Aite PARTNER. ADVISOR. CATALYST.

Enterprise Fraud Management: Still Evolving After All These Years

THIS DOCUMENT IS AN EXCERPT OF A TWENTY-FIVE PAGE INDEPENDENT RESEARCH REPORT PUBLISHED BY AITE GROUP IN MAY 2014. PROVIDED COMPLIMENTARY BY:

TABLE OF CONTENTS

LIST OF FIGURES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- Financial institutions (FIs) can effectively perform enterprise fraud management (EFM) in a centralized or decentralized manner. A decentralized approach sacrifices operational efficiencies and customer service, while a centralized function can make for more efficient operations, hold one area fully accountable for the function, and extend a career track to employees, yielding greater dedication and productivity.
- EFM has become increasingly important over time as fraud attacks continue to evolve and become more aggressive.
- An effective, efficient EFM department has many components. True EFM covers all of them, from detecting and preventing fraud to handling customer claims, investigating and recovering funds in fraud cases, processing fraud charge-offs, producing desired management reporting, and performing root cause analysis of fraud losses to improve the fraud-prevention function.
- Centralized EFM improves customer service by providing a single point of contact for the victimized customer. The customer does not have to contact multiple departments, and the organization operates more efficiently as well.
- A number of EFM providers offer a full view of customers and their activity through robust case management tools that can integrate the outputs of all fraud-prevention systems (including their own). This is necessary to detect fraud effectively and reduce false positives to a manageable level.
- EFM providers can offer improved operational efficiency through automated workflows with built-in reminders and review and approval steps. They can also ensure compliance with defined time frames or deadlines.
- New solution providers that desire to provide EFM capabilities are emerging. FIs looking for a provider should consider them as these new providers continue to make progress.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

Effective EFM is essential for financial institutions to protect themselves and their customers against financial fraud. Institutions across the globe are under attack by hackers, organized fraud rings, opportunistic amateurs, and clients' family members and friends; in the case of first-party fraud, the customer and fraudster are one.[1] These parties are constantly attempting a wide variety of fraud types, from opening new accounts to account takeover to transactional fraud. No financial product or delivery channel is safe from fraud attempts.

Enterprise fraud management is a phrase that is often used, but it means many different things to different people. Throughout this report, the phrase will allude to the capability to manage fraud across an entire enterprise; in the real world, this applies to the list of products, services, and delivery channels the fraud department is responsible for supporting. For example, at a bank, fraud management may cover all types of loan and deposit accounts as well as brokerage, insurance, and others. It will also encompass all delivery channels: branch, ATM, online, contact center, mobile, and mail. Managing fraud across an enterprise entails understanding customer behavior as well as analyzing transactional activity within the context of all delivery channels—both are necessary to have a true view of what is happening in a specific customer's accounts.

Many companies claim to offer EFM capabilities to financial institutions. Some have made the bulk of their offerings available as products, while others prefer to provide custom -developed software to meet each specific client's needs. One essential component of EFM is a robust case management system. This report will focus on EFM; a second report will perform a vendor evaluation of case management providers.

METHODOLOGY

This report is based on interviews and demos with EFM providers, financial institution executives, and Aite Group's in-house knowledge.

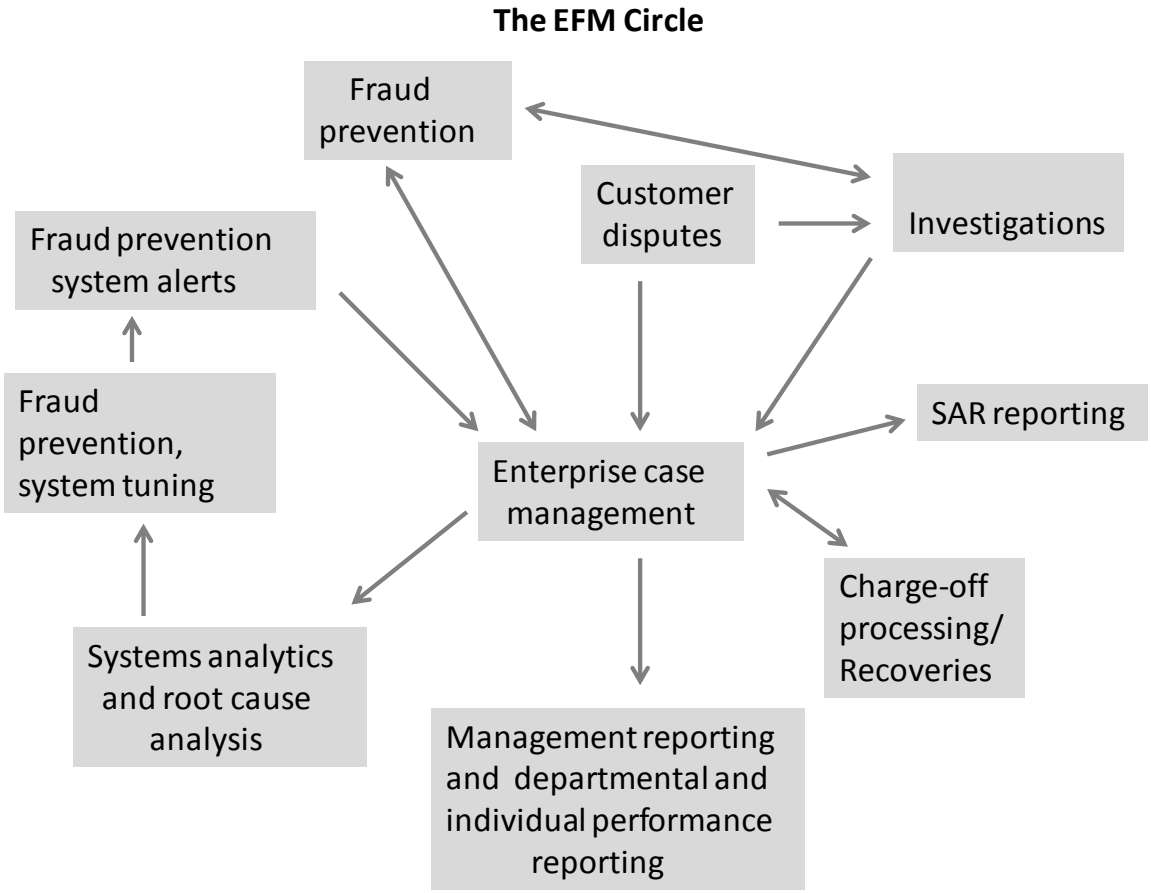
1. See Aite Group's Report *First-Party Fraud: The Global Battle Against Diabolical Charge-Offs*, October 2012.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

EFM COMPONENTS

Many elements make up an effective EFM function. As shown in Figure 1, data flows back and forth among many of these components and enterprise case management. Fighting fraud effectively requires an enterprise case management system, which is the hub of all activity. Analysts and investigators can view information about customers and their accounts (monetary and maintenance transactions) in one location, and alerts from all fraud-prevention systems can be aggregated together. Fighting fraud begins with fraud prevention and moves from department to department, ending with input from fraud case analysis (also known as root cause analysis), which is used to better future fraud-prevention detection alerts. Thus, fraud efforts revolve in a full circle, with case management always at the heart of the activity. The following sections describe and explain each of the EFM components in detail.

Figure 1: EFM Diagram



Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CASE MANAGEMENT

Everything in an effective EFM operation revolves around a robust case management capability. Key benefits of case management include:

- Aggregating and decisioning alerts
- Case transition
- Customer disputes
- Suspicious activity reports (SARs)
- Workflow techniques

Effective case management saves a tremendous amount of time over manual processes and leads to increased operational efficiencies. In addition, management can run reports out of the case management system, detailing the results of individuals, individual functions, and the overall EFM department. Such reports can provide valuable information related to budget goals, loss levels, and individual performance metrics.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

FRAUD PREVENTION

The best EFM solutions allow the institution to select from a number of fraud-prevention modules as well as provide decisioning capabilities and the ability to ingest alerts from other systems, thereby enabling a 360-degree view of customers' activity and accounts. FIs cannot afford, nor do they necessarily desire, to replace all existing fraud-prevention capabilities. Typically, they will begin by choosing an EFM provider that can address their most pressing need, which may be an Automated Clearing House (ACH) and wire fraud solution, a case management solution, or something else.

Over time, these providers have seen a lot of success with a "land and expand" approach: They begin with one module, and the FI purchases additional modules over time. The consensus among EFM providers is that financial institutions understand the need for one provider that can help them achieve a single view of the customer, and while many FIs still are in search of a point solution for a pressing need (most commonly ACH and wire fraud detection, case management, or enhanced online fraud detection), almost all are asking if the provider of that point solution can grow with them over time and eventually morph into their EFM provider.

Many fraud-prevention providers offer point solutions to mitigate one or several types of fraud. A few of these companies even offer their own simple methods of working the alerts generated by their prevention solution, but they do not offer the robust case management product that enables effective EFM. There is no silver bullet to fighting fraud, but many of these point solutions are very effective. Table A highlights solution providers for some types of fraud.

Table A: Fraud-Prevention Point Solutions

Fraud-prevention problem	Fraud solution providers		
Check fraud—on-us checks	BAE Systems Fiserv Orbograph	FICO Intellinx Softpro	FIS NICE Actimize SQN
Check fraud—deposits	BAE Systems FIS NICE Actimize	Early Warning Services Fiserv	FICO Intellinx
Check fraud—kiting	Banker's Toolbox FIS Verafin	BAE Systems Fiserv	Computrol Intellinx
Debit card fraud	ACI Worldwide FICO NICE Actimize Verafin	BAE Systems FIS SAS	First Data Fiserv Vantiv
Credit card fraud	Accertify BAE Systems FICO Fiserv Vantiv	ACI Worldwide CyberSource First Data NICE Actimize	Alaric Experian FIS SAS

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Fraud-prevention problem	Fraud solution providers		
Online fraud	41st Parameter FICO NICE Actimize ThreatMetrix	ACI Worldwide Fiserv RSA	BAE Systems ID Analytics SAS
Contact center fraud	Auraya Systems FICO Natural Security Phone Factor TradeHarbor VoiceTrust	Authentify Fiserv NICE Actimize Pindrop Security TrustID VoiceVault	Convergys Mattersight Nuance SpeechPro Verint Voxeo
ACH and wire fraud	ACH Alert FICO Guardian Analytics SAS	ACI Worldwide FIS Larue Technologies Verafin	BAE Systems Fiserv NICE Actimize
ATM fraud	BAE Systems Fiserv Parascript	Diebold NICE Actimize SAS	FICO Paragon
Employee fraud	BAE Systems Intellinx	FIS NICE Actimize	Fiserv
New account fraud	BAE Systems Experian ID Analytics Verafin	Early Warning Services FICO Lexis Nexis	Equifax Fiserv TransUnion

Source: Aite Group

CUSTOMER DISPUTES

Despite financial institutions' efforts at fraud prevention, clients still detect and report the majority of fraud. In fighting fraud, time is money; the quicker an institution is made aware of fraud on an account or card, the faster it can prevent additional fraudulent activity. Often, consumers use a centralized phone number to report fraud, although some institutions have different numbers for different types of fraud. Regardless, capturing all fraud reported in one case management system allows a full view of what is happening in a customer's account(s), and allowing a single point of contact for all fraud improves customer service.

INVESTIGATIONS

While fraud prevention is a worthy goal, no financial institution, no matter how many prevention solutions it deploys, is able to prevent all fraud. Investigators are always needed to examine the details of a case, determine what steps should be taken, decide whether to reimburse the customer (and whether to pursue reimbursement for the bank from the offender or prosecution through law enforcement or small claims court), and try to recover funds that have left the institution fraudulently. Again, time is of the essence. While wires and out-going ACH

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

transactions are guaranteed funds, if the investigator acts quickly enough, he or she may locate the funds and successfully retrieve them by sending the necessary documentation (e.g., hold harmless agreements) to the institution where the funds reside. (To avoid potential confusion, customers do have the right to dispute unauthorized ACH transactions received by their financial institution and posted to their accounts, and those transactions can be returned on a timely basis; only ACH files originated by a financial institution and sent to the ACH network are guaranteed funds.)

A case management system that captures all steps taken in an investigation is essential. It allows a supervisor to determine if steps are missed or if training is needed as well as to quickly see how each investigator is performing. It can track metrics concerning each investigator's case load as well as success in recovering funds. It also facilitates documentation that can be turned over to law enforcement or federal agencies in cases where prosecutions are pursued, and it provides a historical record of all case activity, which can be extremely useful in case of lawsuits or other future inquiries.

CHARGE-OFF PROCESSING AND RECOVERIES

Working fraud alerts, handling customer disputes, and investigating fraud cases quickly will never enable an institution to avert all fraud losses. Therefore, charge-off processing is a necessary function, at most institutions handled by a dedicated person or team. In no situation should an investigator handle his or her own charge-offs or recoveries or make any entries to these general ledger accounts—ensuring adequate segregation of duties prevents internal fraud opportunities. Since avoiding losses and recovering funds are often part of an investigator's performance review, it is important that these entries reflect the person responsible for the case or recovery of funds. In addition, there must be an entry and approval process that requires two people to review each general ledger transaction. Whether the case management system has an actual interface to the general ledger system or just generates a batch file of entries, this capability will result in additional operational efficiency within the enterprise fraud department.

MANAGEMENT REPORTING

Management reporting is essential to the success of any enterprise fraud department. After investing in various fraud solutions, executive management may not understand why fraud losses continue to occur. In the current environment, in which fraud attempts of all types are escalating rapidly, it is essential to be able to produce timely, accurate departmental reports to show the results of fighting fraud. To keep losses flat or growing only slightly may require additional staff, a cost that may not be approved unless facts and figures document the need. Financial fraud is big business, with fraud rings around the world focused on institutions and

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

their clients in the United States. Accurate management reports can also help educate executive management about these challenges.

SYSTEMS ANALYTICS AND ROOT CAUSE ANALYSIS

It is essential for any EFM department to accurately assess how and why losses are occurring. It may be that a simple tweak to a procedure or system will detect similar future fraud attempts, or an investment in a new fraud solution may be necessary, and data must be tracked and captured to create a business case. Without accurate root cause analysis of current losses, FIs may invest in solutions that fail to address the true gap that is allowing fraud losses to occur. For these reasons, and because the skills required to perform root cause analysis are similar to those required by EFM systems analytics personnel, these functions are often performed by the same person or department within the EFM division. If the true fraud problem is not diagnosed properly, the FI may invest in solutions that don't lead to the reduced fraud losses projected in the business case.

FRAUD-PREVENTION SYSTEM ALERTS

As noted previously, fraud alerts flow into a case or alert management system. But it is very important to monitor the number and quality of alerts being generated by each prevention system. A large number of false positives is very detrimental to the success of fraud prevention, as is a large number of false negatives. Prevention analysts who must go through many alerts daily without detecting fraud cannot feel they have accomplished much, and, over time, may become dissatisfied with their job. After reviewing dozens of alerts without detecting fraud, a prevention analyst is more likely to mishandle the one alert that represents fraud due to job fatigue or daydreaming. Systems with very high false positives should be adjusted to the extent possible and replaced with improved technology, as funding allows. Systems with high false negatives just can't be tolerated, and the solution provider or in-house IT personnel who wrote the code should be held accountable until that code performs as expected.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ORGANIZATIONAL STRUCTURE

FIs may choose a centralized approach to EFM or a decentralized organizational structure. Either can work effectively as long as there is good communication, cooperation, and integrated systems. Even in centralized organizations, there are differences in the responsibilities given to the enterprise fraud group. As an example, at some institutions that cover liability risk management, responsibility is limited to retail customers, while at other banks, the department supports fraud mitigation for treasury services and small-business clients as well. Debit and credit cards may be supported in the line of business instead of in the enterprise group, or debit cards may be supported because they are associated with the checking account, but not credit cards. The point is that while there is a multitude of variations, executives combating fraud all have the same responsibilities and needs.

Management should consider a centralized approach to EFM for many reasons.

- Attracting and retaining talent
- Consulting services
- Technology
- Customer service
- Operational efficiency

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

SOLUTION PROVIDERS

Many companies claim to be EFM solution providers but address only a portion of an EFM department's needs. This Impact Report profiles only companies that address several of the requirements detailed previously. Since case management is essential to the success of any EFM group, a robust case management system is an essential requirement for any solution provider to be included here, along with some fraud-prevention capabilities (Table B). This report describes a centralized model for each provider, but most of the information can be applied to a decentralized environment as well.

Table B: EFM Solution Providers Overview

Company name	Year founded	Headquarters	Number of employees	Top 2 markets
ACI Worldwide	1975	Naples, Florida	4,500 total	Americas, Europe
BAE Systems Applied Intelligence	1971	Boston, Massachusetts	800 in fraud and AML; 2,800 total	Americas, Europe
FICO	1956	San Jose, California	2,600 total; over 150 in EFM	United States, Europe
FIS Memento	1968 (as Systematics)	Jacksonville, Florida	37,000 total	Unites States, Europe
Fiserv	1984	Brookfield, Wisconsin	21,000	Americas, Europe
Intellinx	2005 (from Sabratech Ltd.)	Israel		United States, EMEA
NICE Actimize	1999	Israel	Over 600	United States, Europe
SAS	1976	Cary, North Carolina	14,000	United States, Europe

Source: Aite Group

SAS PROFILE

SAS is one of the best-kept secrets among enterprise fraud solution providers. Headquartered in Cary, North Carolina, the privately held company is best known for its superior analytics and ability to do custom projects to meet the needs of its clients. While financial services companies use SAS in many areas, its focus on fraud is relatively recent. SAS has developed many fraud modules and has a strong case management system that helps integrate all the data needed. In addition, it can add any custom work desired by the client. SAS is currently enhancing the deposit and on-us check fraud detection modules to support faster payment processing needs, while mobile fraud detection is currently deployed as a customized solution on the enterprise

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

architecture. SAS' process is to then take that learned intellectual property from live deployments and incorporate those capabilities into the out-of-the-box SAS solution.

Fraud and security intelligence has become a top priority for SAS and is now becoming its fastest area of growth. SAS' clients send data to a consortium model quarterly, which is then used for all clients. A few of the largest banks still require custom models, not wanting to rely on consortium models alone. Currently, the company is focused on extending real-time interdiction beyond card issuance and POS, as well as on building the capability to use Hadoop to refresh and use all data in a matter of seconds for detecting fraud. The use of SAS fraud management is growing quickly around the globe.

Table C highlights the modules SAS currently has to offer.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Type of fraud/ AML	SAS
Check fraud—On-us, deposit, and kiting	Yes
Debit card fraud	Yes
ACH and wire fraud	Yes
Credit card fraud—Issuing	Yes
Credit card fraud—Acquiring	Yes
Online fraud	Yes
Contact center fraud	B
ATM fraud	Yes
Retail branch/ Store fraud	B
Mobile fraud	No
Employee fraud	B
Other fraud types	Application fraud for loans, broker surveillance
AML—Know Your Customer (KYC), watch lists, suspicious activity monitoring (SAM)	Yes

A—No productized solution, but can take a data feed from this delivery channel on a custom basis; B—Can be customized during implementation; C—A partial solution addressing bust-outs and common point of compromise can be customized
Source: Aite Group

ANALYTICS

The use of analytics is extremely important in fighting fraud. As fraud becomes more sophisticated and schemes more complex, simple rules are not enough to protect the FI or its customers. Table D profiles the types of analytics SAS has incorporated in their product set. EFM solution providers also offer varying functionality. Table D summarizes the capabilities offered by SAS.

Table C: Analytic Capabilities of EFM Providers

Company	Fraud detection methods used
SAS	Analytics is viewed as a key differentiator for SAS; many types of analytics are used

Source: Aite Group, company data

Table D: EFM Provider Functional Checklist

Function	SAS

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Function	SAS
Real-time interdiction	Yes
Ability to import and decision all fraud alerts, including other vendors'	Yes
Enable workflow	Yes
SAR reporting	Yes
Management, employee, and departmental reporting	Yes
Charge-off processing	No
Ability to use unstructured data	Yes
Utilizing big data (language such as Hadoop)	Yes
Offer hosted solution	Yes
Offer public or private cloud storage	Yes

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CONCLUSION

EFM continues to evolve as fraud attacks become increasingly complex and sophisticated. Here are a few recommendations for FIs and solution providers in the space.

For financial institutions:

- **Talk with providers to ensure you have a current picture.** The strongest providers are regularly updating their solutions with new features and modules, so information may become outdated quickly.
- **Select a provider that can help integrate your existing fraud-prevention system outputs;** no FI can afford to replace all its existing tools, nor should it wish to. Many point solutions provide valuable insight needed to obtain a complete customer view.
- **Ensure the EFM provider you select has a healthy research and development budget.** Fraudsters and organized fraud rings are attacking with increasing creativity and vigor. The provider you select must be committed to upgrading its solution so it remains viable.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is an independent research and advisory firm focused on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, securities & investments, and insurance, Aite Group's analysts deliver comprehensive, actionable advice to key market participants in financial services. Headquartered in Boston with a presence in Chicago, New York, San Francisco, London, and Milan, Aite Group works with its clients as a partner, advisor, and catalyst, challenging their basic assumptions and ensuring they remain at the forefront of industry trends.

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+44.(0)207.092.8137
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com