

Internal Fraud: Building the Business Case for Investment

A Financial Services Industry Briefing Paper

*The second in a series of papers on
internal fraud management
created by The Santa Fe Group
Vendor Council*

THE **SANTA FE** GROUP

A Publication of The Santa Fe Group Vendor Council

October 2007

Foreword

The Santa Fe Group Vendor Council created this paper for senior financial institution executives responsible for fraud prevention, loss management, corporate security and human resources. *This briefing paper is the second in a series created to educate senior financial services executives on the high-level business processes and technology solutions for addressing internal fraud.*

The Santa Fe Group Vendor Council promotes the development of secure, best-in-class technology solutions, standards, and improved business processes for the financial services industry and beyond. For more information about The Santa Fe Group Vendor Council, please contact Robin Slade, senior vice president, at 630-653-9340 or robin@santa-fe-group.com.

The Santa Fe Group is a strategic consulting company providing holistic risk management expertise to clients. Drawing from the most advanced thinking in the industry, access to business, technology and security experts, and a deep knowledge of regulatory and legislative issues, The Santa Fe Group brings outstanding results to its clients. For more information, visit us on the web at www.santa-fe-group.com or write to us at info@santa-fe-group.com.

Other papers by The Santa Fe Group Vendor Council:

Fraud in the ACH System: A Holistic Approach for Financial Institutions

Electronic Discovery 2007: A Primer for Financial Institutions

Internal Fraud: Surveying the Current Landscape

Table of Contents

| | |
|---|----|
| I. Introduction | 4 |
| II. The Problem of Internal Fraud: Background | 6 |
| III. Making the Case for Investment: The Context | 8 |
| IV. Value Drivers | 11 |
| V. Cost Drivers | 15 |
| VI. Measuring Ongoing Value | 16 |
| VII. Taking Action: Considerations for Achieving Approval | 19 |
| Appendix: Internal Fraud Case Study | 21 |
| Acknowledgments | 27 |

I. Introduction

A senior private banking manager at a top 10 global bank steals from client accounts by exploiting holes in the bank's IT controls. The theft is discovered three years after it began, when almost \$3 million has been embezzled. The bank is fined more than \$700,000 by local regulators for lax fraud detection and prevention controls.¹

Rogue employees can cause significant, lasting and even permanent damage to financial institution revenues, stock prices, reputations and even company survival. Every day, a few employees working in the financial services industry in a variety of roles — some seemingly “safe” or risk-free — violate policies and bypass controls to embezzle, collude and steal. Without appropriate mitigation, employees can commit fraud against your customers and your institution over a period of hours, days, months and even years.

Despite its potentially disastrous consequences, internal fraud is rarely talked about and difficult to quantify. What is known is that the impact of crimes committed by employees can be serious and lasting, and in the worst of situations can put the entire enterprise at risk. The incident above actually occurred in 2006, with devastating consequences for the financial institution. The story was publicized, damaging the trust essential to the institution in attracting and keeping its customers.

No financial institution is immune to the risk of internal fraud. Every organization needs to consider its risk, formally discussing it among upper management, fraud departments and legal counsel. Damages can just as easily occur at the hands of top executives as tellers or associates, making proactive planning and monitoring difficult.

We encourage readers to consider the real-life examples in this paper and ask themselves: Could this have happened at my institution? What systems do we have in place to detect internal fraud?

A vice president of a business unit at a top 25 U.S. financial institution created fictitious loans and transferred them into his personal bank account, exploiting weak controls and poor fraud monitoring systems. The company had no method of detecting the transactions and identifying them as possible fraud. The illicit activity went undetected for three years. An investigation revealed the executive embezzled more than \$40 million.²

Senior executives at a subsidiary of a top 100 U.S. financial institution colluded to commit loan fraud by subverting internal controls. The parent company had no means of monitoring the transactions of the subsidiary beyond static controls. When the fraud was discovered, the institution took a charge to its earnings of more than \$140 million and faced numerous costly lawsuits. The stock price plummeted more than 50% in the weeks following the announcement. The bank was ultimately acquired at a significant discount.³

A teller at a branch of a regional U.S. financial institution used the general ledger to create fraudulent transactions. The institution had no method of monitoring the transactions. The employee's activities went undetected by the bank for six years, during which time the teller stole more than \$3 million.⁴

A vendor set out to win the affection of an accounts payable clerk who handled his company's account at a large corporation. The vendor succeeded, and the clerk began charging various locations through journal entries for fictitious products. A manager saw an unusual charge and an investigation unraveled the case. Eight months passed before the illicit activity was stopped, representing a loss to the financial institution of \$1.2 million. Both the vendor and the clerk were prosecuted.⁵

A mortgage banker falsified loan documents by inflating incomes and issuing "straw" loans to individuals who were not the true recipients. A senior US District Court Judge sentenced him to 25 months in prison and ordered a \$50,000 fine upon his conviction on two counts of wire fraud. He was also ordered to pay \$190,000 in restitution to one of the mortgage lenders and FNMA for losses incurred as a result of the scheme.⁶

The Santa Fe Group Vendor Council created this paper to continue our conversation with the financial services industry on the growing risk of internal fraud. Our first paper provided an overview of the current internal fraud landscape. In this paper, we detail the serious risks involved when crime goes undetected inside a financial institution. We then provide a "how-to" for fraud managers to create a business case for investment in solutions to combat internal fraud.

This paper assumes what readers likely already know: Managers seeking support for investment in internal fraud solutions face substantial challenges because these investments do not create new revenues. Our premise is that a successful business case is built upon risk data and other supporting information that suits the institution's needs and sets the stage. To make a compelling case, we suggest creating a framework from which to assess value. Data collection and identification methods should be appropriate for the risks associated with your organization's unique structure, geographic region, size, workflow, product lines and services. The business case must also anticipate and address questions and challenges from a variety of stakeholders.

Fraud managers may use this paper to gain context on the internal fraud landscape, build their case, and anticipate roadblocks to gaining internal support. Ultimately, we hope this paper will be used to engage colleagues, stakeholders and company leadership, building awareness about the risk of internal fraud and gaining support for investment to mitigate that risk.

II. The Problem of Internal Fraud: Background

Internal fraud is a perennial, ongoing, and serious challenge for the financial services industry. According to one Federal Reserve Board study, more than 60% of bank fraud cases involve company employees.⁷ The 2006 *ACFE Report to the Nation on Occupational Fraud and Abuse* published by the Association of Certified Fraud Examiners (ACFE) found that the typical U.S. business loses 5% of its annual revenues to internal fraud, creating a total aggregate loss of \$625 billion annually. According to the ACFE report, the greatest proportion of internal fraud cases occurs inside financial institutions.⁸ These trends show no sign of slowing; internal fraud is instead likely to increase as fraudsters continue to be emboldened by new technologies, the Internet, and burgeoning markets for stolen information.

The evolving impact of internal fraud

The ACFE defines "occupational fraud" as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets." While once internal fraud at financial institutions meant primarily theft of cash, recent years have seen a surge of crimes involving theft of data, particularly customer data. Incidents range from retailers losing thousands of customer records (including confidential financial

data), to financial institutions losing records on customers (including personal and account data), to service providers losing similar customer and account records. Of the 148 financial institution internal fraud cases in the ACFE study, non-cash schemes made up 15.5% of cases, and the majority of those involved theft of proprietary information about financial institution customers.⁹ Data theft contributes to identity theft, and identity theft is a subset of identity fraud, which makes up a significant portion of businesses' total fraud losses.

A global challenge with local impact

Data availability, combined with the widespread use of the Internet, greatly raises the stakes. Criminal activity inside financial institutions extends far beyond material gain for the individual worker, beyond national borders even — since it feeds the activities of fraud rings and other criminal groups operating around the globe. Industry associations and trade bodies continue to raise awareness of organized criminals that attempt to gain employment at financial institutions for the express purpose of stealing data.

Globally, internal fraud is on the rise. According to KPMG Forensic's Fraud Barometer, in 2006 company managers in the UK were responsible for 40% of the nation's total frauds by value. Financial institutions were the second most common target for fraud by organized criminals, after the government. According to KPMG Forensic, criminal gangs are increasingly infiltrating financial institutions or coercing their staff to commit crimes against their employers.¹⁰ Though little hard data exists, similar trends have been found in Canada and Australia. One Australian study found that more than 50% of fraud against organizations was committed by employees.¹¹

Delayed response means greater losses

It takes a median length of 18 months before a company detects an internal fraud scheme.¹² Because of this time lag, financial institutions are often unable to recover funds. With data theft it is often impossible to know what data escaped and into whose hands it has fallen. The potential for loss, damaged reputations, and downstream identity theft is considerable.

Organizational complexities make mitigation harder

Fraud perpetrators can be full-time or part-time employees working inside the institution, or remote employees. Employees may be inherited through corporate merger or acquisition, or promoted from other departments. A fraudster may also be a contract or temporary worker, a supplier, or an individual operating from an outsourcer's location. All of these players expand the scope of the term "employee."

Other challenges compete for attention

Today's financial institutions must be alert to external fraud threats. They must also comply with complex and evolving laws and regulations — including anti-money laundering and “know your customer” requirements and Sarbanes-Oxley and USA PATRIOT Act provisions. These demands can make it difficult for managers to devote adequate time and resources to monitoring employees and looking for indicators of internal fraud.

III. Making the Case for Investment: The Context

Financial institutions are understandably reluctant to publicize information about internal fraud incidents. Even inside their own walls, internal fraud can be a sensitive topic. Thus, data about frequency and cost are scarce, and when they are available, they are often understated.

Statistics

There is much we do know about internal fraud, however. PricewaterhouseCoopers's 2003 and 2005 surveys on economic crime found:¹³

- The impact on company reputation, brand image, and staff morale can be as or more damaging than the direct financial loss.
- Companies with more employees are more likely to have suffered from economic crime.
- Forty percent of respondents suffered significant damage to the company's reputation and business relationships, as well as decreased staff motivation.
- More than one-third of internal fraud activity was discovered by accident, making “chance” the most common fraud detection tool.¹⁴
- Between 2003 and 2005, there was:
 - a 71% increase in the number of companies reporting cases of corruption and bribery
 - a 133% increase in the number reporting money laundering
 - a 140% increase in the number reporting financial misrepresentation
 - a 50% increase in the amount of assets lost as a result of internal fraud

Though one-third of respondents said that their company's board of directors had ultimate responsibility for preventing or managing internal fraud, just over one-quarter had provided risk management training to their board members.

According to the ACFE report, internal fraud perpetrators were:¹⁵

- In the accounting department in just over 30% of incidents
- Upper managers or executives in slightly more than 20% of incidents
- In the sales department in 14% of incidents

The study found that frauds committed by owners or executives were the most damaging, causing a median loss of \$1 million, an amount almost five times greater than the cost of frauds by managers, and almost 13 times the median loss caused by lower-level employees.

The ACFE report also found that small businesses suffer a disproportionate amount of fraud losses, in part because of an illusion of trustworthiness. The most common small-business internal frauds involve employees writing bad company checks, skimming revenues, and processing fraudulent invoices.

Employee issues

Internal fraud risk is not limited to financial losses and reputation damage. Secondary risks can be significant. Plummeting stock value is one example of a direct cost. Indirect costs can range from increased costs of attracting and retaining top talent to lost opportunities when the company is unable to execute a growth strategy following the loss of key managers.

Internal fraud can erode employee loyalty. Employees who witness crimes or become aware of internal fraud through rumors or the media may begin to question the company's integrity and leadership. This erosion of loyalty and respect can lead good employees to seek employment elsewhere, and unscrupulous ones to violate company policies and commit crimes themselves.

Employees who are disillusioned by the company, unhappy with its policies, or otherwise lack personal investment in the enterprise may be more likely to create and exploit gaps in the system for their own or others' use, or to take advantage of existing opportunities to commit fraud. Policy violations and code of conduct issues can be signs of larger problems. Activity that starts small can escalate, particularly if employees have the opportunity and motivation. If a crime is identified, financial institutions may want to consider whether colluders might be involved.

Employees who serve customers are expected to deliver high levels of customer satisfaction. Increasing competitiveness often means greater employee access to customer information — sometimes without increased monitoring of what they are doing with that information. Many times, staff and managers are not adequately informed about technology risk, leading to multiple databases, duplicate information, and weak information security. Employees may intentionally or unintentionally open doors that allow information to escape. Similarly, service providers may know more about your business and your customers than they should — also in the name of customer service. One employee's misuse of customer information is all it takes to create enormous losses and dangerous risks to your company's good name.

Regulatory challenges

Financial institutions face serious regulatory consequences for failing to adequately mitigate internal fraud. Relevant federal rules include:

- The Social Security Fraud Statute [42 U.S.C. 408(a)(7)(A)-(C) of 2001]
- Identity Theft Penalty Enhancement Act of 2002 (Aggravated Identity Theft Statute)
- Privacy Commission Act introduced 2002
- White Collar Crime Penalty Enhancement Act of 2002
- Corporate and Criminal Fraud Accountability Act of 2002
- Foreign Corrupt Practices Act
- USA PATRIOT Act
- Sarbanes-Oxley Act

At the time of this writing, federal examiners are treating internal fraud inconsistently. Regulatory agencies are aware of this problem and are working to make examinations more uniform. Until that time, financial institutions are left to speculate on what the regulators will expect, knowing that fines for failing to take “appropriate” measures can be severe.

In addition to federal rules, companies are also subject to state regulations. Those operating in multiple states must coordinate their policies according to varying requirements. A compliance officer can help you understand applicable state regulations.

IV. Value Drivers

If your goal is to convince your executive management to approve investment in an internal fraud monitoring system, you will need to justify the value of that investment to the company. How well you communicate that value will largely determine management's decision to fund your project. Management is skilled considering the merits of proposals like yours and will deny those that do not demonstrate value.

Different organizations require different metrics. However, most organizations require a clear articulation of the expected value of the investment's benefits and the costs involved. To do this, you'll need to translate qualitative concepts of benefit into quantitative dollar figures. Many successful proposals compare costs and benefits to arrive at a figure that indicates return on investment (ROI).

Investment in fraud mitigation will not generate revenue, so the value drivers of your business case are likely to be based on cost-savings logic. While the value drivers indicating hard dollar savings tend to be the most beneficial, less quantifiable drivers can also help build your case. Ideally, each driver should plant a seed in the reviewer's mind that contributes to the plan's ultimate approval. Your business case should also disclose all costs associated with the proposed investment. If costs are omitted, doubt may be cast on the viability of the entire proposal.

Value Drivers

1. Reduce fraud losses

Fraud loss reduction is usually the strongest of all value drivers. However, loss reduction figures can be difficult to obtain. A culture that encourages employees to be forthcoming in reporting suspicious activity can mitigate this challenge. If internal data is available, consider combining it with data from the industry to calculate hard dollar benefits.

An effective fraud monitoring solution will detect fraudulent activity earlier in the fraud event lifecycle. Many internal fraud incidents begin with a small dollar amount and escalate over time. Even if financial loss is not totally avoided, the impact of the fraud is likely to be less if it is caught early, and in some cases it may be prevented altogether. For example, unusual activity is often a precursor to fraud. If your institution is aware of the unusual activity, it can take action to avoid that particular fraud loss and reduce fraud losses overall. In this way, fraud monitoring actually reduces overall costs.

2. Detect more fraud

An effective fraud system will detect more incidences of fraud, some of which may have once been miscategorized as other operational expenses. Improved fraud detection can provide better insight into the profitability of lines of business by eliminating these miscategorizations. To avoid the perception that the fraud system is itself producing more fraud losses, be prepared to demonstrate how the system is working: it is bringing to light activity that previously went undetected.

In addition to finding more incidents of fraud, an effective fraud-detection solution will create associations among apparently disparate cases. The result is a broader view of fraud and a clearer picture from the criminal operator's level (as opposed to the transactional/fraud-incident level) by linking fraud events that otherwise would be pursued as separate cases.

3. Improve overall productivity

Most financial institutions maintain complex processes to monitor fraud. Checks and balances are built into operational processes to help assure institutions function in a way that is safe and secure. Each of these processes is associated with a cost that impacts your bottom line. With continued calibration and ongoing management, internal fraud mitigation technologies can reduce these costs overall by enabling analysts and investigators to access information quickly and effectively.

Consider these productivity questions as you build your business case:

- Can our existing fraud mitigation processes be reengineered to improve efficiency?
- How will automation reduce our manual fraud monitoring needs?
- Will the internal fraud solution facilitate our investigators' ability to retrieve pertinent information on specific cases? What is financial impact of early detection on fraud loss estimates?

Internal fraud monitoring systems have a secondary benefit: they provide an overall pattern of employee activity, allowing companies to compare employee behavior against a standard or among individuals. Workflow analysis can uncover poor operational design, inefficient work habits, risky behaviors, and process improvement opportunities.

Why is employee "Andi" faster and more accurate than employee "Brooke?" Is there a difference in the way Andi approaches her tasks? Or is Brooke better suited to a different role? Analytics like these can help set performance standards and provide true productivity metrics.

4. Mitigate reputation risk

A successful business case makes clear the potential of the proposed investment in internal fraud monitoring for decreasing the institution's exposure to reputation risks. In assessing this risk, consider these questions:

- **How do internal fraud losses affect market capitalization?** Fraud losses directly impact your company's bottom line, affecting its financial and stock performance. But damage can extend beyond financial performance. If a story about criminals operating inside your walls were to hit the front pages, what would happen to stock value? How would public perception affect the recommendations of industry analysts? Could it move an "outperform" rating to "hold," or a "hold" rating to "sell"?
- **Can an incident affect your institution's long-term strategic planning or execution?** Reputation damage can paralyze a company and affect long-term strategy in unforeseen ways. Management may have to abandon plans to merge, acquire, or be acquired, altering strategies critical to company evolution and growth. Reputation damage can also limit access to capital and delay plans to introduce new products or explore new growth markets.
- **Could a reputation incident spur customer attrition? What would be the revenue lost per customer?** Customers don't always complain. Instead, they just leave. Increasing evidence shows significant attrition rates for customers who lose faith and trust in their financial institution as a result of a negative experience. A 2005 study performed by a large U.S. financial institution found that when customers were affected by fraud on their deposit accounts, they closed their accounts at approximately three times the rate of accounts not impacted by fraud — even when the financial institution had made them whole. The study, which covered a 12-month period, also showed that customers react quickly: 75% closed their account relationship within three months of the fraud claim and 96% did so within six months. Your marketing or product management department can help you calculate the attrition rate for your organization and estimate lost revenue opportunity.
- **Could an incident threaten the institution's viability?** Occasionally, an internal fraud event is so serious it impacts a company's ability to continue independently. This occurred in 2007, when fraud at a financial institution subsidiary resulted in a significant charge to the parent's bottom line, resulting in decreased shareholder value and an auction.¹⁶

5. Enable regulatory compliance

Regulatory examiners change their emphasis periodically, increasing the importance of certain areas of financial institution operations. As internal fraud becomes more visible, examiners will be more interested in the actions companies are taking to monitor and suppress internal fraud. An initial employee screening process may not be enough. A fraud detection system can demonstrate a company's due diligence to examiners, helping to avoid possible fines.

As the Basel II Accord is accepted and implemented, operational risks are likely to have a larger influence on capital requirements. Internal fraud monitoring solutions can help financial institutions demonstrate their diligence and decrease their capital requirement calculation.

6. Retain key employees

A publicized internal fraud event affects employee morale. This is especially true if the incident generates public distrust of the institution. Valuable employees may seek employment at another financial institution, causing additional employee replacement expense, in addition to replacing the perpetrator(s). There can also be a general talent drain. Your HR department should be able to provide the cost to replace a valued employee; generally, the true cost of employee turnover can be calculated as one-and-a-half to four times the employee's annual salary.

7. Reduce other costs

An internal fraud monitoring system can help reduce or avoid:

- **Legal settlement costs.** An internal fraud event can cause significant legal expense, including court-ordered or out-of-court settlement costs. A class-action lawsuit could present an even greater financial burden. Your legal department can help you estimate these costs.
- **Financial restatement costs.** Could an internal fraud event cause the restatement of the institution's financials for the quarter or year? To use this cost in your business case, add it to the costs of potential effects on market capitalization (see #4 above on reputation risk).
- **Increased insurance rates.** An internal fraud monitoring system may help you to negotiate a better rate with insurance carriers, similar to homeowner's discounts for installing a home security system.
- **Operational costs for remediation.** When internal fraud results in a data breach, remediation can be expensive: closing and opening accounts, reissuing cards, increasing account monitoring and review, paying for customer credit monitoring services, and extending additional protection for customer data and accounts can all be costly. To estimate the cost, consider developing a figure for every 1,000 accounts closed or opened. Publicized data breach information could be used to estimate this cost.

V: Cost Drivers

An effective business case will identify all costs associated with the proposed investment. Remember that many stakeholders will review your investment proposal, each with his or her own perspective and expertise. If costs are omitted, doubt may be cast on the viability of the entire proposal.

Level One Analysis: What do today's efforts cost?

Knowing the cost of solutions already in place to thwart internal fraud can provide a benchmark, leaving you better prepared to argue for cost reductions. Establishing a reference point also helps to avoid double-counting costs: if you are already incurring costs for an activity required by your proposed solution, be sure to record only the incremental impact on that cost rather than the entire cost.

To be sure you are associating the appropriate costs with the appropriate benefits, ask yourself, "How will I generate this benefit?" Benefits rarely materialize without a proper accounting of the costs of delivering them, so be sure to account for all of the costs. This process addresses any unrecognized and unbudgeted costs associated with the project, which can result in project overruns that could hurt you on your next investment proposal.

Level Two Analysis: What are the development/acquisition, implementation and operational costs?

When your analysis of the cost of current solutions is complete, the cost of development (or acquisition), implementation, and ongoing operational costs must be examined. This Level Two analysis may consider:

- **Initial costs to develop or acquire the technology.** Technology costs are rarely restricted to software and maintenance. Be sure to account for the cost of acquiring the operating system, database management system, and other supporting software. Hardware acquisition for application and database servers or expansion of existing server capacity may also be included.
- **Costs to redesign internal processes and assign resources.** To ensure a new internal fraud monitoring system performs optimally, your organization will probably need to make some adjustments to its operating environment. Be sure your business case accounts for the effort and expense associated with evaluating and adjusting the operating environment.
- **Operational costs of managing and supporting the technology.** Also consider the cost of installing the system and its daily operation. For example, if you add two new servers, there will be a monthly cost of operating them and application and end-user support costs. You'll also need disaster recovery and backup plans.

VI: Measuring Ongoing Value

The primary goal of implementing an internal fraud monitoring solution is to detect more fraud; ultimately the goal is to reduce losses associated with internal fraud. The companion goal is to manage this process cost effectively. A successful business case describes a method for measuring the fraud solution's performance and tracking overall ROI. A more efficient monitoring system can help identify fraud schemes while they are still immature, allowing the institution to reduce associated losses or prevent them altogether.

The metrics below can be used to evaluate the effectiveness of your fraud detection and prevention solution:

1. Number of alerts produced per actionable incident

The total number of alerts as a standalone number is not meaningful as a metric, as it will include false positives. False positives can be the bane of fraud prevention units. An increase in alerts does not necessarily mean an increase in frauds identified. Instead, an increase in alerts could mean that the system needs to be calibrated to eliminate alerts on acceptable behavior. It is as important to know what you don't want to alert as it is to know what you do want to alert. Excessive false positives can result in the need to invest in more analysts/investigators, and/or leave a significant portion of those alerts uninvestigated for long periods of time (if they are investigated at all) due to a lack of investigative resources.

A good metric that addresses this efficiency issue is the number of alerts produced per actionable incident. An actionable incident is one that results in an investigation, discovery or prevention of a fraudulent act, supervisor or management consultation with an employee, or other action taken as the result of the alert. An effective and well-managed system will show a low alert per actionable item ratio.

2. Number of fraud incidents

A subset of the actionable incidents described above, the absolute number of fraud incidents resulting from the fraud-detection solution and the ensuing investigation provide a tangible metric by which to measure the solution's success. In the shorter term, an effective fraud solution should increase the number of fraud incidents investigated. (These are incidents that previously would have gone undetected.)

3. Average duration of fraud schemes

The average time between an employee's initial act of fraud and the time that the fraud is discovered and investigated is an indicator of how effective the fraud solution is at catching fraud — and can potentially proxy for the avoidance of higher fraud losses. Since internal fraud schemes often start small and escalate over time, detecting incidents earlier in the cycle reduces the number of higher-impact losses. Average duration of fraud schemes can be benchmarked early in the solution's deployment, with the expectation that it will decrease over time.

4. Dollar amount of fraud losses

The total dollar amount of fraud losses is a complicated metric to measure. Fraud often goes undetected and fraud losses are frequently miscategorized, so a successful solution will increase known losses by improving detection. Over time, detecting fraud earlier will probably result in a lower average loss per fraud incident and lower total fraud losses. These opposing forces can be difficult to reconcile.

Average fraud loss per fraud incident, on the other hand, can be more useful in evaluating fraud detection. An effective solution will lower this number over time.

5. Loss avoidance

Loss avoidance can be tricky to estimate since it requires speculation: What damage would the institution have suffered if scheme X had not been stopped? Loss avoidance per dollar spent on fraud detection is also an effective metric because it can clearly indicate the value of the fraud detection/prevention system.

6. Cases investigated over time

The number of cases investigated over time can clearly demonstrate success. More cases are generated initially, as previously undetected fraud is caught. At the same time, associations are being made among disparate alerts. The result is a broader view of fraud and a clearer picture at the criminal operator's level (as opposed to the transactional/fraud incident level), by linking fraud events that otherwise would be pursued as separate cases.

But cases investigated over time can also bring the monitoring system's necessity into question. While fraud cases increase initially, fewer are produced over time. Additionally, if the system is successful in identifying precursor behavior and preventing the fraudulent act, technically there is no case or loss. Documenting these "saves" as faithfully as losses can help demonstrate the system's necessity through evidence of its efficiency and deterrent effect.

Metrics over time can help justify continued funding for your program and its resources. Measuring what you've learned and how you developed your program based on data and indicators of gaps and successes can go a long way in keeping stakeholders invested.

7. Average number of cases managed per investigator

This number indicates the solution's effectiveness in boosting investigator productivity. This metric will vary depending on the job responsibilities of the individual. Some banks have an analyst identify actionable incidents and refer them to an investigator or a supervisor for action, while others have the individual confirm the fraud or other unacceptable behavior, complete an investigation, and refer the case to management for action. Be clear what you are measuring in order to understand what the metric means. If your analysts are doing full investigations, there will be more affecting their productivity than just the monitoring system. If you want to measure their efficiency in regard to the detection aspect, then record the total number of alerts they work.

8. "Total cost of ownership" (Loss avoidance per dollar spent)

Fraud detection is a major undertaking. Companies must invest significant resources to be successful. These resources (outlined in Section V) include:

- Initial costs to develop or acquire fraud solution technologies
- Costs to redesign internal processes and assign resources appropriate for fraud solutions
- Ongoing operational costs of managing and supporting fraud technologies, including:
 - Investigators/analysts
 - IT staff time for ongoing data management
 - Internal hardware, such as servers and use of mainframes

Financial institutions may want to incorporate some measure of "total cost of ownership" into cost evaluations of internal fraud monitoring solutions. Loss avoidance per dollar spent divides the total annual loss avoidance by the annual costs. If a solution is detecting large amounts of fraud and preventing significant losses, it has justified the resources used to maintain it. (See #5 in this section on measuring loss avoidance.)

VII. *Taking Action: Considerations for Achieving Approval*

How you present and communicate your business case may be as important as what it says. Approval processes usually involve several stages. Expect to be asked to present your business case to multiple audiences. To be successful, you'll need to be aware of the organizational context, including other projects or corporate initiatives against which your investment proposal may be directly (or indirectly) competing. Identify the relevant stakeholders within each audience and frame the business case appropriately for them.

Competing for scarce funds

Today's business landscape is fiercely competitive, and globalization has only intensified the competition. Realize that you may be competing against your colleagues for funds. Therefore, it makes sense to assess your internal environment. Fraud managers must not only build a quantitative business case that supports the investment, they also will want to align their project proposal with the strategic initiatives of senior management. A constantly changing business climate and shifting priorities require regular assessment and reassessment of your internal environment. For example, even though internal fraud results in significant amounts of hard dollar losses each year, a key selling point might be the protection of customer data and the resulting protection of the bank's reputation.

Identify stakeholders and seek backing

Stakeholders include personnel who will help produce the result, as well as those who will be affected by the solution's effect on fraud. Put yourself in each stakeholder's shoes and ask: "What's in it for me?" Determine the appropriate messaging for each audience, anticipate reactions and objections, and prepare appropriate responses. Each stakeholder in the process will have his or her own concerns, including the potential budgetary impact of your proposal.

As you consider stakeholders, identify which will be likely allies and champions of your proposal. It may be wise to seek the backing of an executive sponsor. An executive sponsor should understand the value of the investment you're proposing and be able to articulate it at the executive level. Seek backing prior to the meeting and pre-qualify approvers. If possible, be confident of the outcome before you enter the room.

Develop an approach for internal messaging

Effective communication is in large part driven by your audience. Each audience will be different and you will need to vary the focus and emphasis of your message (for example, a line of business may have very different priorities than the general auditor). Some audience members will need to be communicated with on different timetables. Some will need more education than others. An effective presentation will address each constituent's concerns, and the most successful will make everyone feel as comfortable as possible with the proposal.

Gaining approval for an investment in internal fraud detection and prevention will remain a challenge for some time. But with a solid business case, a well thought-out presentation of that case, and a clear understanding of how the case supports corporate objectives, fraud managers can be successful in advocating for investments that protect their institutions against the very real threat of internal fraud.

Appendix: ABC Bank Case Study

Building an Internal Fraud Business Case

Rebecca Hawes, Senior Manager of Loss Prevention at ABC Bank, stared out of her office window and contemplated the best way to convince executive management to invest in technology to battle internal fraud. Earlier that same day, George Mendoza, VP of Risk Management, lamented the company's tight budgets. He indicated that ABC's CFO was even more reluctant to devote resources to non-revenue generating projects. Rebecca knew she faced an uphill battle since ABC already had rudimentary fraud management policies and procedures in place. However, she knew that implementing the right fraud detection system could actually improve the bottom line and positively impact share price.

ABC Bank had recently acquired several smaller institutions, forming a top 30 U.S. bank with \$60 billion in assets and 15,000 employees. They had inherited a group of employees that they did not really know. On the heels of an IT systems conversion, Rebecca believed ABC had lost the ability to effectively detect and investigate employee fraud. Management thought internal fraud might be a problem, but did not seem to grasp the size of the problem nor its cost to the bank. Lacking headline-grabbing fraud incidents involving ABC employees, the bank's executives were simply not losing sleep over internal fraud.

Rebecca oversaw a team of 16 fraud analysts, four of which were dedicated to monitoring for incidents of employee fraud. Through a largely manual process, these analysts reviewed thousands of potentially suspicious transactions annually. During the previous year, they had forwarded 350 cases of inappropriate employee activity to field investigators. ABC's internal fraud analysts had repeatedly expressed frustration with the review process. They had to manage data from siloed systems with little historical transactional data, limiting their ability to find cases of fraud. Rebecca spoke with the head of corporate security and learned that whistleblowers reported an additional 140 cases directly to the investigative team, and branch managers found 280 cases by accident. Rebecca suspected that a sizeable number of internal fraud cases probably had escaped detection.

Rebecca needed to persuade ABC's executive management of the value of investing in technology to mitigate internal fraud. She had gathered compelling statistics, high-profile examples, and anecdotes, but knew she had to lay out a tactical business case, one that clearly outlined the costs, benefits and return on investment (ROI).

The primary value driver for a fraud detection investment, and indeed the fundamental reason for such an investment, is to detect more fraud. Undetected fraud will continue to grow, so catching it early in the cycle is critical. After collecting data from her fraud analysts and ABC's accounting department, Rebecca mapped the distribution of fraud cases by total losses experienced. She categorized fraud cases into four groups:

- Small: \$500 average fraud loss per case (55% of cases)
- Medium: \$5,000 average fraud loss per case (38% of cases)
- Large: \$30,000 average fraud loss per case (6% of cases)
- Extremely Large: \$90,000 average fraud loss per case (1% of cases)

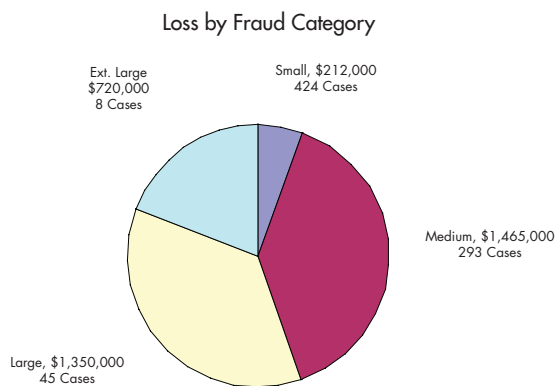


Figure 1. Current fraud cases segregated by fraud loss. Total fraud loss = \$3,747,000. While large and extra-large account for 7% of the total number of cases, together they represent more than half of total fraud losses.

After analyzing the data, Rebecca knew that if her team had been able to find more of the cases earlier on, or if they had been prevented altogether by identifying suspicious activity before the fraud was actually perpetrated, they would have reduced ABC Bank's financial losses. Fraud detection technology could help her analysts detect unusual activity associated with incidents of internal fraud much earlier in the cycle, which would migrate the distribution toward lower-impact fraud cases or prevent them altogether. Rebecca spoke with a few of her peers at other banks and made some assumptions about which cases could have been detected earlier in the fraud cycle or prevented. This allowed her to project the distribution of fraud cases by fraud loss that ABC could expect if it invested in a fraud detection technology. She found that 158 of the 770 cases could have been detected as policy violations before any loss had been incurred at ABC, and that many of the larger fraud loss cases could have been caught much sooner in the process, moving those cases to the "small" category.

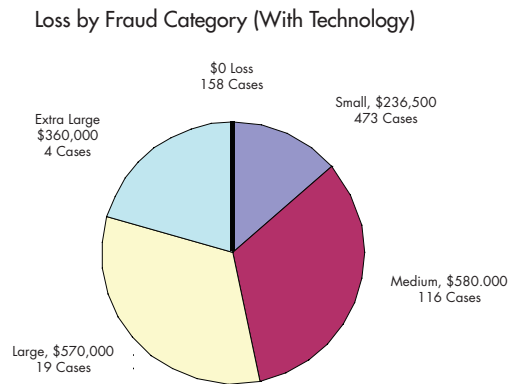


Figure 2. Fraud loss projection with technology implemented. Catching fraud earlier migrates distribution toward lower impact. Total fraud loss = \$1,746,500.

Rebecca estimated that with an investment in fraud detection technology would reduce annual fraud loss to about \$1.75MM per year, resulting in savings of \$2MM.

Using manual processes, the fraud analysts were able to identify 350 incidents during the first six months of the year. Anti-fraud technology would enable ABC to automate many processes, and the investigators could become more productive. Rebecca felt they could potentially identify all 770 internal fraud cases; as well as additional cases that would otherwise remain undetected. She calculated a value for this efficiency using a fully loaded annual cost of \$85,000 for each fraud analyst.¹⁷

| Improvement in Productivity | Current | With Investment |
|---|----------------|------------------------|
| Number of employee fraud cases identified: | 350 | 770 |
| Number of internal fraud analysts (FTE): | 4 | 4 |
| Fully loaded cost per analyst: | \$85,000 | \$85,000 |
| Resource cost per fraud case: | \$971 | \$442 |
| Cost to investigate 770 cases | \$748,000 | \$340,000 |
| Value from fraud detection investment: | | \$408,000 |

Table 1. Value of increased productivity gained with use of fraud technology.

In the past, ABC had incurred operational costs for managing identity theft and account takeover situations. ABC's accounting department provided data for Rebecca about these costs, broken out by account, which included on average \$10 for outbound letters, \$5 in outbound telemarketing, \$72 for one year of credit monitoring services, \$10 for legal and public relations costs, and \$50 in lost revenue due to customer churn (\$2,500 average lifetime revenue per customer * 2% churn rate). The total cost on average to manage these incidents was about \$147 per at-risk account. Rebecca reconciled these costs against those provided by an insurance underwriter that provides an online calculator estimating the costs associated with data breaches and identity theft.

In the previous year, ABC had caught 5 employees stealing account information. These employees had accessed about 20 accounts each day, which translates to about 25,000 at-risk accounts per year. By catching employee fraud earlier in the cycle, Rebecca estimated that the at-risk accounts could be lowered by as much as 30%. Using the figures from the accounting department, Rebecca computed the value of a decrease in at-risk accounts.

| Reduction in Operational Costs | Current | With Investment |
|--|----------------|------------------------|
| Number of customers at risk annually: | 25,000 | 17,500 |
| Operational cost per customer: | \$147 | \$147 |
| Total operational cost of post-fraud management: \$3,675,000 | | \$2,572,500 |
| Value from fraud detection investment: | | \$1,102,500 |

Table 2. Estimated value of decrease in at-risk accounts resulting from fraud technology.

The last value component Rebecca considered was the potential cost associated with a high-impact, headline-grabbing internal fraud event. Difficult to quantify, the costs associated with reputation damage include erosion of share price, loss of customer confidence and trust, and general damage to the bank's brand. Rebecca had seen disastrous consequences result from internal fraud at other banks, and knew that the intangible cost of insurance against such consequences could only bolster her tactical business case.

With a solid understanding of the value to be expected from an investment in internal fraud detection technology, Rebecca figured the total annual business value.

| Fraud Detection Investment: Value Drivers | |
|--|--------------------|
| Catching more incidences of fraud earlier: | \$2,000,500 |
| Improving productivity of fraud investigators: | \$408,000 |
| Reduce post-fraud operating costs: | \$1,102,500 |
| Decrease reputation risk: | ? |
| Total Annual Business Value | \$3,511,000 |

Table 3. Total estimated business value of investment in internal fraud technology excluding reputation risk.

Rebecca's next step was to analyze the incremental cost of investing in this technology and compare it to the incremental benefits. She outlined ABC Bank's current costs of managing internal fraud, including investigators, server usage, and other basic technology. Rebecca evaluated several technology vendors as well as the cost to develop technology internally. She selected one vendor that was the best fit for ABC Bank. She also determined that ABC would need to dedicate IT resources to the implementation and integration of the fraud detection system, as well as personnel to manage the systems internally and hardware to support it. The total costs of the vendor and the internal resources added up to \$1,000,000 in the first year (including initial implementation costs), and \$600,000 for each year thereafter.

Rebecca pulled the benefits and costs together to calculate the ROI for fraud detection technology. She used the bank's cost of capital of 15% with a three-year timeframe to reflect the likelihood of reinvestment in several years, and calculated a net present value of \$2.92 million dollars, excluding the value of the protection against reputation damages that the investment could provide.

| ROI Calculation | Year 1 | Year 2 | Year 3 |
|----------------------------|--------------------|---------------|---------------|
| Incremental business value | \$3,511,000 | \$3,511,000 | \$3,511,000 |
| Cost of technology | (\$1,000,000) | (\$600,000) | (\$600,000) |
| Free Cash Flows | \$2,511,000 | \$2,911,000 | \$2,911,000 |
| Net Present Value | \$6,298,642 | | |

Table 4. ROI calculation to arrive at net present value.

Rebecca felt that her business case and cost-benefit analysis were very compelling. She had assembled an impressive set of statistics, industry data, and anecdotes about high-profile fraud incidents at other banks in order to properly frame her business case. Rebecca had carefully evaluated the value that such an investment would deliver to ABC bank, quantifying the monetary impact of the benefits on ABC Bank's bottom line. She had also meticulously assessed the costs with a fraud technology investment, including both the cost of the technology itself and the associated internal costs that would arise due to this investment.

Armed with a clear business case supporting an investment in fraud detection technology, Rebecca requested a chance to present her case to George and ABC's other risk and compliance executives. Rebecca was confident that the rationale supporting this investment was both comprehensive and logical. She was also certain that ABC Bank would increase its bottom line and ultimately its share price by moving to the forefront of customer and bank asset protection.

- ¹ “Paribas fined £350,000 over fraud,” BBC News, May 10, 2007, <http://news.bbc.co.uk/1/hi/business/6641831.stm>
- ² “KeyBank SVP Arrested in Alleged \$40 Million Embezzlement,” BankersOnline.com, November 15, 2006, http://www.bankersonline.com/security/jsb_keybankembezzlement.html
- ³ “Sterling Financial Despoiled by Fraud,” The Philadelphia Enquirer, May 25, 2007, http://www.philly.com/inquirer/business/20070525_Sterling_Financial_despoiled_by_fraud.html
- ⁴ “Employee Accused of Stealing 3.2M from Seminole BancFirst,” The (Oklahoma City) Journal Record, February 19, 2007, http://findarticles.com/p/articles/mi_qn4182/is_20070219/ai_n18624310
- ⁵ “Employee Theft: 10 Hot Areas for Review,” J. Patrick Murphy, LPT Security Consulting, August 28, 2007, <http://www.lptoday.com/consulting/employeetheft.htm?gclid=COinqpPUlo4CFRl14gAodmGmAPA>
- ⁶ “Alaska Mortgage Banker Sentenced to 25 Months in Prison,” National Mortgage News, James Comtois, September 12, 2007 <http://www.nationalmortgagenews.com/fraud/stories/?storyid=20070911a.htm>
- ⁷ “Financial Fraud - Biometrics Point a Finger,” Celent, March 2002, <http://www.celent.com/reports/Biometrics/Biometrics.pdf>
- ⁸ 2006 ACFE Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2006, <http://www.acfe.com/documents/2006-rttn.pdf>
- ⁹ 2006 ACFE Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2006
- ¹⁰ “Boom in Organized Crime Takes Fraud Cases to Record Levels,” KPMG Forensic Fraud Barometer, January 29, 2007 (press release)
- ¹¹ “The Changing Nature of Fraud in Australia,” Office of Strategic Crime Assessments, Commonwealth of Australia, 2000
- ¹² 2006 ACFE Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2006
- ¹³ “Economic Crime Survey 2003,” PricewaterhouseCoopers, http://www.acfe.com/documents/2003_PwC_CrimeReport.pdf and http://www.pwc.com/gx/eng/cfr/gecs/PwC_2005_global_crimesurvey.pdf
- ¹⁴ “Global Crime Survey 2005”, PricewaterhouseCoopers, http://www.pwc.com/gx/eng/cfr/gecs/PwC_2005_global_crimesurvey.pdf
- ¹⁵ 2006 ACFE Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2006, <http://www.acfe.com/documents/2006-rttn.pdf>
- ¹⁶ See section I.
- ¹⁷ “Fully loaded” cost includes salary and all benefits provided by ABC Bank.

Acknowledgments

The Santa Fe Group Vendor Council would like to acknowledge and thank the project group Chair, Mike Williams, Memento Inc., for his leadership and active participation in developing this white paper. In addition, we would like to recognize the following individuals who made important contributions to this paper:

Michelle Thiel & Kristine Regele, ChoicePoint

ChoicePoint provides businesses, government agencies and non-profit organizations with technology, software, information and marketing services to help aid Identity Risk Management (IRM) as well as the management of economic and physical risks.

Mike Mulholand, Metavante

Metavante Corporation delivers banking and payments technologies to financial services firms and businesses worldwide, with products and services that drive account processing for deposit, loan and trust systems, image-based and conventional check processing, electronic funds transfer, consumer healthcare payments, electronic presentment and payment, and business transformation services.

Doug Kohen, Memento

Memento, Inc.’s flagship software product, Memento Security, enables financial institutions to proactively monitor, detect, and investigate inappropriate activities—from trusted insiders to criminal outsiders—across the enterprise.

Additionally, the Vendor Council thanks **Robert Jones of RW Jones Associates** and **Peter J. Baldassaro of INC Consulting Ltd.** for their contributions.