

Internal Fraud: Surveying the Current Landscape
A Financial Services Industry Briefing Paper

*The first 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

March 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 first in a series to educate senior financial services executives on the high-level business processes and technology solutions for addressing internal fraud.

While insider fraud involves serious compliance issues, this paper focuses on the business problems associated with internal fraud. The paper describes internal fraud issues facing financial institutions and makes common-sense recommendations—hiring considerations, cultural issues, and technological solutions—drawn from the expertise of Santa Fe Group Vendor Council members.

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. The Santa Fe Group is a strategic partner and preferred provider to BITS, the nation's foremost authority on technology and financial services. For more information, visit us on the web at www.santa-fe-group.com or write to us at info@santa-fe-group.com.

I. The Problem of Internal Fraud: An Overview

Internal fraud is a perennial, ongoing, and serious challenge for the financial services industry. 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 report, the greatest proportion of internal fraud cases occurs inside financial institutions.¹

Internal fraud is likely to increase as fraudsters continue to be emboldened by new technologies, the Internet, and burgeoning markets for information. This white paper begins to define some of the steps financial institutions can take to address the challenges of internal fraud. Future white papers by The Santa Fe Group will continue to explore the problem of internal fraud and identify relevant solutions.

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 an explosion of internal fraud involving theft of data, particularly customer data. Of the 148 financial institution insider 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.²

A global challenge with local impact

Data availability, combined with the ubiquity of the Internet, greatly elevates the stakes involved in insider fraud. Criminal activity occurring 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 crime groups that attempt to gain employment at financial institutions for the sole 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 percent of the nation's total frauds by value, about £350 million. 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 in the UK to commit criminal activity against the financial institution.³ Though little hard data exists, similar trends have been noted in Canada and Australia. One Australian study found that more than 50 percent of fraud against organizations was committed by employees.⁴

Delayed response means greater losses

It takes a median length of 18 months before a company detects an internal fraud scheme.⁵ Because of the time lag between the start of an employee's illicit activity and its detection, financial institutions are often unable to recover funds. With data theft, it's difficult to know what data escaped and into whose hands it has fallen. Though costs to financial institutions from insider fraud aren't made public, the potential for loss, damaged reputations, and downstream identity theft is clearly enormous.

Complex organizations make mitigation harder

Organizational complexities can make sources of internal fraud more difficult to identify. While some fraud perpetrators are full-time employees working inside the institution, others are employees inherited through corporate merger or acquisition, or individuals promoted from other departments. A fraudster may also be a contract or temporary worker, a supplier, a remote or part-time employee, or an individual operating from an outsourcer's location.

Other challenges compete for attention

Today's financial institutions must pay attention to external fraud threats. They must also comply with complex new laws and regulations—including anti-money laundering and “know your customer” requirements, as well as 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 identifying internal fraud.

Staying competitive means information access

Financial institutions must stay competitive. Employees are expected to provide higher levels of customer satisfaction. Increasing competitiveness often means greater employee access to customer information—often without increased monitoring of what the employees are doing with that information. Most staff and managers are not adequately informed about technology risk,

leading to too many databases, duplicated information, and weak information security. As a result, employees end up creating more ways for the information to exit an organization. More and more external resources know more about your business and your customers than they should—all in the name of customer service.

The market for information is hot. One employee misusing customer information is all it takes to create enormous losses and dangerous risks to your company's good name.

II: A Closer Look

Internal fraud is diverse and wide ranging

Internal fraud at financial institutions spans a wide range of activities. A sampling of recently publicized cases illustrates the diverse nature of internal fraud:

- A scheme in which criminals operating inside 10 major US financial institutions stole personal data from as many as 500,000 customer accounts and then sold the information to a middleman
- Embezzlement of more than \$800,000 by a head bank bookkeeper
- A teller's conspiracy with a local business to fraudulently approve 245 rejected auto loans
- False accounts created by a financial institution manager for fictitious customers
- A human resources manager who sold employee data to an outside agent
- Bribery of a financial institution employee who then siphoned money from the accounts of elderly customers into accounts controlled by criminals
- Concealing trading losses

Common categories and motivations

Insider fraud schemes generally fall into three major categories. With the exception of teller fraud, all of these are associated with back-office processes:

- Stealing money from the financial institution—Taking cash or negotiable instruments, stealing equipment, taking bribes or kickbacks
- Stealing money from customers—Taking funds from customer accounts
- Stealing proprietary data—Stealing data, such as customer information, competitive data, and other sensitive information

Exposure to employee fraud can be divided into the following themes and motivations:

- Placement and re-employment. Companies must be vigilant to avoid employing a person who has previously been dismissed for fraud at another company.
- Duress, grooming, entrapment, and employee compromise. Organized criminals are targeting

financial institution employees, asking them to use their position to facilitate crimes.

- Collusion. Employees who cooperate with organized criminals, or who have associations and connections with them, may supply criminals with information to perpetrate a fraud.
- Addiction to drugs, alcohol or gambling. Employees may be compromised or commit defalcation to support an addiction.
- Employee grievances. Employees may be motivated to commit fraud if they feel they have been affected adversely by mergers and acquisitions, overlooked for a promotion, discriminated against, or unfairly compensated under a remuneration and bonus plan. An employee may see a cultural or ethical disagreement with the institution's corporate plan as justification for committing fraud.

Technology challenges: Legacy systems and competing technologies

While financial institutions see the need for proactive and sophisticated action, technology challenges often create significant barriers to fighting internal fraud. A combination of legacy mainframe computer systems, myriad business technology applications, and ever-evolving business processes create:

- Massive amounts of data
- Inconsistency of information and log files between applications
- Data that is semi-structured of variable length
- Variation in the availability of source data

Solution providers follow the lead of financial institutions. With internal fraud on the rise, technology companies are developing products that take these challenges into account and enable financial institutions to better manage and mitigate internal fraud and its associated losses.

III: A Holistic Approach to Managing Internal Fraud

Because internal fraud schemes are varied and always evolving, financial institutions must rely on technical and nontechnical solutions to identify and mitigate fraud. Broad categories of solutions include hiring practices, employee training, corporate policies, employee supervision, auditing, behavior sampling, balancing controls and checks, dual control, video surveillance and access controls.

Successful internal fraud management includes:

1. Intervening effectively

Companies that want to combat internal fraud need a solid intervention plan. Financial institutions must recognize the extent of internal fraud threats and their need for a unified approach that combines human resources, training, and corporate culture partnered with intelligence-based technology and tools.

2. Screen employees carefully

Financial institutions' first and best opportunity to mitigate internal fraud is to prevent employees who are a fraud risk from entering their institutions. The application and screening process is an opportunity to gather information and identify tendencies toward illicit behavior, such as fiscal irresponsibility, addictions and criminal and civil records.

A new database launched in 2006 is helping financial institution human resources personnel identify applicants who have been fired for committing fraud at other financial institution. The Internal Fraud Prevention Database, managed by Early Warning Services, LLC, follows the lead of the retail industry, which has been using ChoicePoint's Esteem® database since 1995. More than 75,000 retail locations nationwide use Esteem to screen potential employees and more than 30 million inquiries have been processed against it. Hit rates range from 1 to 4%, with an overall average of around 1.7%. In 2006, more than 15 million inquiries were processed through Esteem, with an average monthly hit rate of 1.72%.

3. Raise fraud awareness through training and culture

New hires should be trained on specific fraud detection responsibilities when they begin work in a new position and on a regular, ongoing basis. Additionally, general fraud awareness training should be mandatory at all levels at employment as well as periodically.

Employees should be encouraged to be vigilant and recognize the risk of entrapment or compromise by criminals. Employers have a duty to assess staff risk and assess threats based on employee risk and role.

Maintaining open lines of communication between managers and their staff is the linchpin of a culture of responsibility and accountability. An internal fraud hotline can help employees be responsible without negative consequences. When employees at all levels are enlisted to be responsible and accountable, insider fraud is less likely to occur and is more likely to be discovered when it does happen.

4. Use internal surveillance and monitoring tools

Technology allows financial institutions to review staff activity and identify individuals for closer manual scrutiny. Monitoring tools identify customers and accounts that are at risk for compromise while employees are investigated. This approach allows the institution to act swiftly if fraudulent behavior is detected, before a theft occurs.

IV: Integrated Systems and Processes Fight Internal Fraud

Internal fraud monitoring and detection

Two broad levels of monitoring and detecting are available to mitigate internal fraud and related losses:

1. An employee's general behavior and adherence to policies and procedures, and the system access and functionality permissions granted to the person to perform his or her job
2. An employee's daily activities, including the transactions the individual generates, and the systems and functions he or she accesses

Today's technologies allow businesses to:

1. Identify suspicious behavior. Internal fraud management technologies can monitor for suspicious employee activity and detect anomalous behavior worthy of investigation. A fraud analyst can determine if the behavior is fraud or a likely precursor.

The analytics used to identify unusual behavior must be flexible and adjustable by the user to account for the dynamic nature of fraud schemes. Thresholds and other parameters may vary by group or job code.

Automated monitoring includes tracking and retaining all computer and telephone activity by any employee accessing corporate systems and external Internet sites or email, including outside email.

Typical monitored activities include:

- Online transactions (monetary and non-monetary) and inquiries
- The date, time and source of online access (especially if the system can be accessed from a WAN or the Internet)
- Report generation and downloading, including operational and custom reports or queries, especially those containing customer or account information
- Cell/camera phone and flash drive use as compared with company policies and guidelines, including area restrictions
- Accessing of company and external websites by the employee
- E-mails sent and received and attachment sizes
- Telephone use, including use of restricted phone numbers

2. Control system access

Companies may structure their permissions to allow system and function access appropriate to an employee's duties. Technologies can help to identify when an employee's access falls outside his or her responsibility.

3. Implement strong information security practices

Financial institutions can capitalize on resources traditionally used for data security management, such as:

- Internal firewalls that restrict employee access to certain parts of the company LAN
- System logon requirements after a set period of computer inactivity
- Strong passwords (minimum length, upper/lower case combinations, alphanumeric combinations) that expire automatically
- Enforcement of "clean workstation" rules to limit theft of physical information

4. Enable technology solutions

Technology empowers companies to address the high-level business requirements necessary to fight internal fraud, including:

- Data management, which aggregates transaction and reference data sources
- Fraud scenario management, which enables fraud teams to create and modify behavior profiles
- Investigations management, which allows efficient and effective forensic research and analysis
- Reporting, which presents insider fraud leads in a clear format for internal review and follow-up

Internal fraud management solutions should monitor proactively for suspicious employee activities and detect patterns of behavior worthy of investigation. A fraud analyst can then determine if the employee's behavior is fraud or a precursor to it. A few examples of behavior worthy of investigation include:

- A teller performing an excessive volume of account balance inquiries over lunchtime without any intervening monetary transactions
- A branch manager making debits against a miscellaneous fee rebate general ledger account without corresponding credits
- A call center representative changing a customer's address, ordering a new debit card, requesting a new PIN, and restoring the address back to the original
- A senior teller making early (pre-maturity) withdrawals from time deposit accounts (CDs, IRAs, etc.) and waiving the penalties

Pattern analysis and monitoring can help detect when an employee's behavior is outside the expected range. Behavior may be compared to:

- The employee's historical activity
- Model activity appropriate to the employee's job responsibilities
- A "model" employee's activity
- The average activity of a group of employees with the same job responsibilities

The rules used to identify unusual behavior must be flexible and modifiable by the user to adjust for the dynamic nature of fraud schemes. Various thresholds and other parameters are needed, which may vary by group. Deviations from the norm can be defined as percentages, a fixed number, or both.

Enable faster, more thorough investigations

Fraud investigation units need efficient, effective access to research to keep from being overwhelmed by the magnitude of their task. Inquiries should be able to be made from a number of perspectives, including:

- The Customer—Who has "touched" this customer in the last x days and what did they do?
- Account—Who has "touched" this account in the last x days and what did they do?
- Employee—What has this employee done in the last x days? (This should include online activity and report generation and queries.)

V. Fixing Internal Fraud Requires a Learning Organization

Internal fraud is not going away. Every investigation generates new insights into insider schemes, criminal activity, organizational vulnerabilities and data structures. To be effective, strategies for improving monitoring and detection systems and complementary corporate processes and practices must grow and evolve with these insights. When internal fraud data and investigation results are incorporated into the organization as part of a holistic education process, financial institutions can make important improvements to decrease their internal fraud losses.

Companies that understand the business challenges associated with internal fraud, that implement best practices for hiring and training, that create a culture of responsibility and trust, and that implement holistic, integrated technology solutions will be best prepared to minimize their losses and mitigate risk of financial and reputational damage. The Santa Fe Group Vendor Council will address these areas in greater detail in future briefing papers.

1. 2006 ACFE Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2006. Downloadable at <http://www.acfe.com/documents/2006-rttn.pdf>
2. 2006 ACFE Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2006.
3. KPMG Forensic's Fraud Barometer press release, "Boom in Organized Crime Takes Fraud Cases to Record Levels," January 29, 2007.
4. Office of Strategic Crime Assessments, "The Changing Nature of Fraud in Australia," Commonwealth of Australia, 2000.
5. 2006 ACFE Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2006.h

Acknowledgements

The Santa Fe Group Vendor Council would like to acknowledge the following individuals, who made important contributions to this paper:

Jayne Dicus, ChoicePoint

ChoicePoint partners with organizations to develop comprehensive employment screening solutions that include background investigations, online applications, drug-free workplace programs, fingerprinting and more.

Andy Morris, Carreker Corporation

Carreker provides an enterprise fraud management platform that includes Detection, Alert and Case Management, enabling financial institutions to mitigate fraud risk through intelligent cross-channel transaction monitoring and a holistic understanding of customer and employee behavior.

Mike Mulholand, Metavante

Metavante Corporation delivers banking and payments technologies to financial services firms and businesses worldwide, with products and services 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.

Tony Selway, Early Warning Services, LLC

Early Warning Services, LLC, an integrator of information and technology to fight identity and payment fraud, maintains and operates the Internal Fraud Prevention service to help identify job applicants and employees who were released by another financial services organization because they knowingly caused or attempted to cause financial losses.

Mike Williams, Memento

Memento, Inc.'s flagship software product, Memento Security, enables financial institutions to proactively monitor, detect, and investigate inappropriate activities of authorized insiders.

Additionally, the Vendor Council thanks Robert Jones of RW Jones Associates and Jodi Pratt of Jodi Pratt & Associates for their contributions.