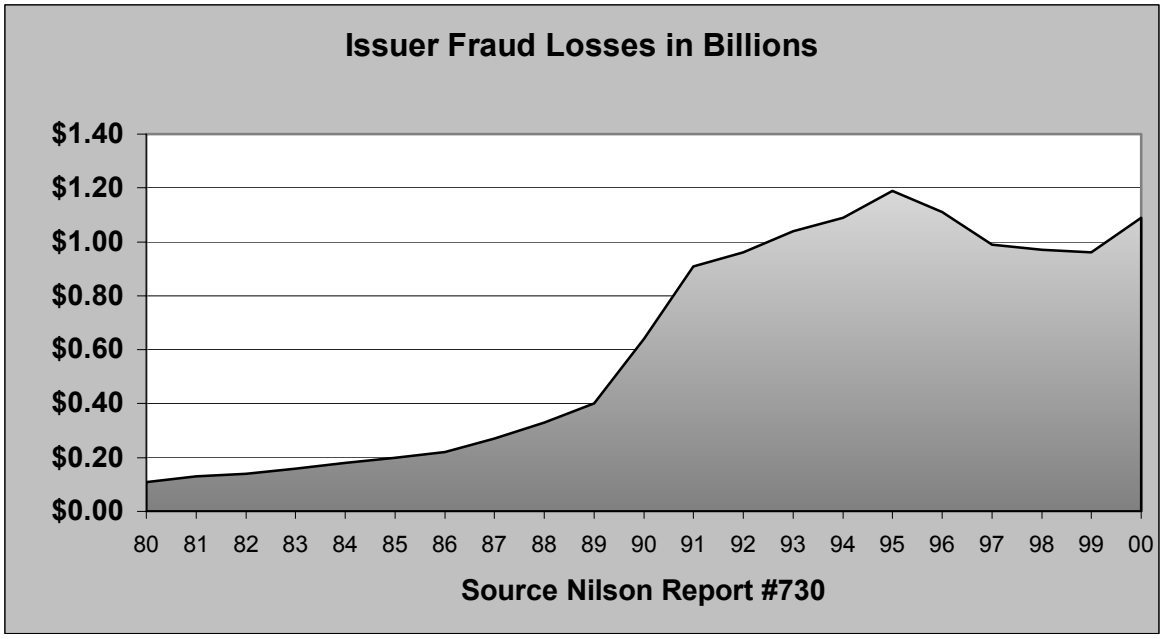

Figure 4. The Nilson Report #730. Credit Card Fraud Losses 1980 through 2000.

Figure 4 shows fraud losses were stable through much of the 1980's. Increased counterfeiting and significant growth in the number of cards in use resulted in dramatic increases late in the decade. The trend continued upward until 1995 when counterfeit reduction measures and statistical-based pattern recognition detection programs improved fraud detection. Fraud losses began to trend upward again in 2000 as a result of a rise in Internet card-not-present fraud and identity fraud. Generally, the fraud trend for the last twenty years is upward. As Figure 4 indicates, credit card losses, in real dollars, remain at or near their all time highs as an absolute number even though they are half of what they were as a relative number.

When these losses are viewed with an awareness of the numerous "successful" security enhancements and advances in fraud detection over the same time period, especially the highly effective neural network pattern recognition software solutions, one is left in a quandary. If the technological advances in credit card fraud detection are so significant, why then are losses not significantly reduced?

The hypothesis of this study is that fraud detection is but a single component in a comprehensive Fraud Management Lifecycle that includes fraud deterrence, fraud prevention, fraud detection, fraud mitigation, fraud analysis, fraud policy, fraud investigation, and fraud prosecution. When these stages are not successfully integrated and balanced, the benefits of advancements in fraud detection technologies are muted.

Previous research regarding fraud generally, and credit card fraud in particular, has focused upon the crimes, the criminals, or both. For example, Mativat and Tremblay (1997) studied credit card counterfeiting and offenders along with displacement, as opposed to the methods, procedures, and policies employed by the victims to prevent the fraud. It is this author's premise that no comprehensive analysis has been performed of the entire Fraud Management Lifecycle and the appropriate relationships among each of the various stages and the activities therein.

Should this premise prove correct, it would provide a starting point in explaining the magnitude of fraud losses in the credit card industry as well as fraud losses in other industries. When fraud management professionals fail to balance the various stages of the Fraud Management Lifecycle successfully, and do not integrate new technologies into each of the Lifecycle's stages, they expose the companies they represent to unnecessary fraud losses and/or excessive expenses, and create a negative externality effect on society. An excessive focus on investigation and prosecution appears to yield a deficiency in detection and analysis. An exclusive focus on detection appears to result in inferior deterrence. A lack of thorough analysis appears to create ineffective policy. It is these and other statements of lifecycle interrelationships which were tested and evaluated in the study phase of this project. The underlying premise is that ignorance of the lifecycle and, consequently, the need to balance and integrate the activities and technological innovations available to each stage, results in ineffective and inefficient fraud management.

The costs of credit card fraud are alarming: in excess of one billion dollars in credit card fraud in 2000 alone, and over ten billion dollars in the 1990's. The costs of fraud across the insurance, telecommunications, banking, Internet, and credit card industries are staggering. Awareness of, and the successful management of, the Fraud Management Lifecycle provides the promise of significantly reduced fraud losses and reduced societal impact.

The Fraud Management Lifecycle

Effective management of the Fraud Management Lifecycle starts with a common understanding or definition of the stages in the lifecycle. Without this awareness and understanding, fraud management professionals are unlikely to communicate effectively with each other, with their peers in other industries, and within their respective businesses. The terms "lifecycle stage" and "stage"

throughout this document are used as a reference to a set of activities. The use of the term stage does, however, bring with it references to a series of sequential independent actions that is not representative of the concepts being advanced by this document. Webster's dictionary refers to a lifecycle as "a series of stages in form and functional activity through which an organism passes between successive recurrences of a specified primary stage" (1997, 1976, &1941) . Webster's also refers to a network as "an interconnected or interrelated chain, group or system" (1997, 1976, & 1941). The Fraud Management Lifecycle can be best described as a combination of these two definitions, a network lifecycle. Unlike a traditional linear lifecycle, a network lifecycle's stages are not necessarily linked sequentially, where activities in one stage are completed and then the functioning is passed on to the next stage in the chain. To the contrary, a network lifecycle facilitates simultaneous and sequential actions within each of the lifecycle stages or network nodes. The convenient term "stage" in a network lifecycle is more specifically a reference to the activities, operations, and functions performed. One can reasonably think of the various lifecycle stages as various disciplines within fraud management. The linking of the lifecycle stages as network nodes allows the representation of non-linear, non-sequential, even recursive activity. The interrelationships and interdependence of the stages or nodes can be explained without the restriction of the traditional sequential lifecycle stage progression. The Fraud Management Lifecycle is, therefore, a network lifecycle where each node in the network, each stage in the lifecycle, is an aggregated entity that is made up of interrelated, interdependent, and independent actions, functions, and operations. These activities can, but do not necessarily, occur in a sequential or linear flow.

The Fraud Management Lifecycle is made up of eight stages. Deterrence, the first stage, is characterized by actions and activities intended to stop or prevent fraud before it is attempted; that is, to turn aside or discourage even the attempt at fraud through, for example, card activation programs. The second stage of the Fraud Management Lifecycle, prevention, involves actions and activities to prevent fraud from occurring. In detection, the third stage, actions and activities, such as statistical monitoring programs are used to identify and locate fraud prior to, during, and subsequent to the completion of the fraudulent activity. The intent of detection is to uncover or reveal the presence of fraud or a fraud attempt. The goal of mitigation, stage four, is to stop losses from occurring or continuing to occur and/or to hinder a fraudster from continuing or completing the fraudulent activity, by blocking an account, for example. In the next stage, analysis, losses that occurred despite deterrence, detection, and prevention activities are identified and studied to determine the factors of the loss situation, using methods such as root cause analysis. The sixth stage of the Fraud Management Lifecycle, policy, is characterized by activities to create, evaluate, communicate, and assist in the deployment of policies to reduce the incidence of fraud. Balancing prudent fraud reduction policies with resource constraints and effective management of legitimate customer activity is also part of this stage. An example is the requirement that any cash transaction over $10,000 be reported.

Investigation, the seventh stage, involves obtaining enough evidence and information to stop fraudulent activity, recover assets or obtain restitution, and to provide evidence and support for the successful prosecution and conviction of the fraudster(s). Covert electronic surveillance is a method used in this stage. The final stage, prosecution, is the culmination of all the successes and failures in the Fraud Management Lifecycle. There are failures because the fraud was successful and successes because the fraud was detected, a suspect was identified, apprehended, and charges filed. The prosecution stage includes asset recovery, criminal restitution, and conviction with its attendant deterrent value.

Stage One: Deterrence

Successful deterrence is the stopping of fraud before it happens. Deterrence or "to deter," is defined as, "to inhibit or discourage through fear; hence to prevent from action by fear of consequences" (Webster, 1997, 1976, & 1941). In the fraud arena we need to expand this definition to include the aspect of difficulty. Fraudsters tend to migrate toward the path of most anonymity and least resistance. Therefore, increasing the difficulty of committing the fraud effectively functions as an incremental increase in deterrence. For example, when conducting an online transaction, requiring address verification provides an incremental increase in deterrent value, because the perpetrator must know how to circumvent and defeat the verification process. Adding a component to the online transaction becomes a deterrent, as it makes the fraudster work harder. For the purposes of this study deterrence will be defined as: activities designed, through fear of consequences or difficulty of perpetration, to turn aside, discourage, or prevent fraudulent activity from being attempted. The aggregate nature of deterrence is implied; deterrence is not viewed as a monolithic whole, but rather an aggregation of activities with varying degrees of deterrent value. Deterrent value is a summation of the deterrent contributions and detractions provided by each stage in the Fraud Management Lifecycle. Thus, successful deterrence is contingent upon the performance of the other stages of the Fraud Management Lifecycle.

Stage Two: Prevention

In the fraud arena, prevention, detection, and deterrence are sometimes used synonymously. This contributes to confusion within the organization, as well as in external entities, about the focus of prevention activities. The activities in the prevention stage, though closely associated with deterrence and detection, occur after deterrence has failed and before the suspicion or detection of fraud has been accomplished.

Prevention is defined as, "to prevent, to stop or keep from doing or happening, to hinder a person from acting" (Webster, 1997, 1976, & 1941). Prevent is a general term meaning hindering, checking, or stopping. In the fraud arena the use of the term prevention emphasizes both common forms of the definition, to keep from doing and to hinder the fraudster from performing fraudulent activity. For the purposes of this study the definition of prevention is to hinder, check, or

stop a fraudster from performing or perpetrating a fraudulent activity.

Prevention stage activities are intended to prevent the fraud from occurring or to secure the enterprise and its processes against fraud. The ability of prevention to stop losses from occurring versus stopping fraudulent activity from continuing is an important distinction. The latter activities are more appropriately mitigation stage activities. Prevention, when perceived from a security perspective, can be thought of as hardening the target. Prevention actions are frequently similar to security activities in the information technology area. Deploying protective procedures, processes, systems, and verifications, etc. that make fraud harder to commit prevents fraud. Prevention activities are designed to make fraud more difficult to commit. For example, the purpose of the many security features on credit and debit cards is to make card based fraud more difficult. Telecommunications subscription fraud is made more difficult by interactive verification and authentication procedures. Know your customer (KYC) processes for opening accounts in the financial industry make it more difficult for fraudsters to open fraudulent accounts. Querying historical fraud claim files in the insurance hinders fraudsters.

Stage Three: Detection

The third stage of the Fraud Management Lifecycle, detection, is characterized by actions and activities intended to identify and locate fraud prior to, during, and subsequent to the completion of the fraudulent activity. While “prior to” may sound like deterrence, it refers to the detection of testing or probing activity used by criminals to facilitate a fraud attempt. “To detect, is to uncover or reveal, to discover the existence or presence of the fact of something hidden or obscure” (Webster, 1997, 1976, & 1941). Detection encompasses three closely related activities in the fraud arena: fraud testing, fraud attempts, and fraud successes. The separation is derived from the facts that not all fraud attempts are successful and that not all perceived fraud attempts are intended to be successful. These “tests” are attempts to reverse engineer the current fraud policies and detection activities in order to locate vulnerability. Thus, detection in the fraud arena must include revealing the existence of fraud testing and fraud attempts, as well as successful frauds. The identification of testing, attempts, and successes are typically clustered in the detection, prevention, and mitigation stages, but are also relevant in each of the other stages of the Fraud Management Lifecycle. Detection includes identification of a testing component, an attempt component, and a success component. Only detection in all three of these areas provides the required support for the rest of the stages in the lifecycle. To miss any of these is to run the risk of creating a vulnerability that the fraudster will turn to his advantage.

Stage Four: Mitigation

Mitigation is begun once the presence or a reasonable suspicion of fraudulent activity has been detected. In short, mitigation stops fraud. Other common and relevant terms for the activities in this stage are interdiction and intervention.

Sometimes mitigation activities are called prevention and aftercare, where the prevention is focused on stopping the ongoing fraud from continuing. Mitigation is defined as, "to cause to become less harsh or hostile" and "to make less severe or painful" (Webster, 1997, 1976, & 1941). Mitigation focuses upon fast actions that are intended to reduce the extent of the fraud, the amount of the associated fraud losses, and the effort and expense required to recover or correct the impact of the fraudulent activity. This last goal is especially important when identity theft and the resulting identity fraud are involved. The faster the fraud activity is detected and mitigation activities initiated, the less time, effort, and expense will have to be invested in correcting the consumer's credit record. The definition of mitigation in the fraud arena is to stop a fraudster from continuing or completing the fraudulent activity, to reduce their success. Mitigation activities can range from real time to delayed. Clearly the faster mitigation activities can be undertaken, the better for all involved, except, of course, the fraudster. The environment in which the business enterprise operates defines the meaning of real time. For example, real time can range from a ten second authorization in the payment card industry to a one minute phone call in the telecommunications industry, to a ten minute instant credit application in the retail industry, to a week long mortgage application process, to a month long insurance claim process, to an extended internal employee fraud investigation. Clearly the environment defines the mitigation activities that can be taken in real time.

The fundamental premise is to begin mitigation activities as quickly as possible. The speed with which mitigation can be initiated is constrained by the timeliness and capabilities of the detection systems and processes utilized. If the fraud involves an employee and detection is accomplished through receiving calls from a customer or tips from an external agency, the opportunity to mitigate losses, expenses, and impact will be significantly constrained. If, on the other hand, detection systems can alert special investigations investigators to the strong likelihood of internal fraud before customers and outside agencies become aware of the fraud, the opportunity to mitigate losses, expenses, impact, and exposure will be significantly enhanced. Mitigation performance, then, is constrained by both the business environment and the detection tools being used. Fast mitigation actions provide the promise of speedy termination of the fraud event, reduced losses, and reduced expenses and impact. Much of the resource balancing in the Fraud Management Lifecycle revolves around the appropriate allocation of sufficient, efficient, and early mitigation efforts.

Stage Five: Analysis

Analysis is characterized by activities to identify and understand losses that occurred despite the deterrence, detection, prevention, and mitigation stage activities. Analysis must evaluate the impact of fraud management activities upon legitimate customers. The product or service cost structures must be evaluated and understood to ensure the appropriate prioritization of casework. Analysis is defined as, "the separation of anything into its constituent parts or elements, to analyze, to make an analysis of, to study in detail the factors of a

situation, problem or the like, in order to determine the solution or outcome" (Webster, 1997, 1976, & 1941).

The analysis stage receives data regarding performance from each of the other stages in the Fraud Management Lifecycle and provides them with feedback regarding performance. Analysis provides the performance reporting metrics that allow fraud management to make informed, calculated, and relevant decisions. Analysis processes include the evaluation of the volume and causes of losses, the evaluation and reporting of analyst and investigator performance, the evaluation and reporting of individual and aggregate rule (detection) performance, the evaluation and reporting on predictive score performance, the individual and aggregate customer service impact for each of the various stages, the analysis of staffing productivity in each of the disciplines, the appropriate mix of resources in each discipline, the performance of new and existing strategies, the comparison of the performance of competing (champion-challenger) strategies, and supporting policy's request for retroactive and prospective hypothetical analysis.

Stage Six: Policy

Policy activities create, evaluate, communicate, and assist in the deployment of fraud policies to reduce the incidence of fraud and the inconvenience to legitimate customers, and to allocate the resources required to successfully combat fraud. Policy is defined as, "wise management, prudence or wisdom in the management of affairs, management based primarily on material interest" (Webster, 1997, 1976, & 1941). Policy must seek to balance deterrent value, loss reduction, sales volume, operational scalability, and cost effectiveness. The ability to balance all of these demands surely requires the wisdom referenced in the definition of policy. In many ways policy development is the process of constantly reassembling the situations just disassembled in the analysis stage. The reassembly needs to take advantage of the knowledge gained by analysis and combine it with internal, external, and interactive environmental factors in order to craft policies that address the whole, while leveraging the knowledge of the parts. Policy development staff are most frequently the leaders within the fraud management organization, as they must be able to consider all the disciplines within the fraud management department, as well as the needs of the rest of the business enterprise.

Stage Seven: Investigation

Investigation activities obtain enough evidence and information to stop fraudulent activity, to obtain recovery of assets or restitution, and to provide information and support for the successful prosecution and conviction of the fraudster(s). Investigation is defined as, "to investigate; a careful search or systematic inquiry; to follow up or make research by patient inquiry, observation, and examination of facts" (Webster 1997, 1976, 1941). In the fraud arena the definition of investigation needs to be expanded to include the important coordination activities with law enforcement entities.

Fraud investigations are focused upon three primary areas of activity: internal investigations, external investigations, and law enforcement coordination. The first area, internal investigations, includes investigations of employees, contractors, consultants, or vendors. External investigations are conducted on "customers" (fraudulent claims), "fraudsters" (individual crooks), and "organized groups" (an association of criminals). Frequently fraud cases are neither exclusively internal nor external. In these situations, internal fraudsters and external fraudsters work in concert to commit fraud. One of the more common examples of this situation is when a fraudster or organized group targets an employee to assist them with the commission of the fraud.

Law enforcement coordination is the provision of information and resources to, and the maintenance of, a partnership with federal, state, regional, and local law enforcement authorities. Rigorous and routine investigations provide for both an incremental lift in deterrence and the maintenance of an effective relationship with law enforcement. A rigorous investigation includes comprehensive and detailed case documentation, complete detailed descriptions of the activity, accurate and complete interview notes, extensive contact information, and high quality physical and digital evidence documentation and storage. Each case is investigated with the idea that it will be prosecuted. Case files are prepared assuming an appeals court level of review. The investigations stage benefits greatly from the planned, systematic search for facts and other supporting information, as well as the ingenuity, initiative, thoroughness, and responsiveness of the investigator. The law enforcement relationship is not a one-way street. An important part of the relationship is providing substantive responses, professional assistance, and detailed documentation when calls and other inquiries are received. Depending on the business environment these requests for information can and are received twenty-four hours a day, 365 days a year. One of the most critical support components in the investigative function is the development of training on, and maintenance of, detailed investigative procedures.

Stage Eight: Prosecution

The communications in this stage are focused upon prosecutorial and judicial authorities as well as with law enforcement. Prosecution is defined as, "the act or process of prosecuting; to conduct legal action against, to pursue by legal proceedings for redress or punishment, especially because of some crime or breach of law" (Webster, 1997, 1976, & 1941). There are three aims of prosecution in the fraud arena. The first is to punish the fraudster in an attempt to prevent further theft. Secondly, prosecution seeks to establish, maintain, and enhance the business enterprise's reputation of deterring fraud, so that the fraud community becomes aware of it. This is accomplished by the aggressive and successful catching and punishing of fraudsters who target the company. The third goal is to obtain recovery or restitution wherever possible. Some would argue that there is a fourth aim, that of satisfaction for punishing the fraudster. The emotional feelings of satisfaction, though positive, are fleeting and tend to obscure the realistic evaluation of prosecution activities. The importance of prosecution should be limited to deterrence, recovery, and restitution.

After a case has been forwarded to law enforcement for the apprehension of a suspect, the philosophical point of no return has been crossed. From this point on, the case should be prosecuted to its natural conclusion. The charges filed should be maintained and the case prosecuted even in the face of offers of restitution and mounting witness expenses. It is always advisable to request appropriate restitution as part of the sentencing recommendations.

An additional activity important to the prosecution stage is the consistent and visible coordination of supportive legislative and regulatory activities to stop fraudulent activity. This activity frequently falls to senior managers and legal counsel due to their experience, industry contacts, and broad perspective. These efforts often require, and should receive, the support of line managers and supervisors in assessing the impact of recommendations, the creation of alternatives, and the creation of committee recommendations and presentations.

Information Technology

Information technology plays a valuable role throughout the Fraud Management Lifecycle. There is not a stage in the Fraud Management Lifecycle that does not benefit from the effective application of information technology resources or suffer from inefficient or inflexible systems, processes, or staff. Information technology resources are frequently the key to the success or failure of the activities in the individual fraud stages and at times to the success or failure of the entire Fraud Management Department.

Each of the eight stages reside on a foundation of technology, as shown in Figure 5.

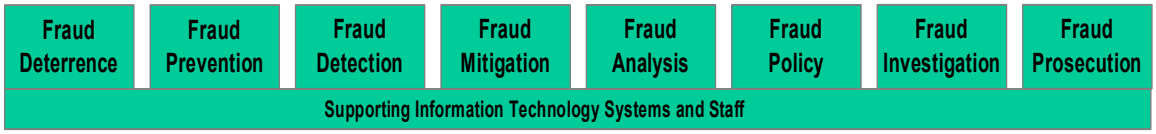

Figure 5. The Linear Representation of the Fraud Management Lifecycle Theory.

A more realistic representation of the Fraud Management Lifecycle includes not only the flow of activities from the front end (deterrence & prevention) to the back end (investigation & prosecution), but the interactions and interrelationships between each of the various lifecycle stages. The completely interconnected nodes of a Fraud Management Network are pictured in Figure 6. The linear front end to back end process is facilitated by the flow of information around the exterior of the network, while the interactions and interrelationships between the stages are represented by the connections through the center of the network.

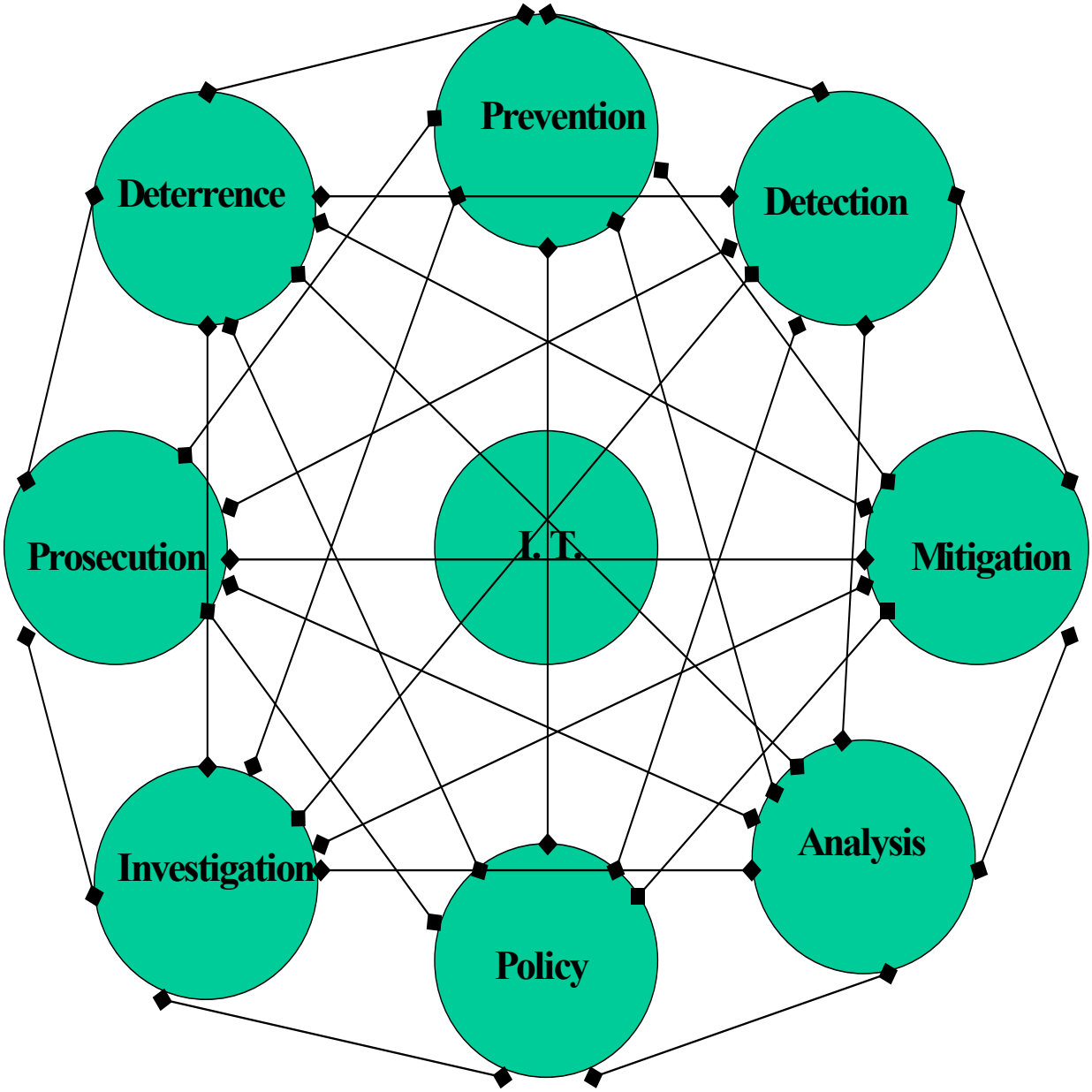

Figure 6. The Network Representation of the Fraud Management Lifecycle Stages.

The interrelationships among each of the stages or nodes in the Fraud Management Network are the building blocks of the Fraud Management Lifecycle Theory. For example, professionally run and successful investigations result in both specific and general deterrence. Similarly, increases in the difficulty component of deterrence will yield fewer cases to investigate, allowing for a more proactive prioritization of cases and more detailed and thorough investigations. In this study each of the interrelationships supporting the Fraud Management Lifecycle was assessed and evaluated. The study tested the theory that the

existence and effective management of the entire Fraud Management Lifecycle is what provides the opportunity for significantly reduced fraud losses.

Hypothesis

The primary hypothesis of this study is that there is an eight stage Fraud Management Lifecycle that drives success or failure in fraud management. A secondary hypothesis of this study establishes the premise that the successful balancing of activity within and among the Fraud Management Lifecycle stages results in improved fraud management performance. An exclusive focus on prosecution can lead to insufficient detection activities. Similarly, a lack of attention to prosecution stage activities, be they civil or criminal, can result in a reduction of the various types of deterrence. The activities in the various stages need to be balanced for effective Fraud Management. Balanced activity levels do not imply balanced or equal resource allocation, but rather the correct allocation of resources to ensure a coordinated and effective fraud mitigation effort.

The Fraud Management Lifecycle is postulated to be present in many different industries with differing fraud problems and unique responses to fraud. Much of the value of the Fraud Management Lifecycle theory is inherent in and derived from its applicability across various industries. Although the study encompassed only retail financial institutions, mortgage, telecommunications, and insurance companies, the focus was to determine if the Fraud Management Lifecycle Theory is functional across various industries. Industries from banking and insurance to telecommunications and healthcare all endure significant fraud. This study, then, was designed to identify the applicability of the Fraud Management Lifecycle theory and the absence or presence of interactions among deterrence, prevention, detection, mitigation, analysis, policy, investigation, and prosecution in several different industries.

Methodology

An extensive and detailed analysis of the available literature dealing with each phase of the Fraud Management Lifecycle was undertaken. Much of this policy-based hypothesis was evaluated against existing writings about individual lifecycle stages. Figure 7 depicts a matrix identifying the specific interactions and influences between and among the various lifecycle stages. These interactions are derived from an analysis of the ANTA (Australian National Training Authority) competency standards, interviews, case study responses, consulting engagements, fraud and security publications, AAAI (American Association for Artificial Intelligence) workshop papers, and other relevant processes, procedures, guidelines, and analysis. The Fraud Management Lifecycle stage relationships were evaluated on both the stages involved and the direction of the interaction. For example, relationship number fifty-six (56) represents the impact of prosecution stage activities upon deterrence, while relationship number forty-

nine (49) represents the impact of deterrence stage activities upon prosecution. One of the study interview respondents shared the following anecdote. The representative institution received a call from a law enforcement agency subsequent to an arrest where the fraudsters had indicated to the authorities that they stayed away from the respondent's institution because they could only get a limited amount of money. Instead they went to other institutions where more money could be gained from the same effort. This example shows the impact of detection on deterrence (relationship number fifty-one (51)), where aggressive detection efforts resulted in increased deterrence. If the fully interconnected Fraud Management Lifecycle network exists, identifiable and explainable relationships should exist in all the fifty-six relationship categories.

Stage	Prevention	Detection	Mitigation	Analysis	Policy	Investigation	Prosecution	Deterrence
Prevention	N/A	1	2	3	4	5	6	7
Detection	8	N/A	9	10	11	12	13	14
Mitigation	15	16	N/A	17	18	19	20	21
Analysis	22	23	24	N/A	25	26	27	28
Policy	29	30	31	32	N/A	33	34	35
Investigation	36	37	38	39	40	N/A	41	42
Prosecution	43	44	45	46	47	48	N/A	49
Deterrence	50	51	52	53	54	55	56	N/A

Figure 7. The Fraud Management Lifecycle Relationship Matrix

In addition to looking to the literature for signs of the existence of a Fraud Management Lifecycle, interviews, questionnaires, and case study responses were included. The author used the views and observations of individuals working in and managing fraud prevention operations. Unlike the open-ended questions utilized in Jakubowski, Broce, Stone, & Conner, the interviews included both open-ended and closed-ended questions and was supported by a respondent review of an introduction to the Fraud Management Lifecycle Theory. In addition to the introduction, a hypothetical case study was presented to some of the respondents. The respondents' questions, comments and responses were analyzed by industry and across industries for the presence or absence of lifecycle stages, as well as interactions between stages. The author further evaluated the theory through a series of direct observations and onsite visits at a fraud management organization that was undergoing significant change and reorganization. The industries represented by the respondents and the author's observations are retail banking, credit/debit card issuers, insurance, telecommunications, and mortgage.

The limited direct and indirect observations have validity and reliability issues

along with potential ethical concerns. The ethical considerations revolve around the disclosure of proprietary and confidential deterrence, prevention, detection, mitigation, analysis, policy, and investigative information. The risk of inappropriate information disclosure was two-fold; first was the risk of fraudsters (internal and external) obtaining access to critical information and then being able to adapt and create new attacks. Second was the risk that competitors would obtain critical information and be able to deploy superior measures that could drive the fraud to a competitor. In order to protect against these risks no details of the respondents' specific deterrence, detection, policy, prevention, or investigation activities were published. Any examples used have been made anonymous and provided in general form. The respondents' names, titles, and employers have been left out. Only the respondent's industry is referred to in order to establish the cross industry applicability of the lifecycle. The onsite observations do not refer to the companies by name and any performance information has been generalized in order to ensure anonymity.

The existence of the lifecycle and the linkages and interactions between the stages were the topics for this analysis, rather than the detailed strategies deployed in each stage. The anonymity limitations were not considered to be significant, as the study used the interviews, responses, and observations as a confirmation of, and a supplement and challenge to, the literature review. The methodologies employed in the study include theoretical research, opinion polling, exploratory interviews, case study responses, and direct observation.

Continued research, interviews, surveys, case studies, and direct observation of companies undergoing significant change in fraud management approach will likely provide fruitful analysis. The evaluation of a fraud management organization that is evolving from a reactive approach to a proactive approach will provide highly relevant and useful information. This information can be used to further confirm the existence and importance of balance in the Fraud Management Lifecycle.

Study Findings and Discussion

Key Findings

The interview and case study respondents confirmed the existence of the Fraud Management Lifecycle stages in their business environments. Each participant indicated that all eight of the Fraud Management Lifecycle stages were present. The industries represented by the respondents were insurance, telecommunications, mortgage, and retail banking. Confirmation of the lifecycle in four industries separate from the payment card industry, from which the theory was initially conceived, is encouraging. The second hypothesis, successful balancing of Fraud Management Lifecycle activities leads to improved performance, was also detected, although not as universally as the presence of the lifecycle. One of the companies specifically attained improved loss performance as a result of increasing their focus and attention on prevention

stage activities. Another company attained improved performance through the introduction and use of new detection technology and techniques based upon advanced statistical analysis techniques. Although these are encouraging findings, more detailed analysis and research is required to go beyond the initial identification of the importance of correctly balancing the lifecycle stage activities. As further analysis is undertaken it will be important to take into consideration the environmental impacts upon the appropriate weighting of and emphasis placed on the Fraud Management Lifecycle stages. Several of the interview respondents indicated that the environment strongly influenced their ability to undertake activities in some of the lifecycle stages. For example, one of the insurance industry respondents indicated that prevention stage activities were difficult to implement due to the nature of the claims process and a diverse legal environment.

The case study was designed, in part, to elicit responses regarding the optimal way to structure a fraud management organization that spanned multiple product or organizational silos. Each of the individual Fraud Management Lifecycle stage activities was specifically addressed from this organizational perspective. Since the lifecycle stages were presented as part of a clear organizational challenge, they could be evaluated in detail as a supporting element in the organizational redesign that the case study was designed to generate. Since the overall focus of the case study was bigger than the individual lifecycle stages, the potential for influencing the answers to the questions by the content was reduced. A telecommunications respondent answered the question; “Do you have any general comments or questions on the material?” with the following observation: “…for me the case reflected a clear need for organizational restructuring to accomplish the ideal resolution.” The restructuring referred to replacing the existing decentralized approach with a structure that “established cross unit accountability to a common CRO (Chief Risk Officer) function.”

It is interesting to note that the banking-based case study, with multiple fraud departments structured around product groups, provided a significant departure from the structure in place at the telecommunications company. This is partly due to the limited number of fraud types in the telecommunications industry and the broader diversity of fraud in the banking and financial services industry. In responding to the question; “How are the fraud management functions in your company organized?” the telecommunications respondent answered “centralized under two separate teams…” The two teams were usage fraud and payment fraud and they were described as follows. “Usage fraud resides within an enterprise risk management organization. This team uses customized fraud detection tools to monitor usage on the network to detect patterns of fraud and it administers prevention tools (i.e. handset authentication). It also serves as the forward looking think-tank to determine what types of usage fraud are likely to appear in the future, and plan for preventative and detection measures.” In contrast, “Payment fraud resides within the receivables management organization, reporting to a risk management call center director and is

responsible for monitoring patterns of fraudulent electronic (credit card, EFT) and check payments." It would certainly be expected that working in a more centralized structure would lead to a recommendation to centralize the disparate functions in the banking case study.

It is also interesting to note that the payment card fraud groups were distributed across various payment methodologies and call center locations. This distribution resulted in different levels of deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution. This is quite similar, although smaller in scope, to the product line distribution in the banking example. It reinforces the historical evolutionary creation of fraud structures and integration, as opposed to an approach that seeks to maximize the interaction among and balance the resources allocated to the various fraud management lifecycle stages.

In addition to the confirmations of the presence and managing of the Fraud Management Lifecycle, there were some initial indications of a need to adjust and expand the lifecycle to realign the original prevention stage and introduce a stage of activity more focused upon stopping the fraudulent activity from succeeding or continuing. The stage names considered were interdiction, mitigation, and intervention. Mitigation was selected because it was the most applicable to both the inherent actions in the stage and the objective of reducing losses. It was also the term most recommended by the study respondents. Introducing an eighth stage that is focused on stopping fraud attempts during the commission of the fraud allows the prevention stage activities to be more closely aligned with deterrence, and to precede detection instead of following it. In this alignment, prevention can truly be focused on preventing fraud from occurring, while allowing the combination of detection and mitigation to stop fraud once it has been initiated. The need to further evaluate the relationship between situational deterrence and prevention activities was brought to light in the literature reviews. The ability to separate activities that make the commission of fraud more difficult (prevention) from those activities that intervene to keep the fraud from continuing or being successful (mitigation) will allow prevention to be more appropriately placed after deterrence and before detection. This facilitates the placement of mitigation after detection and before analysis, which appropriately positions the actions to stop fraud from continuing or being successful after the fraud or fraud attempt has been detected. This placement is also consistent with real time environments, where the combination of detection and mitigation efforts can prevent losses from occurring. In these environments realignment is supported because the fraud or fraud attempt was not prevented by prevention stage activities even though loss was prevented by timely detection and mitigation activities.

Another change that came as a result of both the interviews and the literature research was the title for the lifecycle theory. The initial title for the theory was the Fraud Lifecycle. The new title, The Fraud Management Lifecycle, is more

appropriate, as it describes the processes and activities surrounding the management and reduction of fraud losses, as opposed to the fraudulent activity or the fraudster themselves. The new moniker indicates that the theory deals with the actions, activities, processes, procedures, organizational designs, economic analysis, and intra-entity exchanges necessary to manage and reduce the impact of fraudulent activity.

Discussion

The insurance companies, as expected, showed the presence of the lifecycle, as did the retail banks in the survey. However, their focus and activities were different. This could be a result of the environment, the fraud, the business activity, or a combination of the three. Much of the insurance activity was concentrated in the investigation, analysis, mitigation, policy, and detection stages, while less attention was given to deterrence, prevention, and prosecution. The banking responses on the other hand were more focused on prosecution, mitigation, prevention, deterrence and detection. McRae asks an important question regarding insurance companies, "How will practices evolve? The answers may lie in how the credit card and telecommunications industries, which also faced serious fraud issues, have migrated from manual fraud identification processes to sophisticated detection technologies" (McRae, 2001). Whether the insurance industry follows McRae's evolutionary path remains to be seen; however, balancing and managing the Fraud Management Lifecycle throughout the evolution will continue to be important to their success in reducing fraud.

All the industries and interviewees indicated a similar set of organizational characteristics. They were organized around the fraud itself, as opposed to the management of the fraud lifecycle activities. Many of the respondents indicated a decentralized and segmented structure that revolved around the fraud and the line of business impacted. In most cases each line of business had similar repetitive structures. Several of the interview respondents spoke of the presence of a series of vertical structures within the fraud area. These silos of activity limited effective communication and, as a result, reduced the scope of the analysis function and the consistency of the resulting policies, detection, mitigation and prevention efforts.

As was discussed earlier, the two common structural designs involved the type of fraud and a business unit or product line. This reinforces the belief that most fraud reduction organizational structures today are a result of organizing around the fraud, the line of business, or both. These evolutionary and reactive types of designs provide an excellent opportunity for improved performance through the management of the stages of the Fraud Management Lifecycle. For example, one respondent commented that when his company began to expand its focus from investigation activities to preventative activity, their performance improved. This also supports the premise that the more effective the organization becomes at the early "proactive" stages of the fraud management lifecycle, the greater the

impact will be on reducing losses. A mortgage industry respondent confirmed the silo structure's negative impacts upon structured communication when he indicated that cross-divisional communication had "no formal channels" and was accomplished mostly through "informal channels through direct contact." Unstructured communication relies upon individuals and catalyst circumstances that cannot be relied upon to provide consistent or comprehensive information flow between the various Fraud Management Lifecycle stages. All of the respondents had investigation functions that provided some level of specific and general deterrence. This balance between the resources allocated to investigation, detection, and mitigation is critical. Too few investigators results in reduced deterrence, evidenced by escalating caseloads and continuously increasing average losses per case. Too few mitigation analysts results in reduced detection, which also results in escalating caseloads and increasing losses.

One of the most common mitigation activities referred to in the interviews was fraud awareness training, including teller training and underwriter training. Training the individuals who analyze and process customer information and have direct customer interaction is a common and important step in improved detection performance. This is especially true in areas where fraud detection is not yet, or cannot be, automated using statistical techniques. Even after automation, the continuous training of staff to be aware of identify fraud "red flags" has value in improving detection, mitigation, and detection performance. The industries reviewed in the study were providing fraud awareness training to their front line staff.

They were also using a common experience based judgmental process for the prioritization of cases to be worked by investigators. Cases were prioritized for inclusion using the experience and judgment of supervisors and managers and a dollar threshold. The mortgage industry respondent indicated that investigative case prioritization was "filtered through supervising investigator(s)." Their performance and efficiency could be enhanced through better integration and communication between the analysis and investigation stages of the lifecycle. The analysis function, whether performed in the investigative area or the analysis area, can provide support to the judgmental prioritization process through the use of detailed quantitative metrics. Analysis can be useful in assessing the probability of attaining the greatest deterrent, restitution, and recovery impacts, thus maximizing the contribution and value of the scarce and expensive investigative resources. A fixed dollar threshold, $25,000 for example, limits the ability to deter escalating lower dollar fraud cases and those that are intentionally grouped just below the established investigative threshold in order to avoid detection. Tracking individual cases over time by their fraud characteristics, their recoveries, and their prosecutorial success can provide analytical recommendations on case prioritizations. Case prioritization is as common a situation as it is challenging. No business has enough resources to investigate every case of real or suspected fraud. On the other hand, a static dollar

threshold can be easily reverse-engineered and can actually encourage fraudulent activity below the threshold. Analysis can provide investigations with the tools and statistical analysis to evaluate past investigative performance as well as linking analysis. The ability to aggregate cases and link cases early and quickly in the investigative process provides the opportunity to combine seemingly disparate cases into single aggregated investigations. Aggregation provides an important prioritization element, as well as enough combined value to warrant detailed investigation and prosecution. Law enforcement is more likely to accept aggregated cases due to both the dollar amount and an established pattern of fraudulent activity. An increase in successful investigations that lead to prosecution, whether civil or criminal, yields both an increase in general and specific deterrence.

The interviews introduced an expected element into the analysis: environment. Some respondents indicated that their companies did not have an aggressive set of prosecution stage activities. The environments in question were limited in several respects, including diverse geographical jurisdictions and law enforcement's lack of interest, knowledge, and capacity to pursue many criminal prosecutions. The respondents also did not pursue many civil litigation cases. This introduces the question of how various environmental factors from the business and regulatory environment and from society as a whole impact the application and balance of the Fraud Management Lifecycle. Further research will most likely reveal the presence of the lifecycle with differing resource allocations between the lifecycle stages. These varying resource allocations are expected to be driven by the business, regulatory, technical, and social environment, as well as the corporate philosophy of the business.

Another result of the silo or independent vertical structure was a divergence of available systems and technical tools. Some areas within the same company were more advanced than others, usually due to a single or small group of individuals who were able to deploy new analytical and detection tools. The awareness and use of these tools were not shared evenly throughout the organization, often residing in single business lines or individual areas of fraud focus. The use and integration of technology continues to provide substantial value for both efficiency of workflow and the prioritization of mitigation and investigative activities. The tools available today provide the opportunity for faster and smarter work. Deploying technology throughout the fraud management organization is an important component to successful balancing among the lifecycle stages. Although the human element can never be completely replaced, statistical analysis is essential to effective fraud management.

Leveraging tools, resources, knowledge, philosophy and the Fraud Management Lifecycle theory across existing silos is vital to the evolution of methods and the overall success of the fraud management department. The common stage interactions in the various silos of a distributed fraud management organization provide a basis with which to foster performance, enhancing cooperation instead

of destructive competition. If treating fraud management as a competitive advantage is risky in the external environment, it is completely counter productive in the internal environment of a company. Everett Whatley describes the relationship between card security and corporate security. “Corporate security and card security have never had the same perspective, and, in my experience, rarely even cooperate beyond a superficial level. There is sharp competition between them …” (Whatley, 1998).

Interview Summary

Although limited in scope, the interview portion of the study provided confirmation of the presence of the Fraud Management Lifecycle. Each interviewee and industry performed deterrence activities through the application of other stage activities as well as warnings, access controls, and other security measures. Each industry undertook direct prevention activities. Detection, either through automated systems, manual review, or combinations of the two was employed by all the respondents. They also all reported mitigation activities to reduce fraud losses. Analysis by each of the industries and respondents was performed throughout the organization, focusing on an analysis of the fraud and on the performance of detection activities. Each industry performed policy stage activities in the establishment of the rules of engagement for the various stage activities. Investigative activities were present in each industry with variances in approach due both to environmental issues and corporate philosophy. Similarly, prosecution activities were dealt with in each industry, again with varying degrees of emphasis. All of the respondents relied upon technology to enhance their efficiency and effectiveness. The interviews and the literature research both reinforced the presence, relevance, and applicability of the Fraud Management Lifecycle Theory.

Onsite Observation Summary

The fraud division observed was part of a company that has approximately ten million consumer accounts, 3,500 locations, and in excess of 33,000 employees. Their annual fraud losses at the time were approximately seventy-nine million dollars. The onsite observations were performed over a twelve month period from November 2002 to November 2003 and will continue for approximately another eighteen months. The results described here are preliminary, as approximately one-third of the planned changes have been made and implemented as of this writing. Changes to the fraud organizational design and fraud reporting were the initial focus. The remaining changes, which deal with integrated and automated case management capabilities and the implementation of statistical detection models, are planned for the remaining eighteen months of the project.

The intent of the organizational plan that was implemented was to make the fraud division more proactive in the identification and mitigation of fraud losses. The organization had five types of fraud operational centers in eight physical locations. In addition to the inefficient and ineffective decentralized structure, six

other areas were identified as causes for low operational productivity. There was (1) too much effort on investigation in the mitigation stage, (2) no defined strategy or fraud policy, (3) too much time being spent on inbound calls of little fraud reduction value, (4) a lack of appropriate focus on working fraud cases, (5) no consistent and accurate productivity reporting and therefore poor analysis, and (6) a significant amount of manual work that could be automated using information technology tools.

The recommended operational changes addressed improvements in each of the following areas. Appropriate fraud management information reporting was established. Productivity was improved by increasing the number of cases worked per hour by analysts and investigators. Standard policies that ensured a consistent and controllable set of tactics were created and deployed. Organizational design changes were implemented to centralize and coordinate activity, resulting in fewer teams, consistent work, and predictable results. Standards were enhanced to ensure consistent work performance measurement and feedback across the organization.

To overcome the division's fragmentation the reporting structure and physical locations were centralized. Three new units were created to accomplish this: Strategy and Policy, Operations, and Special Investigations. The strategy and policy unit was designed to include the analysis, policy, prevention, and prosecution lifecycle stages in addition to the internal fraud function. It includes teams responsible for analytics, policy, and liaison with police. The analytics team was set up as the central point for data analysis. The policy team then uses the output from the analysis team to drive policies across the organization. The police liaison team was established to ensure consistent and regionally targeted coordination with law enforcement and prosecutors.

The operations unit covers the implementation of the detection, mitigation, and investigation lifecycle stages and includes the following six focused teams, all of which have daily interactions and communications with the strategy and policy teams.

1) A fraud mitigation team	Uses the current tools and the soon to be deployed analytics and case management system to confirm the presence of fraud and stop it from continuing.
2) A fraud call center	To handle the increased volume of calls generated by the mitigation teams and the investigation team.
3) An investigation team	To perform in-depth review where linkage, loss amounts, and suspects warrant additional activity.
4) A fraud challenge and aftercare team	Tasked with assisting customers with the impact of fraud and challenging customers who have submitted fraudulent claims of fraud.
5) A fraud recovery team	To manage collection of outstanding balances and restitution.
6) An operations and administration team	To ensure the creation of metrics, measurements, and required clerical support.

The separate special investigations unit was established to ensure coordination and confidentiality in the employee-employer relationship.

This combined effort resulted in approximately twelve and one-quarter million dollars of net benefit in the first ten months of the project. In addition, the special investigations team suspended, dismissed, and referred for prosecution sixty-one employees in the first nine months of the project. Continued improvements in loss performance are expected as enhanced analytical detection tools and improved case management capabilities are deployed by I.T. Though preliminary, these results, when combined with the results of the interviews, case study, and literature review, provide a positive reinforcement of the Fraud Management Lifecycle theory. They are a testament to all the consulting team members. Analyzing the interactions between the various lifecycle stages shows further evidence of its existence and significance.

Interactions in the Fraud Management Lifecycle

The Fraud Management Lifecycle theory is a representation or model of the steps, stages, or phases through which fraud abatement activities flow. This lifecycle, though impacted and influenced by numerous environmental, industry, and economic factors, is present wherever fraud mitigation efforts exist. The Fraud Management Lifecycle can be pictured as a completely interconnected set of nodes in a network. Each node or stage has direct interactions with and influences upon each of the other stages in the lifecycle, as well as with the internal and external environment. Internal environmental factors are those arising from within the business enterprise, e.g., fraud management philosophy, information technology resources, product margins, and risk tolerance. External environmental factors are those derived from outside the organization, including regulatory requirements, fraud trends, fraud methods, competitors, and business partners. The combination of internal and external factors influences the fraud management

organization. For example, the constantly evolving interaction of fraud abatement and fraud perpetration activities drives a migrating equilibrium. The equilibrium is achieved as the costs of reducing fraud begin to approximate the value of the fraud targeted. It migrates as new fraud methods are conceived and implemented, and the process begins again.

The analysis and evaluation of the circular, recursive, non-sequential relationships among all of the stages in the Fraud Management Lifecycle is important in order to establish an understanding of how the components of the lifecycle influence each other. The trend of evolution in fraud management is toward increased complexity and increased speed of change in an expanding environment. The challenge for the fraud management professional is to manage the evolution effectively. Fundamental changes in structure are necessary to maintain a fraud management function that can adapt quickly and successfully balance fraud control, customer impact, resource requirements, and information technology budgets. The interactions of the stages in the Fraud Management Lifecycle illustrate the flexibility and adaptability of the network design.

Prevention Interactions

While the focus of the prevention stage is preventing fraudsters from succeeding, it is also an objective of all the stages. Each of the stages participates in and influences prevention's attempts to stop fraud once deterrence has failed to keep it from being attempted. From developing and evaluating prevention actions in policy and analysis to training on red flags and methods reviews in investigations and prosecution, prevention is integrated with each of the other stages.

A common example of the interaction between prevention and analysis deals with the identification and creation of fraud profiles. Analysis is responsible for the creation of these profiles and frequently prevention is the stage where the actions on the profiles are deployed. Fraud profiles are a judgmental assessment of the potential fraudster, methods, target, and impacts of various types of fraud that are relevant to the organization. Once created, fraud profiles provide specific direction to prevention, policy, and other stages in the fraud management lifecycle. Samociuk and Iyer provide excellent guidance when they say "participating employees [creating fraud profiles] should 'think like a thief' in order to identify fraud opportunities" (Samociuk, et. al. 2003). Their focus and that of fraud profiling in general is to understand the risk of fraud.

Detection Interactions

Detection includes the identification of fraud, fraud attempts, and testing of fraud methods. This broad definition goes beyond just the detection of fraud where losses occur. When asked the question, "Does the definition of detection make sense? Is it relevant in your environment?" the mortgage industry respondent answered, "Yes, well done to include attempts and testing in your definition." Confirmation of the need to include detection of testing and failed fraud attempts crossed each of the industries evaluated.

Detection occurs throughout the Fraud Management Lifecycle. One of the keys to success in fraud management is to use detection as early as possible. However, it is important to be aware of and focus on the detection of fraud wherever it occurs in the Fraud Management Lifecycle. While early detection is desirable, it should not be the sole aim of detection activities. In fact, depending upon the environment, multiple detection layers can increase efficiency, reduce customer impact, and reduce staffing expenses.

Mitigation Interactions

When a fraud is perpetrated in spite of deterrence and prevention, the actions taken at the mitigation stage allow the first opportunity for fraud management individuals to see the circumstances surrounding the fraudulent activity. The frauds identified and detailed in the mitigation stage -- successful, attempted, and testing -- provide valuable feedback on the limitations of the current detection activities. The types of mitigation activities deployed drive the categories of analysis that are possible. Much of this stage's impact upon policy revolves around the required reaction to fraud that was not detected and stopped completely or soon enough. The activities at this stage provide information about specific fraudsters and evolving fraud trends for the investigations stage. Mitigation stage activities are crucial to the effective prosecution of employees involved in internal fraud. Aggressive, efficient, and proactive mitigation activities can result in increased general deterrence. The level of I.T. support can greatly impact the speed and breadth of the actual loss avoidance activities.

Analysis Interactions

The estimation and evaluation of the value provided by new, enhanced, or altered prevention activities is an important analysis activity. Analysis stage activities drive the creation, evolution, and performance measurements of detection methods, processes, and tools. Analysis provides feedback to mitigation regarding the performance of activities to successfully act upon detection alerts to reduce fraud losses. It provides the information on current performance across the fraud unit and provides information about the existence of policy opportunities. Analysis provides investigation with an analytical understanding of the environment as well as an evaluation of their investigative success and activity. Fraud and performance analysis are important elements of prosecution stage activities. Analysis is able to estimate deterrent impact. Information technology provides analysis with the necessary access to the data surrounding legitimate and fraudulent activity.

Investigations Interactions

Investigation activities are represented by the gathering of enough evidence and information to stop fraudulent activity, mitigate the impact of fraud losses, provide support for prosecutions, and reinforce deterrence. As a result of these and other relationships, there are numerous interactions between investigations and other lifecycle stages. Investigative activities, such as link analysis used both to

investigate and aggregate cases, uncover the existence of frauds, attempts, and testing that were unknown to the detection, mitigation, and analysis activities. Feedback on these cases provides valuable input to the analysis, prevention, and policy stage evaluations and actions. Investigations can support mitigation by providing an awareness of tactics, patterns of behavior, and methods of operation. These result in an increased awareness and accuracy of mitigation actions. Investigation provides micro case by case analysis of the fraud, which is complemented by the macro level analysis of overall case statistics. Finally, investigation interacts directly with prosecution. Investigative actions provide, or fail to provide, the basis of foundation a prosecution needs to proceed.

Prosecution Interactions

Prosecution, like deterrence, is the culmination of actions throughout the various lifecycle stages. Prosecution attempts to obtain asset recovery, criminal and/or civil restitution, and provide specific and general deterrence as a result of prosecuting the case. Prosecution, then, is dependent upon and controlled by the various successes and failures of the other stages in the fraud management lifecycle. Successes are represented by evidence gathering in investigations, evidence retention in mitigation, and case identification in detection. Similar relationships exist between policy implementations and performance analysis. Failures are represented by failures of deterrence and prevention, as well as potential failures in the speed of detection and mitigation actions. Prosecution relies heavily upon successful, thorough, and accurate investigations to provide a properly prepared and presented prosecutable case. Policy interactions with investigations can be represented by the ability to deploy consistent, non-discriminatory policies in an internal fraud investigation, as well as the ability of policy staff to communicate fraud policies clearly and accurately to the courts.

Deterrence Interactions

Deterrence is enhanced by actions throughout the Fraud Management Lifecycle, from the consequences created by investigation and prosecution activities to the front-end prevention and detection difficulties and road blocks, to the ability to perform fraud. Each stage in the lifecycle can and should contribute to effective deterrence. This is represented by policies to prosecute all staff members who engage in fraud, fast analysis of new fraud trends, the fast adoption of new preventative policies, and continual security enhancements to make fraud increasingly harder to commit. Deterrence, then, is inherent in the actions taken in each of the other lifecycle stages.

The deterrent value (difficulty component) of a fraud management operation is enhanced by the timely and accurate deployment of automated verification, confirmation, and validation activities that occur at the front end of the transaction process. The deterrent value of deploying industry standard checks and verifications is represented in two ways. First, if the enterprise is the only, or one of a few, not to deploy the tool, fraudsters will move to them because of the ease of success. Secondly, there is an inherent increase in difficulty when the tool is

deployed. When you are the only company, or one of a few companies to deploy, you divert the fraudulent activity to your competitors.

The lifecycle stage interactions are well illustrated through the use of graphs with a polar perspective. The following series of diagrams illustrate how the interactions between stages can create weak points in fraud protection. They also show quite visibly how imbalances cascade to create broad vulnerabilities. Samociuk and Iyer utilize this method to illustrate companies with low and high resistance to fraud. Although their six categories are "objectives, understand the risk [Analysis], reduce the risk [Prevention], detect attempts [Detection], manage incidents [Mitigation], and review and enhance," they are similar to stages in the Fraud Management Lifecycle. Their treatment can be expanded to include the stages of the fraud management lifecycle, the level of fraud resistance, and the impact of the relationships between the lifecycle stages. For example, the first diagram shows both a balanced strong and weak resistance. The inner circle displays a weak resistance while the outer octagon represents a strong resistance.

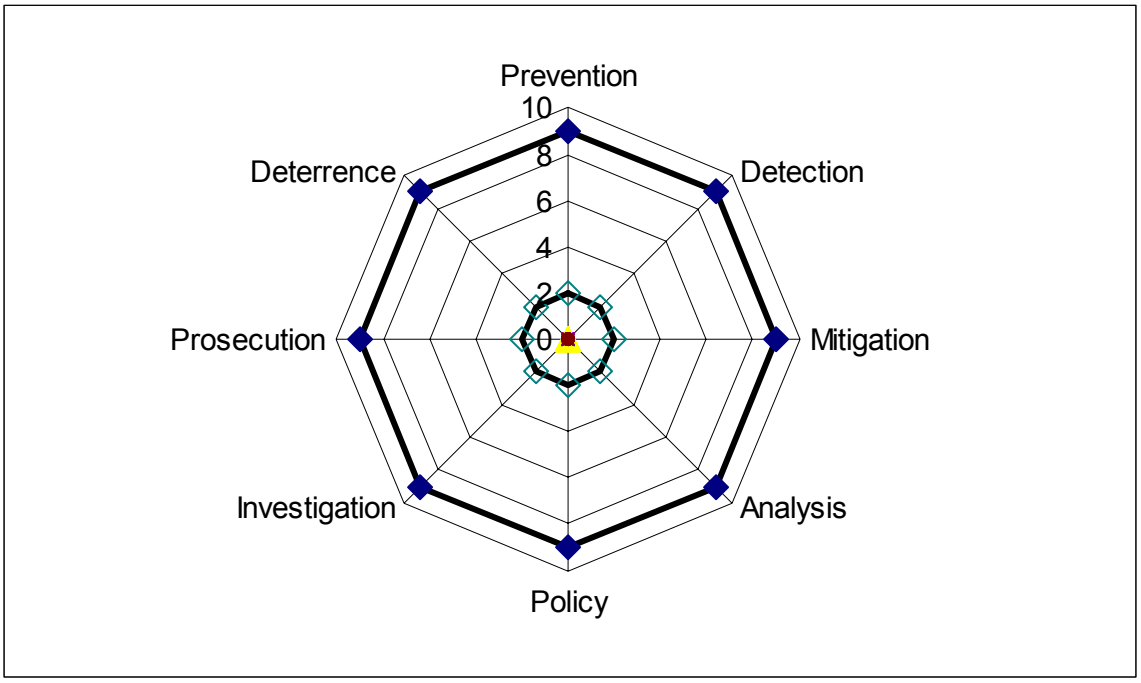

Figure 8. Strong and weak fraud resistance.

The second diagram, Figure 9, illustrates a fraud management organization with significantly weak detection systems, processes, and procedures. The weaknesses in this stage clearly identify a strong likelihood for excessive losses and a prime target for improving the balance of the fraud reduction efforts.

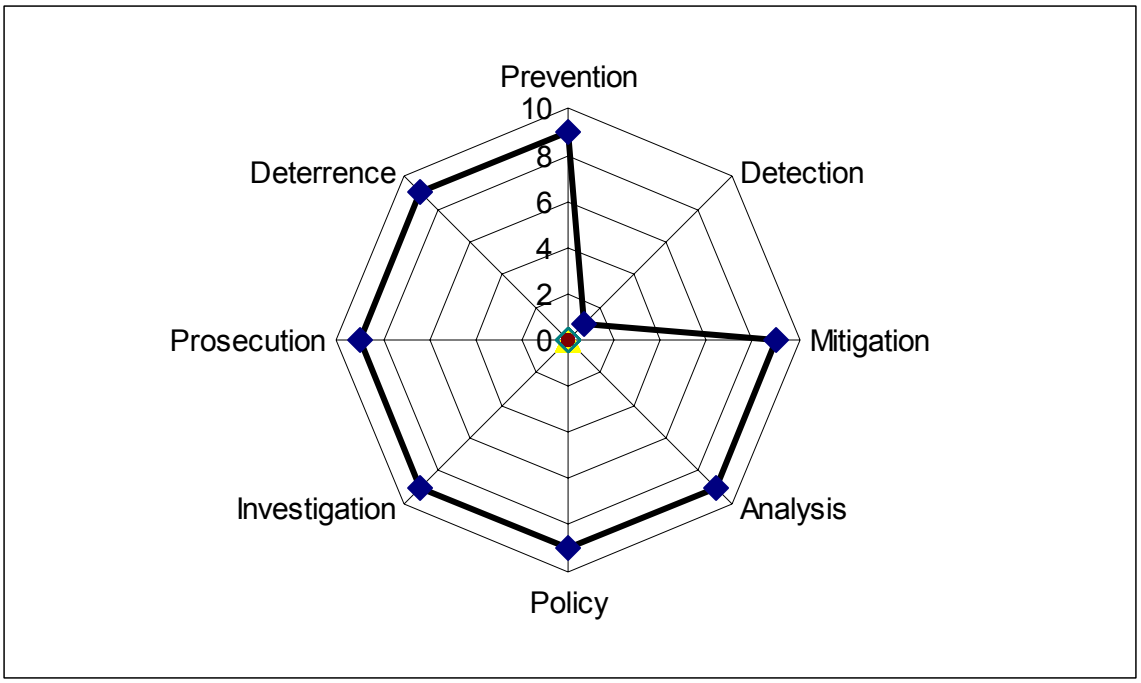

Figure 9. Weak fraud detection performance.

The third diagram illustrates a condition where mediocre investigation performance results in almost non-existent prosecution opportunities and, as a result, significantly reduced deterrence results.

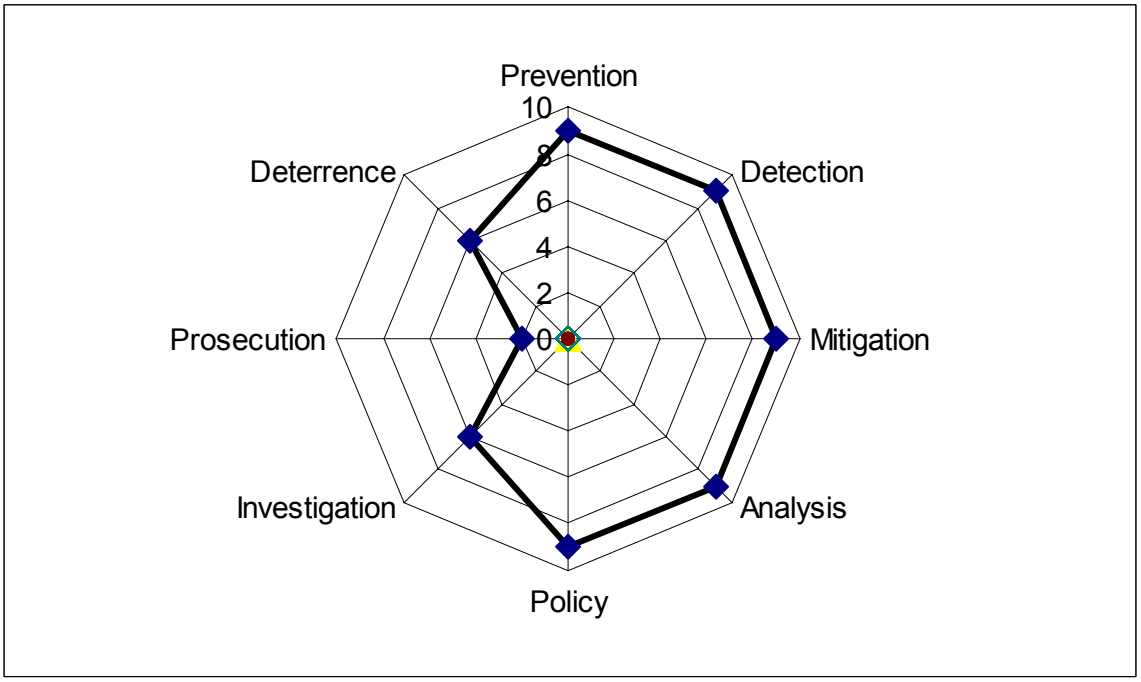

Figure 10. Mediocre fraud investigation and its impacts.

The fourth diagram shows the impact of weak fraud analysis and how it results in

ineffective fraud policies which, in turn, result in inferior prevention and reduce detection.

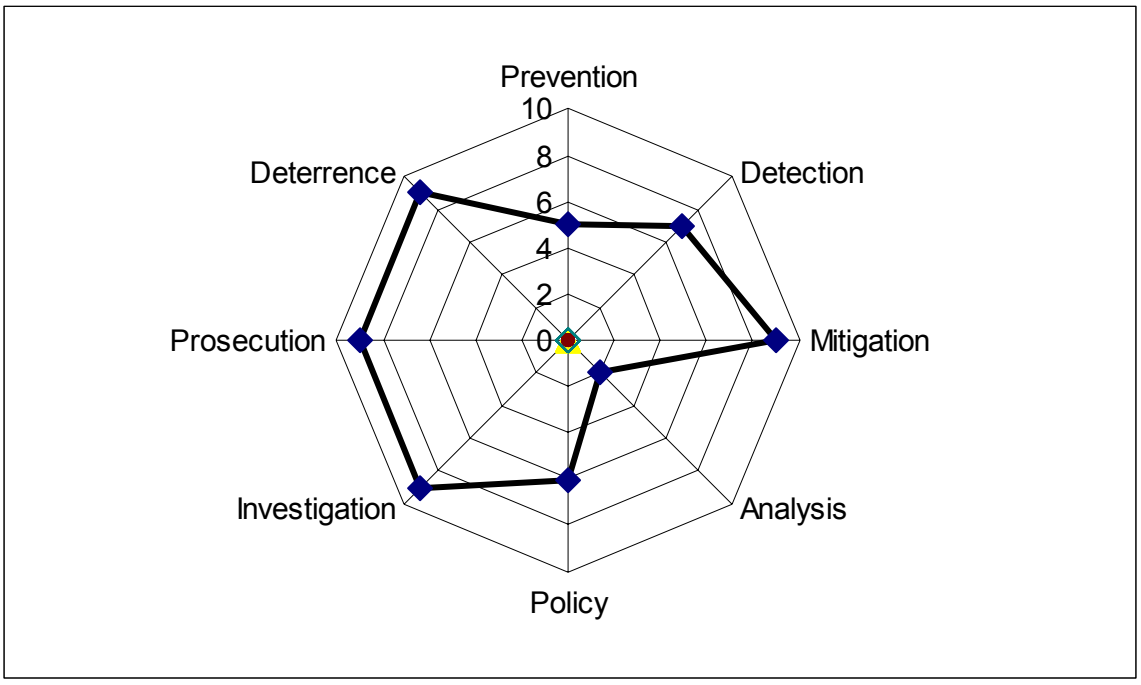

Figure 11. Weak fraud analysis and its impacts.

Conclusion

The successful identification of the presence of the Fraud Management Lifecycle by this study reinforces the belief that effective fraud management balances the activities in each stage of the Fraud Management Lifecycle. The preliminary confirmation, from the retail banking industry, that a balanced approach was more successful than a single focus, reinforces the hypothesis that the activities throughout the lifecycle should be balanced. However, this balance does not indicate an equal allocation of resources among all the lifecycle stages. Successful application of the theory into practice will require a sequence of intervention activities. The activities proposed are:

- identification of the current stages receiving focus;
- identification of environmental risks and constraints;
- identification of existing and missing interactions between the various stages;
- identification of the correct resource balance among the stages;
- identification of technical improvements and enhancements to facilitate fraud reduction;
- introduction of a new fraud management philosophy focused on the continual improvement of technical tools and the successful balancing of the activities in and among all the stages in the fraud management lifecycle.

The size, scope, duration, and success of such an intervention will vary significantly from business to business and industry to industry. However, a focus on selecting the correct balance for the lifecycle stages remains the core element to immediate and continuing success in fraud risk management.

The tentative confirmation of the Fraud Management Lifecycle led to the next level of evaluation which was to evaluate different industries for the presence of the lifecycle and review implementations of the lifecycle concept. The importance of the Fraud Management Lifecycle lies in its applicability in many different industries and environmental situations. Therefore, it was necessary to expand the scope and depth of participating companies. The ability to apply the lifecycle structure will provide not only superior fraud loss reductions, but it will provide a template that can be utilized by fraud management professionals across a broad range of industries. As the theory is refined and its application expanded, many companies and industries now operating with significant fraud losses can begin to reduce those losses in an economically efficient manner. The benefits to individual companies are realized in a number of areas: lower costs for providing the product or service, yielding either lower prices for consumers or higher margins for companies or both, greater investment opportunity in new or enhanced products or services, lower fraud prevention expenses and reductions in the opportunity costs of fraud reduction activities, and a reduced impact on legitimate customers through improved customer relations and simpler customer acquisition. The successful management of the fraud management lifecycle also provides a more cohesive and coherent approach to fraud management that can be explained to and understood by the rest of the functional disciplines in the business. Each area of a business, from accounting to customer service and from sales to marketing, will be better able to understand the needs of and value provided by fraud management. Their awareness and understanding is important to continued fraud reduction, because fraud prevention is never, nor should it be, the core business focus. Businesses exist to provide goods and services, while fraud management plays a supporting role to the larger business objectives. Successful implementation of the Fraud Management Lifecycle increases the likelihood of proactive fraud risk management and, therefore, the success of the enterprise.

Although the second study identified the presence of the lifecycle in two additional industries, mortgage and telecommunications, further research is needed for a more detailed confirmation of the presence and impact of the lifecycle within the industries studied. The details and importance of the various intra-cycle interactions need to be observed, analyzed, and evaluated in depth. In addition, other industries, such as health care, casinos, and securities need to be evaluated for the presence and impact of the Fraud Management Lifecycle. When these and other industries are evaluated for the presence of the Fraud Management Lifecycle, the intra-cycle interactions and their environmental impacts and constraints can be evaluated.

The adaptability of the lifecycle to diverse business and regulatory environments is worthy of continued analysis and evaluation. Further research of published material on each of the lifecycle stage activities, as well as fraud and fraud reduction activities, will provide an expanding base for application of the Fraud Management Lifecycle theory. In addition, continued research will likely identify additional opportunities for testing and validating the theory. The opportunity to implement the theory in practice and observe its applicability and performance through additional case studies would be a logical step in continued research of the Fraud Management Lifecycle. The opportunity to continue implementing the theory in practice will help to establish its relevance and validity in various industries.

By adopting the Fraud Management Lifecycle approach to fraud risk management, it is possible for businesses to obtain and maintain superior fraud loss performance. The lifecycle provides a methodology and structure that is easily adaptable to new fraud trends as they emerge. And emerge they will. The network of lifecycle stage interactions allows a business to continually evolve and enhance its fraud management activities. To paraphrase W. Edwards Deming in *Out of the Crisis*, (Deming,1986) continuous fraud management improvement is the most effective way to compete with continuously evolving fraud methods and tools. Ernst and Young in its survey, "Fraud The Unmanaged Risk," said it another way. "Fraud protection is an ongoing task, not a one-time fix it job that lasts for eternity" (Ernst & Young, 2000). Adopting a fraud management structure that can easily adapt to new challenges is the key to reducing fraud's negative impact on society. The following excerpts from the United States Secret Service testimony to the United States House of Representatives committee on Banking and Financial Services tells a vivid and true story reinforcing the importance of successfully preventing fraud.

> The United States Secret Service has seen the emergence of several international organized criminal groups systematically attacking the financial systems through financial institution fraud, counterfeiting of U.S. currency, credit card fraud, advance fee fraud, computer fraud, and telecommunications fraud. All of those violations are investigative program areas within the United States Secret Service, in which we have accumulated specific expertise and ongoing pro-active initiatives. While the sophistication and organizational levels of these groups increase in all areas of financial crimes, one of the most disturbing aspects the Secret Service has observed is the proliferation of the so called "white collar" criminal groups' involvement in the more violent types of criminal activities. The service believes it is a common myth that credit card fraud, bank fraud and the counterfeiting of U.S. currency are completely "white collar" criminal offenses with no relationship to the violence viewed on nightly news programs.

> Many people still believe that the majority of these "white collar" schemes are being perpetrated by individuals as an end in themselves. In fact, the Secret Service and other law enforcement investigators are constantly encountering organized criminal groups who are targeting U.S. and other nations' financial systems with a multitude of fraudulent schemes designed to support violent criminal lifestyles. The Secret Service has come to recognize the clear relationship between "white collar" crime and the perpetrators of inherently violent activities such as murder, drug trafficking, extortion, purchase and exchange of firearms and explosives, money laundering, alien smuggling, car theft, and prostitution. (Visa, USA Inc. 2000)

It is in this environment that the Fraud Management Lifecycle can provide direct value to the businesses that deploy it and derivative value to society as a whole.

About the Author

Wesley Wilhelm earned his Masters of Science in Economic Crime Management from Utica College. He earned his Bachelor of Arts in Economics and Political Science from the University of California and has completed graduate level course work in computer science and management information systems at Eastern Washington University. He is a graduate of the American Bankers Association National School of Bankcard management. He is a member of the International Association of Financial Crimes Investigators (IAFCI), the Association of Certified Fraud Examiners (ACFE), and the Pacific Northwest License, Tax, Fraud Association (PNWLTFA). Wilhelm is involved in co-teaching two courses in Utica College's Economic Crime Management program: Advanced Fraud Analysis and Risk Assessment and Mitigation. He has also taught and presented at both the IAFCI and PNWLTFA annual training seminars. Wilhelm has published articles on a variety of fraud issues in White-collar Crime Fighter, Cyber-crime Fighter, Card Technology, Electronic Payments International, Internet Retailer, and Card-Forum.

Wesley Wilhelm is a risk manager in strategic planning for Fair Isaac Company. He has over 24 years of experience in Banking, Software, and Risk Management and has been with Fair Isaac Company (formerly HNC Software) since 1997. At Fair Isaac he develops and customizes fraud detection systems that utilize neural network models and other advanced data analysis solutions. He specializes in banking and financial industry solutions including fraud detection, fraud operations, internal fraud, fraud organizational design, credit risk, and merchant and consumer transaction pattern models. As a recognized expert in fraud

prevention he frequently presents at national and international conferences and consults with governmental agencies regarding fraud management.

References

Australian National Training Authority. (1999). (PSP99) National Public Services Training Packages: Public Service Education Training Australia.

Deming, W. Edwards. (1986). Out of the Crisis. MIT Center for Advanced Engineering Study, Cambridge, MA.

Ernst and Young. (2000). Fraud, The Unmanaged Risk an International survey of the effect of fraud on businesses. 2000 International Survey Ernst and Young. www.E&Y.com.

Federal Bureau of Investigation. (2003). Insurance Fraud Video Text, http://www.FBI.Gov/hq/cid/fc/video_text/if_txt.htm downloaded 5/31/03.

Federal Bureau of Investigation. (2003). Bankruptcy Fraud Video Text, http://www.fbi.gov/hq/cid/fc/video_text/bf_txt.htm downloaded 5/31/03.

Jakubowski, Broce, Stone, and Conner. (2002). SAS 82's effects on fraud discovery.(Illuminating Fraud Detection Responsibility) (Statement on Auditing Standards): The CPA Journal, Feb 2002 v 72 i2 P42(5). New York State Society of Certified Public Accountants. Article # A83486543.

Mativat and Tremblay. (1997). Counterfeiting credit cards: displacement effects, suitable offenders and crime wave patterns: British Journal of Criminology, Spring 1997 v 37 n2 p 165(19) .

MacRae, Jeff. (2001). The Evolution of Insurance Fraud Detection: Claims, Sept 2001 v49 i9 p 51. Insurance Week, Inc. Article #A78542863.

Mena, Jesus (2002). Investigative Data Mining for Security and Criminal Detection, Butterworth-Heinemann.

The Nilson Report, (December, 2000) Credit Card Fraud Losses 1980 through 2000, Issue # 730 Oxnard, CA.

Prieston, Arthur J. and Dreyer, Jaqueline A., (2001) Mortgage Fraud, The Impact of Mortgage Fraud on Your Company's Bottom Line, Mortgage Bankers Association of America.

Samociuk, Martin and Iyer, Nigel (2003) Fraud Resistance, A Practical Guide, SIRCA 01-2003, Standards Australia International Limited ISBN 073375028 1

U.S. Department of Justice. (2002). Financial Institution Fraud and Failure Report, Fiscal Year 2002, Financial Institution Fraud Unit, Financial Crimes Section, Page 2.

U.S. Department of the Treasury, Office of the Comptroller of the Currency et. al.. (2003) Docket No. 03-18; Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Request for comment on page 6 and 15 U.S.C. 6805(b).

Visa, U.S.A. Inc. (October 2000). Resource Manual for Prosecutors and Investigators. VBS.10.01.00.

Webster's New Collegiate Dictionary (1997,1976, 1941).

Whatley, Everett. (1998). Card Security and Fraud Prevention Source Book. Faulkner and Gray. New York.