Compliments of Verafin

FRAML For Dummies®

Verafin Limited Edition

Combine your fraud detection and anti-money laundering efforts

Diana Byron

FRAML FOR DUMMIES®

VERAFIN LIMITED EDITION

by Diana Byron

WILEY

John Wiley & Sons Canada, Ltd.

FRAML For Dummies®, Verafin Limited Edition

Published by
John Wiley & Sons Canada, Ltd.
6045 Freemont Boulevard
Mississauga, Ontario, L5R 4J3
www.wiley.com

For details on how to create a custom book for your company or organization, or for more information on John Wiley & Sons Canada custom publishing programs, please call 416-646-7992 or e-mail publishingbyobjectives@wiley.com.

For general information on John Wiley & Sons Canada, Ltd., including all books published by Wiley Publishing, Inc., please call our warehouse, Tel 1-800-567-4797. For reseller information, including discounts and premium sales, please call our sales department, Tel 416-646-7992. For press review copies, author interviews, or other publicity information, please contact our marketing department, Tel 416-646-4584, Fax 416-236-4448.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

ISBN: 978-1-118-09571-3

Printed in Canada

1 2 3 4 5 STG 15 14 13 12 11

WILEY

Publisher's Acknowledgements

We're proud of this book; please send us your comments at `http://dummies.custhelp.com`.

Some of the people who helped bring this book to market include the following:

Acquisitions and Editorial

Acquiring Editor: Robert Hickey

Manager, Custom Publications: Christiane Cormier

Production Editor: Elizabeth McCurdy

Composition Services

Production Coordinator: Kristie Rees

Layout: Carrie A. Cesavice

Proofreader: Melanie Hoffman

John Wiley & Sons Canada, Ltd.

Deborah Barton, Vice President and Director of Operations

Jennifer Smith, Publisher, Professional and Trade Division

Alison Maclean, Managing Editor

Publishing and Editorial for Consumer Dummies

Kathleen Nebenhaus, Vice President and Executive Publisher

Kristin Ferguson-Wagstaffe, Product Development Director

Ensley Eikenburg, Associate Publisher, Travel

Kelly Regan, Editorial Director, Travel

Composition Services

Debbie Stailey, Director of Composition Services

About Verafin

Verafin is the North American leader in BSA/AML-compliance and fraud-detection software. Its software helps financial institutions protect against banking fraud and comply with the Bank Secrecy Act, the USA PATRIOT Act, and FACTA RED FLAG regulations.

Learn more about Verafin at `www.verafin.com`.

Introduction

Today's business environment makes operating profitably tougher than ever for a financial institution (FI). FIs are challenged to maintain customer trust and loyalty, cut costs, and maximize efficiencies, all while fighting increasingly complex financial crimes and managing growing regulatory burdens. To succeed, FIs aim to balance managing risk, increasing profitability, and ensuring superior customer service.

FIs recognize that embracing a coordinated approach to fighting financial crime can help them achieve these goals. To reflect this unified approach to combating fraud and money laundering, Verafin, one of North America's leaders in fraud detection and anti-money laundering (AML) software, coined a new term: *FRAML* (**fr**aud detection and **a**nti-**m**oney **l**aundering — pronounced fram-*uhl*).

About This Booklet

This booklet is all about consolidation: Bringing AML and other financial crime-fighting and compliance efforts together so your FI can respond to crime more efficiently and effectively. In this booklet, I explain the basics of fraud and money laundering and detail how combining the fights against both can benefit your FI. I also describe how new technologies can help you fight fraud and money laundering, and I offer tips for shopping for new FRAML software.

Foolish Assumptions

If you're reading this book, I assume you work in the financial services industry (most likely at a bank or credit union) and hold a position such as one of these:

- ✓ A compliance officer responsible for your FI's AML efforts
- ✓ A fraud investigator
- ✓ A manager of employees working in a compliance or fraud-fighting capacity
- ✓ An employee who makes decisions related to reducing financial crimes, overseeing compliance obligations, and/or selecting related software

How This Booklet Is Organized

I've divided this booklet into four parts. If you have a specific question, you can turn right to the appropriate part. Or if you're looking for a way to pass the time on your lunch break, put your feet up and enjoy the whole thing.

Part I: Understanding Financial Crime

Financial crime is everywhere and, with its links to organized crime and terrorism, understanding and stopping it are more important than ever. In this part, I introduce you to the basics of fraud and money laundering and point out how the two are connected.

Part II: Combining Anti-Fraud and Anti-Money-Laundering Efforts

In this part, I explain why merging the fights against fraud and money laundering makes sense. I discuss the advantages of consolidating, detail the key components of an integrated approach, clarify how different-sized firms set up their departments, and offer a success story.

Part III: Alerting You to Potential Financial Crimes

Fighting financial criminals requires the right technology. In this part, I examine the two main types of technologies available to help you.

Part IV: Ten Tips for Choosing FRAML Software

Should you decide that a consolidated FRAML approach is for you, the right technology is key for success. I offer some suggestions of what to look for when picking out your software.

Icons Used in This Booklet

Occasionally you'll notice these symbols on the left-hand side of the page, bringing your attention to a particular piece of information. Here's what each means:

REMEMBER Indicates information that's worth remembering in your fight against financial crime.

TECHNICAL STUFF

Signals information of a more technical nature. If it sparks your interest, read it. If it makes your eyes glaze over, you can bypass it without missing critical details.

TIP

Draws your attention to something that may save you time, money, aggravation, or all three.

WARNING!

Alerts you to situations or circumstances that can be harmful to your career or that are just plain illegal.

Part I

Understanding Financial Crime

In This Part

- Finding out about fraud
- Making sense of money laundering
- Understanding how fraud and money laundering intersect

Financial institutions (FIs) are serious about fighting fraud and money laundering. In this part, I explain both of these crimes and point out that although they're different, they're very much related.

Understanding Fraud

Fraud is an attempt to unlawfully obtain money. A wide variety of fraud schemes and scams affect FIs, involving many different instruments, products, channels, and transactions.

Exploring where fraud occurs

To ensure you have a complete and accurate picture of the scale and scope of your FI's fraud threats (and thus how your FI should handle them), you need to consider your fraud risks and vulnerabilities across different

- **Instruments** such as bank drafts, checks, official checks, promissory notes, travelers' checks, and money orders. Fraudsters don't discriminate; they're always looking for weaknesses in how FIs handle monetary/payment instruments. If they find one, they exploit it.
- **Products** including deposit accounts, Automated Clearing House (ACH) and wire services, lending services, and online/mobile banking applications. Fraudsters use these products and services to their advantage, either by using their existing accounts, opening new accounts, or taking over existing customers' accounts without their knowledge or consent.

TIP To get a handle on the fraud risks associated with your products and services, look across all of your FI's business lines and locations.

- **Channels** including your branches, your call center, your ATMs, a merchant's point-of-sale system, the Internet, or a mobile device. Customers and fraudsters alike access your FI's financial services through one or more of those five channels.
- **Transactions** including deposits (credits), withdrawals (debits), and transfers. Customers and fraudsters initiate transactions to move

money around. Other transactions, such as return deposit items or ACH returns, may warrant particular attention because they can be red flags of possible fraud (or at the very least, may identify a customer who poses a potential risk to your FI).

TIP Don't forget international transactions. Recovering stolen funds involving fraudsters in other countries can be particularly difficult and costly, if not impossible.

Investigating how fraud happens

In addition to surveying where fraud may occur at your FI, also think about how fraudsters may commit their crimes. For example, fraud can be committed by

- **Counterfeiting** (as with cash, checks, or debit cards)
- **Outright theft** (of checks, cards, identities, or online bank account credentials)
- **Impersonation** (such as identity fraud or telephone banking fraud, where the fraudster pretends to be the person whose identity they've stolen)

REMEMBER Two or more types of fraud can occur together. For example, a fraudster could commit *identity theft* by stealing a customer's personal information and identity. The fraudster could then use that information to commit *debit card fraud* by creating a counterfeit debit card to gain access to the customer's account.

Be aware of malware

A popular form of fraud involves hijacking online banking accounts. Criminals install *malware* (**mal**icious soft**ware**) on a FI's customers' computers. (Actually, even worse, they have your customers install it for them.) Although some malware simply tracks a victim's keystrokes, other forms of malware alert criminals when a victim's online account becomes active. When they receive an alert indicating that a victim is online, the criminals piggyback on the online banking session and hijack the transactions. The victim does not know what is happening and believes that he's completing his regular transactions.

Keeping customers happy

Regardless of what banking regulations say, customers usually feel that their FIs should be responsible for keeping their accounts safe and reimbursing them for fraud losses. Aside from causing direct losses, fraud can ruin customer relationships and destroy customers' trust in a FI, even when a customer's stolen funds are recovered. In many cases, customers who fall victim to fraud while banking with one FI end up taking their business elsewhere.

When individual consumers notify their FI of theft within a specific timeframe, they're usually protected from fraud losses. That means your FI is on the hook for any outstanding amounts if the funds can't be fully recovered.

Although FIs aren't required to reimburse commercial customers for these types of fraud losses, the resulting investigations, legal proceedings, and negative publicity can prove costly.

Explaining Money Laundering

Money laundering is an attempt to disguise the source of a sum of money. Criminals, including fraudsters, drug traffickers, terrorists, and arms dealers, use money laundering as a way to fund and expand their illegal activities.

Everyone does laundry. You know the drill — when you launder your dirty clothes, you put them in the washing machine and, with the exception of the odd missing sock, they come out clean. The same principle applies when the bad guys launder their money. Instead of using a washer, the bad guys put their dirty money into the financial system, through banks, credit unions, money services businesses, insurance companies, and other types of FIs, so the money appears legitimate.

Money laundering involves three steps, which can occur simultaneously or separately:

- **Placement:** The bad guys put their ill-gotten gains into the financial system. This can be as simple as depositing cash into a bank account. Because FIs must report certain cash transactions — like cash deposits of more than $10,000 from a single customer in a single day, the bad guys often break down a large deposit into several smaller ones to avoid detection.

For example, Bob the bad guy deposits $5,000 to his personal account at bank branch A, $3,000 into his joint account at bank branch B, and $4,000 through an ATM at bank branch C. Breaking up the deposit like this, so the FI will not be suspicious and report it to the Department of the Treasury, is called *structuring*. And it's illegal.

WARNING! Customers who structure their transactions to avoid detection can receive penalties that include up to five years in jail or a fine of up to $250,000. If the structuring involves more than $100,000 in a 12-month period or is performed while violating another law, the penalty is doubled.

- **Layering:** Next the bad guys try to cover their tracks by carrying out a variety of transactions. Moving the money around makes finding its original source difficult. For example, Bob the bad guy creates phony companies (in the form of *shell corporations*) and transfers money between them to make the funds appear legitimate.
- **Integration:** After the money has been deposited into the financial system and its origins have been clouded by a series of transactions, it's "clean." Now the bad guys, like Bob, use the money to purchase material goods (such as a yacht, a vacation home, or a statue for the front lawn) or invest it in further criminal activities.

TECHNICAL STUFF

Laundering the loot

Getting illegally obtained funds into the financial system (the *placement* stage of money laundering) can be time consuming. The crooks must stay below certain thresholds to avoid detection, which means lots of small-scale transactions. Because the crooks are busy perpetrating other crimes, they often contract out these tasks to one of two types of criminals:

Smurfs: These criminals make small deposits on behalf of the bad guys. They earned their nickname because their behavior (scurrying about from bank to bank and depositing small sums of cash into multiple accounts) resembles that of the little blue creatures of Saturday-morning cartoon fame.

Money mules: These people (not donkeys) carry or transfer stolen funds, often to international locations. Sometimes they're willing accomplices, other times they're forced or even tricked into playing the role of money mule. Regardless, money mules move the funds in a variety of ways, including smuggling the cash, using money transfer services, and electronically forwarding the funds.

Connecting Fraud and Money Laundering

So, what do fraud and money laundering have in common? In many cases, criminals perpetrating fraud need to launder the proceeds of their crimes through the financial system. This means those responsible for your FI's response to financial crime must connect the dots between fraud and money laundering. Spotting possible money laundering activity might alert you to possible fraud victims, and vice versa.

Check out the following example to see how crooks commit fraud by hijacking an account and laundering the proceeds:

Note: Although the example presents a case where the victim is a commercial customer, victims can also be individual consumers.

Jim is owner and CFO of J&J Construction, a successful company with 39 employees that is a long-term customer of Anytown Bank. The company uses Anytown's online corporate banking platform to access the ACH network and securely send payroll payments to its employees. On Friday, Jim receives an email that appears to be from Anytown Bank telling him that a problem occurred with an ACH payment, but the problem has been resolved. The email contains a link to a transaction resolution document. Jim opens the link and reads the brief explanation about the error and its resolution. "Gotcha!" says the fraudster. By clicking the link Jim unknowingly downloaded malware giving the fraudster direct access to J&J Construction's online banking account. (For more about malware, see the earlier sidebar, "Be aware of malware.")

The following Tuesday, Jim logs on to the company's online account using the time-controlled, one-time password token provided by Anytown. He prepares and initiates his usual payroll transaction. While Jim is online preparing to send the company's regular payroll, the fraudsters hijack his transfer request. Instead of receiving an ACH transfer request of $81,000 payable to J&J's 39 employees, Anytown receives an ACH transfer request of $431,000 payable to 79 payees (the legitimate transfer, plus a big bonus for the bad guys). This is fraud.

Now the fraudsters need to launder the money they stole. Because the stolen cash is already in the financial system, they can skip the placement stage and jump right to the layering stage (refer to "Explaining Money Laundering," earlier in this part, for more on these stages).

The 40 new payees included in the fraudulent ACH payment work for the fraudsters, and soon after the ACH payment is sent, each payee withdraws slightly less than $10,000 in cash and proceeds to visit multiple money services businesses, sending three wire transfers of less than $3,000 each (the balance represents their commission). And that's the money laundering part of the scheme.

To illustrate how fraud and money laundering also can be connected to other financial crimes, imagine the money ends up with a terrorist organization that uses the money to fund terrorist attacks. Your FI's Bank Secrecy Act (BSA)/AML compliance program will be on the lookout for bad guys trying to do business with you. An early warning about a known bad guy who might be using your FI could, for example, help you identify money laundering more quickly, stop further fraud losses, and prevent laundered funds from reaching a terrorist organization. In Figure 1-1, I illustrate this overlap.

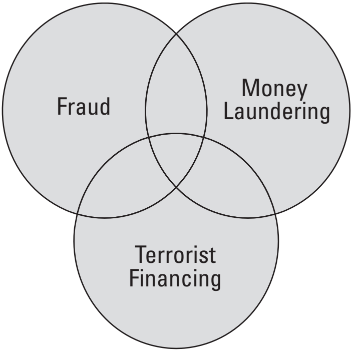

Figure 1-1: Managing overlapping financial crime and compliance concerns.

Part II

Combining Anti-Fraud and Anti-Money-Laundering Efforts

In This Part

- Approaching fraud and AML independently
- Consolidating the fight against financial crime
- Creating an integrated approach
- Implementing FRAML

Financial institutions commonly treat fraud and money laundering as two separate and distinct problems. However, the financial crimes are undeniably linked (in Part I, I explain how). Taking a holistic, cooperative approach that consolidates efforts to fight the two makes sense.

In this part, I discuss why tackling fraud and money laundering threats separately is inefficient and risky, and I look at how adopting an integrated approach can benefit your FI.

Separating Fraud and AML

FIs have traditionally handled anti-fraud and AML efforts separately, implementing multiple programs with independent components and activities. In the following sections, I explore why they take this approach and point out some of its problems.

Understanding the reasons for separation

Historically, anti-fraud and AML efforts emerged in response to separate business drivers, serving different purposes in pursuit of different goals.

FIs understand that they need to invest resources into fighting fraud. Anti-fraud efforts focus on possible criminal activities that have a measurable operational impact, either on the FI or its customers. For example, if a fraudster steals funds from a customer's account, either the FI or its customer absorbs the loss if the funds can't be recovered. Because monetary losses can be huge, the business case for fighting fraud is clear and easy to sell internally.

FIs sometimes fragment their anti-fraud efforts by addressing them at the geographic location or business unit where the suspicious activity is identified. For example, fraud involving checks may be classified as check fraud and handled by that department, even if the check fraud is part of a larger money laundering scheme.

By contrast, your FI's bottom line doesn't directly benefit from discovering money laundering (except by avoiding pesky penalties for non-compliance or possible reputational impacts and customer turnover). Instead, spending money to combat AML helps FIs manage risk and contributes to the safety and soundness of the financial system as a whole and to society at large. As such, investing in AML (and compliance, generally) is often perceived to be a *sunk cost*, with little or no opportunity to recoup a return on program investments.

The cons of separation

The result of all this separation is a number of disparate processes and teams. In the following sections I outline some of the specific impacts that separate anti-fraud and AML efforts can have.

Duplicate efforts

Unfortunately, separating crime-fighting efforts leads to extra work for already busy employees. Check out the following example of a FI using separate crime-fighting processes to see how easily a duplication of efforts can happen.

Lisa Stack, a compliance officer, and Mary Hunter, a fraud investigator, work at the same bank but are so busy they rarely have time to chat. One morning, Lisa grabs her coffee and digs into the latest pile of reports on her desk. A customer, Fred Kiter, had a particularly busy weekend. His activity appears on Lisa's excessive cash report.

She begins an investigation and notices that Fred made several large ATM deposits. She needs to determine if he deposited checks or cash. She makes a note to dig deeper and moves on to the next case.

Meanwhile, Mary settles in for another day of investigating fraud. As she reviews the check kiting report, Fred Kiter's activity jumps out at her. His multiple ATM deposits combined with several check withdrawals seem suspicious, and she begins an investigation.

Now two busy investigators are working on the same case because their processes are separate, with no synchronization between compliance and fraud investigators.

Risk exposure

Maintaining separate processes also exposes FIs to the risk that financial crime may go undetected. For example, fraud investigators review their cases to ensure that no fraudulent activity is taking place. After they've determined that no fraud is present, they close the case and move on to the next one. However, because fraud and money laundering are so closely linked, money laundering could be present even when fraud isn't. By not responding to the possible threat of money laundering, the FI leaves itself open to regulatory censure.

For example, a fraud investigator reviews a sudden flurry of deposits and withdrawals in a customer's account. He determines that the customer isn't kiting checks and closes the case. But that series of transactions often indicates money laundering as well as check kiting. In a cooperative environment, he would pass the case on to a money-laundering investigator instead of closing it, limiting the FI's exposure to crime and regulatory penalties.

Considering Consolidation

Compliance officers used to focus exclusively on Bank Secrecy Act (BSA) compliance and money laundering detection, while fraud managers tackled the growing problem of financial losses due to fraud. But bad guys don't separate their criminal activities, so why separate your crime-fighting activities? Financial crimes are becoming much more complex, often involving multiple lines of business, instruments, products, channels, and types of transactions. In this environment, taking an integrated, cooperative approach to fighting financial criminals increases the chances of beating them.

Benefitting from FRAML

Combining anti-fraud and AML efforts to fight financial crime in a coordinated way offers many advantages, including the following:

- Improved understanding of risk and financial crime as they affect the entire organization
- Increased loss recoveries and reduced losses through better detection of suspicious activities
- Greater understanding of customers, their needs, and their behaviors (suspicious or not)
- Improved operational efficiencies as you standardize and automate work processes
- Happier bank examiners (That's right — during audits, bank examiners look at how fraud and money laundering areas function and communicate with each other.)
- Reduced duplicate suspicious activity report (SAR) filings
- Enhanced employee satisfaction and retention due to improving workload management and training consistency

From a technology perspective, a FRAML approach that consolidates systems and tools and centralizes the management of communication and vast amounts of data and information provides FIs with the following benefits:

- ✓ Fewer false-positive alerts and duplicate cases
- ✓ Better prioritization of suspicious activity alerts and more effective risk-based decision-making
- ✓ Improved data quality and more effective data management
- ✓ Streamlined approach to system tuning because customer behavior parameters can be centrally configured
- ✓ Reduced technology costs for hardware, software, maintenance, support, training, and administration (one consolidated system is cheaper than two or more independent ones)

Overall, a consolidated approach to fighting fraud and money laundering makes detecting, investigating, and reporting suspicious activity easier for FIs. (Don't worry, I offer tips on bringing the two together in the "Creating a Consolidated Approach" section, later in this part.)

Improving efficiency and effectiveness

Using a FRAML approach creates a more efficient and cost-effective crime-fighting team. It also helps to maintain the integrity and stability of the financial system by weeding out more criminals and reducing FIs and customers' exposure to financial crimes. By reducing financial crime, FIs minimize the potential for regulatory censure and losses through theft, and they maintain good reputations.

REMEMBER Financial crimes can hurt a FI's reputation. In today's challenging and competitive economy, maintaining customer loyalty and trust with a solid reputation is more important than ever.

Remember Lisa and Mary from the example in "Separating Fraud and AML"? After their FI adopts a FRAML approach and consolidates anti-fraud and AML programs across all program components (that is, people, processes, and technology, which I talk about in the next section), their situation changes for the better.

Now all alerts are combined on a single system, which Mary reviews. She works on the fraud alerts, and when she receives an alert that may be money laundering, she passes it on to Lisa. Now Lisa has more time to focus on investigating suspicious activity (and other important tasks, such as customer due diligence and training). The FI also saves time and money spent on duplicate investigations.

Considering a Consolidated Approach

Successfully integrating anti-fraud and AML efforts means considering three key components: people, processes, and technology.

People

Fraud teams and money laundering teams attract employees from different backgrounds. Fraud investigators often come from a law enforcement background, and money-laundering investigators most often have a banking or compliance background. These different backgrounds lead to varied approaches and processes when handling financial crimes, which further separates these two groups.

To consolidate successfully, even if you don't physically combine anti-fraud and AML teams, think about how to improve communication between them. Consider cross-training your employees so they understand other roles within the financial crimes management area and know how each stage of the suspicious activity lifecycle (prevention, detection, investigation, reporting, and recovery) is managed.

Cross-training employees doesn't mean they have to become fully versed in another specialty. Instead, simply make sure they are aware of key features of other areas. For example, a fraud investigator should be able to recognize money laundering, and vice versa.

Processes

Merging your crime-fighting endeavors means implementing processes that address financial crime at every stage of the suspicious activity lifecycle, from initial detection and alert generation, to investigation, reporting, and monitoring. You'll need to make changes to core business processes, including:

- Alert management
- Case management
- Compliance management and reporting
- Communication and workflow support
- Data and system management

- Risk management
- Suspicious activity reporting
- Transaction and event monitoring

Technology

The right technology makes merging anti-fraud and AML efforts easier and improves the chances that your staff will support the changes in your processes. After all, they're more likely to embrace new technology that makes their jobs easier. Your technology should provide a common repository for all customer data, complementary money-laundering and fraud workflows, and centralized case management and compliance reporting. (In Part III, I talk about your technology options in detail.)

Structuring FRAML No Matter What Your Size

You may be wondering what your financial crime-fighting team will look like and how it will function after you adopt a FRAML approach. In this section, I point out how some FIs set themselves up for success.

REMEMBER

Taking a FRAML approach means making decisions about how people, processes, and technology will be organized to respond to financial crime, which is not a one-size-fits-all task. Think of FRAML as a continuum of possible approaches. Your job is to find the approach that makes the most sense for your FI, given your risks, available resources, and business strategy.

Organizing your FRAML efforts

Regardless of the size of your FI, in an integrated environment the crime-fighting team oversees all relevant anti-fraud and AML activities, as well as any related BSA tasks and compliance duties. Although everyone in the organization shares responsibility for reducing fraud and identifying possible money laundering activity, one person (or group) should take primary responsibility. When employees know that one person oversees all potential financial crimes, they can easily bring suspicions to his or her attention. Creating a central intelligence hub allows information to flow freely to and from a main source. This key person (or group) does the following tasks:

- Receives, reviews, and analyzes suspicious activity alerts
- Triages alerts and distributes those that require further review
- Coordinates all investigations
- Oversees the creation and filing of regulatory compliance reports

Firms with assets of up to $500 million generally staff their department with one or two people. The coordinator often also looks after BSA compliance. To cope with a bigger volume of customer transactions, larger FIs, with assets of up to $5 billion, have larger anti-fraud and AML teams of between three and eight people on each. And FIs with assets up to $20 billion often have more than one coordinator reviewing suspicious activities and employ up to 20 people per team.

Consider the following team structures:

- **A single, consolidated team**: Create a new team under the control of a unified Financial Crimes Department.
- **Separate teams**: Maintain the status quo of separate fraud and AML teams, but use technology to realign processes and consolidate some aspects of suspicious activity lifecycle management (for example, transaction monitoring or case management).
- **A hybrid approach**: Consolidate some aspects of your programs. For example, create a Financial Investigative Unit (FIU) responsible for investigating all suspicious activity, whether it's fraud or money laundering (or any other financial crime).

Looking at FRAML roles and responsibilities

The FRAML teams in FIs of all sizes share the following responsibilities:

- Acting as main point of contact with law enforcement officials
- Detecting, investigating, and reporting fraudulent activity
- Detecting, investigating, and reporting money laundering activity
- Recommending proactive process changes that may reduce financial crime and improve compliance
- Taking responsibility for garnishments, levies, and liens

In addition, FIs with larger teams and assets ranging from $500 million to $20 billion may also

- Liaise with other departments (such as card services, loans, and operations) to investigate potential cases of fraud
- Offer compliance and fraud training to staff in other departments
- Oversee information technology security, physical security, insurance, disaster recovery, and vendor management

How these responsibilities are divided amongst the members of a Financial Crimes Department (or whatever structure you adopt) varies from FI to FI.

Overcoming concerns

No one likes change, and switching from separate crime-fighting departments to a more consolidated, streamlined FRAML approach is going to present some challenges, primarily

- Overcoming the legacy of the different approaches used to achieve separate anti-fraud and AML goals, and
- Removing the constraints imposed by technology.

Overcoming the first obstacle can be difficult. Because of their different backgrounds (law enforcement and banking/compliance), fraud and money laundering investigators often prefer very different approaches and processes. And as fraud becomes increasingly complex and AML regulations become more stringent, service areas are becoming bigger and more discrete, which only adds to the problem.

Rather than jumping in and making wholesale changes right off the bat, begin by increasing communication and information sharing and aligning work processes to reduce duplication. After staff realize the benefits of consolidation firsthand, they'll be more likely to embrace larger-scale changes.

Gaining support from management is crucial to successfully implementing changes. Sometimes a (gentle) push and encouragement from above can keep the lines of communication open and improve staff's response to change.

Solving the second challenge, and moving away from autonomous technology programs, is (relatively speaking) easier. Behavior-based technologies (which I discuss in depth in Part III) help unite your fraud and AML strategies. Using this type of technology provides FIs with a consolidated solution without the constraints of the rules-based technologies that individual departments use.

Banking on consolidation

Headquartered in Warrenton, Virginia, the Fauquier Bank is a community bank with assets of $640 million and eight branches. It successfully embraces a FRAML approach, and has done so since 2002. Back then, it was looking for a way to better prepare for compliance audits and examinations and hired a former FBI agent with a background in financial crimes to help. Looking at the big picture, he noticed a significant overlap between the bank's fraud detection and AML

(continued)

(continued)

divisions and decided to create a centralized financial security department to avoid duplication of efforts.

Following his retirement in 2004, a new director of security, who also has an extensive law enforcement background, took over. He maintains the consolidated approach and views the security department as both a risk management hub and a communications hub. For example, other departments feed information to the security team, which allows them to enhance their knowledge of particular customers. This means they can proactively apply enhanced due diligence to customers who pose the greatest risk to the bank.

Fauquier successfully manages its FRAML approach by creating cross-trained, cross-functional teams that can handle both BSA/AML and fraud alerts. They're more effective because they use a single technology platform that allows them to review all types of alerts, communicate via the system notes, and stay on top of ongoing investigations through its case management feature.

In addition, the security department requires all bank personnel to attend annual training with the director of security, which keeps them current on important issues and puts the director front and center in the minds of employees, increasing the likelihood that they'll remember to refer any suspicious activity to him. The security department also attends all committee meetings, not only to get exposure across all bank channels, but also to ensure all products and processes are risk appropriate.

The end results of Fauquier's consolidation efforts include: increased efficiencies; improved enterprise-wide communication; a greater ability to protect their customers, assets, and reputation; and very impressed BSA examiners.

Part III

Alerting You to Potential Financial Crimes

In This Part

- Evaluating customer information
- Becoming familiar with rules- and behavior-based software

You need some serious weapons to fight financial crime. Stocking your armory with the right technology is a great strategic move. Technology helps you by automating routine tasks and improving business results. In this part, I look at how technology can help you during the first stage of the suspicious activity lifecycle: *detection*. I also consider common types of technology to help during the detection stage and beyond.

Analyzing Customer Data

At their simplest, anti-fraud and AML technologies transform vast amounts of data from a variety of sources into information that helps FIs determine if a customer's activity is suspicious or not.

REMEMBER

Although you can fight financial crime with a single technology solution, discovering fraud and money laundering requires different analytics. Your system should allow you to easily configure the detection parameters for fraud and money laundering independently. It also should use analytics that reflect the nature and timing of the specific financial crime you're trying to detect.

The data you use to detect suspicious activity can include customer transactions, demographics, events (such as a change of address or new card request), as well as third-party and other data sources.

Be sure you consider where data will come from, where it will be stored, and how it will be managed to ensure its quality and completeness. Don't underestimate the importance of data integration and quality to the FRAML approach.

TIP

Your technology solution should apply a single, unified model to customer data. This ensures that you have an enterprise-wide view of customer behavior available for analysis, review, investigation, and reporting.

Investigating Two Technologies

You can choose from software solutions that typically use one of two broad categories of technology: rules-based or behavior-based. In this part, I explore them both.

Rules-based software analyzes customer data using a set of rules pertaining to transaction limits and timing, but behavior-based software analyzes it using a combination of fuzzy logic (which I explain later), artificial intelligence, and customer behavior pattern recognition.

Relying on rules-based software

Rules-based software uses a simple set of *if-then* statements to model customer behavior and identify suspicious activity. It searches a FI's core banking (or other) system for transactions that match the parameters of a particular rule. Then it flags the relevant transactions so investigators can determine if they're routine or suspicious.

TIP

Unsure what kind of system you have? If you have to create a rule to generate an alert, you have rules-based software.

In Figure 3-1, I illustrate how rules-based software works.

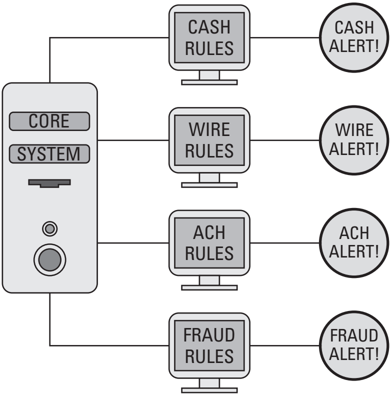

Figure 3-1: Rules-based technology.

For example, consider the following rule that you might use to flag potential cases of cash structuring:

“**IF** a customer has never made any deposit/withdrawal of $10,000 or more,

AND-IF a customer makes four or more cash deposits/withdrawals within 30 days,

AND-IF the total deposits/withdrawals are larger than or equal to $8,000,

THEN generate an alert.”

If you read this rule carefully, you’ll notice that the bad guys can avoid detection pretty easily. (You know how they hate to play by the rules.) If they make three deposits in 30 days, four deposits in 31 days, or four deposits of $7,900, no alert will be triggered because they didn’t break the rule. This means you must create additional rules to try to stop the bad guys from skirting them. Keep in mind that this example only deals with instances of cash structuring. Imagine how many rules you need to create to capture all of the possible instances of financial crime activity at your FI. In the next sections, I talk about some of the pitfalls of rules-based systems.

Exploding with information

Consider the following rule:

“**IF** a customer makes a single cash transaction greater than $3,000,

AND-IF the customer makes a single cash transaction less than $10,000,

THEN generate an alert.”

This rule generates an alert each and every time it's broken — yikes, that's a lot of alerts for you to review. And that's just one simple rule. In today's world, the volume and complexity of data and information make fighting crime with just a few simple rules impossible. The sheer number of variables required to adequately model the complex behaviors associated with financial crimes means you'll be creating a lot of rules. In fact, you may find your rules-based system using more than 1,000 rules in the quest to catch the lawbreakers.

Not only do these systems require constant testing, maintenance, and editing, but the large number of rules can result in something that sounds alarming but is not actually fatal. *Rules explosion* occurs when the number of rules causes an excessive number of false-positive alerts. (Receiving a false-positive alert means you're notified of activity that appears illegal — so you must investigate it — but the activity is in fact legitimate.)

Creating a lot of rules may seem like a good idea — more rules equates to catching more bad guys — but it's not that simple. When you create so many that a rules explosion occurs, you negate the benefits of automation. You spend so much time sifting through false-positive alerts created by an over abundance of rules that your suspicious activity detection process becomes just as time consuming as doing it manually. In this case, you're clearly not getting a good return on your technology investment.

Duplicating alerts and efforts

Rules-based systems typically generate output reminiscent of the paper reports some FIs print from their core banking system to manually monitor specific channels or products, such as cash, check, ATM, ACH, or wire activity (refer to Figure 3-1 if you want a visual aid). And like their paper counterparts, rules-based systems have a tough time combining activity across these channels or products. Unfortunately, this often results in two or more separate alerts for the same activity for a given customer, because that customer's transactions broke multiple rules. Generating multiple separate alerts for a single customer's behavior creates two significant problems:

- **Reduced operational efficiency**. In addition to the time you need to review the alerts, duplicate alerts often trigger duplicate cases, with different departments conducting separate investigations of the same customer. This is particularly likely if you haven't merged your anti-fraud and AML efforts (check out Part II for information on why you should).
- **Reduced detection of crime.** Increasingly, the bad guys perpetrate crime across channels. Separating alerts by channel and reviewing them individually means you may not be able to connect the dots between the customer's various transactions. This affects your ability to speculate about the overall intent of the customer's activity and its degree of suspiciousness.

  In addition, creating multiple cases and submitting separate suspicious activity reports (SARs) for the same questionable activity may negatively affect the quality of the SAR information that regulators and law enforcement staff rely on.

Using behavior-based software

Behavior-based technology moves beyond simple rules-based software by adding fuzzy logic (which I define in the next section), artificial intelligence, and customer-behavior-pattern recognition. It uses data drawn from all of the FI's sources (both transactional and non-transactional) and allows you to configure parameters that relate directly to the behavior you're trying to detect. Figure 3-2 offers a simple diagram of how it works.

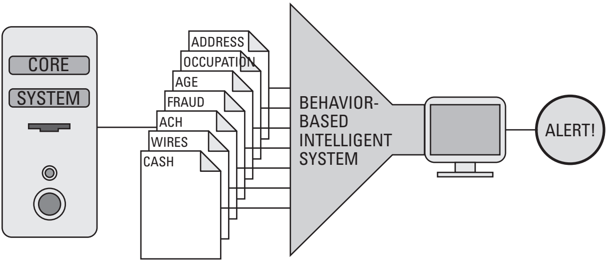

Figure 3-2: Behavior-based technology.

Behavior-based software reduces the number of false-positive alerts generated, eliminates the burden of fine tuning and adding rules in a rules-based system, and can have a significant impact on short- and long-term investment returns.

Focusing on fuzzy logic

Fuzzy logic offers a way to express uncertainty about the answer to a question like "Is this customer's behavior suspicious?” Unlike rules, where the only choices are “yes” or “no,” fuzzy logic provides an answer based on probability, giving an infinite number of possible answers in between “yes” and “no.”

Consider the following example: When asked if you expect it to rain today, if you follow a rules-based approach you would answer with a *yes* or *no* response. Applying fuzzy logic to the same question lets you answer with the probability of precipitation, ranging from 0 (no) to 100 (yes), with values in between representing the relative certainty of your answer.

Check out this example to see how fuzzy logic can help you fight financial crime: Imagine you want to track large wire transactions. With a rules-based system, you could ask, “Has Sally conducted any wire transfers over $3,000 in the past two weeks?” You receive a *yes* or *no* answer, with no way to indicate that she has made a wire transfer of $2,999.

Fuzzy logic offers more flexibility. You could ask, “Has Sally conducted any large wire transfers in the past two weeks, where a large transfer is $3,000 and a small transfer is $1,000?” If Sally only conducted wire transfers under $1,000, then the answer would be false. If she conducted wire transfers over $3,000, the answer would be true. And if she conducted a wire transfer of $2,000, the answer would be half true.

Using fuzzy logic instead of simple rules means you need fewer rules — every fuzzy logic question can replace dozens of rules — and eliminates a lot of the gray areas that crooks use to avoid detection.

Recognizing patterns

As the old adage goes, sometimes to catch a crook you have to think like one. Role-playing a criminal mastermind helps you figure out what someone's up to. As you examine customer behavior, ask, "Is it suspicious, or is it actually normal and legitimate behavior . . . for *this* customer?"

To help you figure this out, behavior-based software analyzes a set of data that combines static information, such as address, employment details, and financial information, with the metrics of a customer's activity, including average daily cash deposits, maximum monthly cash deposits, total weekly transfers out, average frequency between transactions, and so on. Using this data helps you understand each customer's pattern of behavior.

In addition, this approach allows you to compare members of similar peer groups (for example, customers with similar occupations or businesses in the same industry), which helps to identify unusual behavior.

Monitoring data with a behavior-based system

Behavior-based systems clarify the connections between your customers' behaviors and the indicators of risk for suspicious activity. They formulate a consolidated, customer-centric notion of the degree of suspiciousness of a customer's activity.

For example, suppose you're trying to determine whether or not a customer is structuring cash deposits so they fall just below the $10,000 reporting threshold. Before issuing an alert, a behavior-based system analyzes the available data using a combination of fuzzy logic, artificial intelligence, and pattern recognition, which involves the following:

- Searching for excessive cash deposits by determining whether the total cash deposited by a customer is excessive based on his normal pattern of transactions and compared with a peer group
- Calculating the risk that the customer is making deposits just below the $10,000 reporting limit
- Determining the frequency at which the deposits are made
- Reviewing the number of locations used for the cash deposits

This robust analysis indicates suspicious activity better than any simple if/then rule. And because behavior-based systems also provide a detailed breakdown of the evidence used to generate the alert, those responsible for reviewing alerts and investigating cases can better understand why the customer's activity may be suspicious.

Part IV

Ten Tips for Choosing FRAML Software

In This Part

- Bringing crime-fighting efforts together
- Focusing on customers and behaviors
- Getting the most for your money

Technology enables FIs to effectively manage risk and address competitive pressures. Having the right software makes all the difference when merging anti-fraud and anti-money-laundering (AML) efforts and in winning the war against financial criminals. In this part, I share a few tips for selecting your software.

Go All Inclusive

The whole idea of merging anti-fraud and AML efforts is to create one efficient, effective force against financial crime. Because risk and compliance concerns overlap, your software solution should allow you to consolidate all of your key risk and compliance management functions.

Don't look for a solution that simply produces alerts or produces an electronic version of the paper reports you already get from your core banking system. Instead, your software should integrate detection, alerts, investigations, case management, and compliance reporting. This helps ensure that all FRAML data, information, work flows, and reporting are centrally managed, and helps management and board members to see the status of all financial crime and related compliance activities across the organization.

Mind Your Data

FRAML can help you improve your data quality and streamline data management activities. Merging separate data sources results in access to more up-to-date, accurate, and enriched data for analysis and investigations. This means you spend less time looking for, and updating, customer data. Look for a software vendor that has deep expertise in data integration and provides a data model that has been developed specifically for financial services applications.

Break the Rules

Admit it: You've always secretly wanted to be a rule-breaker. Fraudsters and money launderers don't follow rules, so why be limited by using a rules-based system? Multiple alerts, duplicated efforts, false positives, rules explosions — who needs 'em? Behavior-based software greatly reduces these problems *and* allows you to monitor customer activities across the entire FI — through all channels and across all products, geographic locations, lines of business, and transaction types. Indulge your inner rebel, and break away from rules-based systems.

Make It Personal

Find software you can configure on a customer-by-customer basis. As you investigate and identify a particular customer's normal behavior, your system should allow you to adjust the alert parameters for that customer. This reduces the number of false-positive alerts and leaves you with more time to review and investigate truly suspicious activity.

Take a Customer-Centric Approach

Find a system that lets you see everything a customer is doing at a glance, without having to draw information from different external sources or look at transactions in isolation. Reviewing a customer's overall activity gives you a better idea of what he or she is up to and makes identifying suspicious behavior easier.

Let the System Do the Work

An ideal system will automatically update your watch lists in real time and scan customers and third-party vendors, leaving you free for follow ups and investigations.

Keep Up with the Times

Times change and so do criminals and their activities. Look for FRAML software that provides necessary upgrades as regulations and patterns change so you can keep pace.

Get More for Your Money

Seek a software vendor that provides value-added services such as core system integration and end-user training as part of the implementation. Proper training and documentation help you get the most out of your particular solution.

Kick the Tires on Technology (But Don't Forget to Look Under the Hood Too!)

Asking your technology vendor lots of questions helps you understand what the solution provides, such as a way for you to deal with things like repeat alerts on the same customer. But you also want to make sure it's easy to use. Manage your risk and make an informed decision.

Keep It Simple

Let's face it: Upgrading your system is pointless if your staff can't figure out how to use it. The whole point is to increase efficiency and effectiveness, which is tough to do if employees spend too much time figuring out the new system. Installing an easy-to-use system reduces employee stress, training costs, and makes everyone happier.

Compliments of Verafin

Suspicious Activity Reporting FOR DUMMIES®

Pre-order your free copy!

verafin.com/dummies