Strength in Numbers
Fighting Financial Crime with the Power of Cross-Institutional Detection & Collaboration

A Verafin White Paper
For many years, financial institutions (FIs) depended on spreadsheets and basic core banking system reports to uncover potentially suspicious activity. However, this approach was both inefficient and ineffective. Combing through endless pages of transactions and spreadsheet rows in the hope of spotting something unusual — it was like sifting through boxes of assorted puzzle pieces without even knowing how the finished puzzle looks.

In an effort to solve this problem, the first wave of AML technology solutions was introduced. These technologies, still in limited use, generally depend on the creation of rules. Rules are simplistic — essentially if/then statements. For example, if a customer makes daily cash deposits of $9000, then fire an alert. At first, this was a welcome step forward from spreadsheets and core reports. However, their lack of sophistication was (and is) their downfall.

As everyone in the AML and fraud detection industry knows, the criminal landscape is ever-changing. Criminals are always adapting to an FI’s defenses, quickly making rules ineffective and outdated. As a result, more and more rules are created. Before long, a once concise set of rules becomes a continually-growing, unmanageable workload as an FI struggles to keep pace with the rapid rate of change. In a short amount of time, the mass of rules required to uncover crime is no longer sufficient or manageable; more and more false alerts are generated, creating a daily activity alert overload and destroying the efficiency these technologies were supposed to provide. These solutions became outdated trying to apply a rigid, black-and-white paradigm to a world with a full spectrum of color. It was time to move forward.

The next generation of AML solutions looked to utilize cutting-edge technological advances in artificial intelligence. It was in this environment that Verafin delivered its innovative FRAML (FRAud + AML) solution, using progressive behavior-based analytics to help FIs uncover out-of-the-ordinary customer activity. A behavior-based approach was a significant step forward from what were by now outdated rules-based systems.
With behavior-based technology, the customer and their patterns of activity are central to uncovering the truly unusual. Transactional data and customer profile information (such as age, address, occupation/industry, etc.) are analyzed for behavior that is abnormal. These abnormalities generate an alert focused on unusual behavior for the customer, meaning time is not wasted reviewing activity already accepted as representing minimal risk.

So, where are we now?

Once again, financial crime prevention technology is having trouble keeping pace with criminals' ability to adapt and modify their behavior. At first glance, there are a number of competing products offering a very similar set of features that check off a number of standard BSA/AML requirements:


However, scratch the surface of many BSA/AML solutions and a number of deficiencies appear. We know that criminals are chameleons — they excel at adapting to technology to avoid detection. Today, they are morphing into something bigger and scarier than ever before, while much of the technology used to stop them is largely stagnant.

The new breed of criminal

Today's criminal is a team player. They are members of innovative criminal enterprises, growing their activity to unprecedented levels of sophistication.

The types of activity these criminal enterprises are involved in and the number of lives they ruin along the way makes them even more frightening. This is no cops and robbers sketch. These enterprises are comprised of truly villainous individuals who use the U.S. financial system to perpetrate terrible crimes against humanity — on a global scale. Two of the most prominent examples are:

○ **Financing global terrorist organizations such as ISIS and Boko Haram.**
  These organizations are responsible for sickening levels of violence, resulting in the deaths of thousands of innocent people.

○ **Funding human trafficking networks.** These traffickers are responsible for the forced labor and sexual exploitation of millions of victims every year.

The U.S. financial system is their conduit. The Treasury Department's 2015 *National Terrorist Financing Risk Assessment* stated that, “broadly speaking, based on an analysis of U.S. law enforcement investigations and prosecutions relating to TF [terrorist financing], two methods of moving money to terrorists and terrorist organizations have been predominate in the convictions and cases pending since 2001: the physical movement of cash and the movement of funds through the banking system.”
Given the scale of terrorist financing and human trafficking networks, a number of smaller institutions dismiss this as a problem that only affects the country’s largest FIs. This line of thought is both incorrect and dangerous. All FIs are potential targets for this new breed of criminal behavior.

With top tier banks coming under increasing regulatory scrutiny from FinCEN, criminals are looking elsewhere in an effort to move their illicit funds. “If you really tighten things up at the top of the industry, people who want to launder money will search for other entry points,” says Ralph Sharpe, a former OCC enforcement director. “So the emphasis on compliance trickles down to smaller banks.”

In a recent white paper on Section 314(b) of the USA PATRIOT Act, Chris Swecker, retired Assistant Director of the FBI’s Criminal Investigative Division and former Global Security Director at Bank of America, makes direct reference to criminal enterprises targeting smaller institutions. “Many Criminal Enterprises prey on credit unions and community banks knowing that resources are scarce and strategies to link or ‘cross-reference’ crime ring activity are too often reliant on manual processes. They also know that due to intense competition between institutions, sharing data is not a high priority for bank executives who quite understandably are focused on the bottom line. In this environment, collusive criminal activity targeting multiple institutions thrives and prospers.”

The futility of combating the new breed of criminal in isolation

In this new criminal environment, FIs are dealing with a problem of isolation. Criminal enterprises excel at learning how FIs defend themselves. They understand most FIs will discover excessive and highly unusual behavior, so their activity must be subtler; they must be more intelligent. As a result, criminals evolved away from their previously siloed behavior and are now using the isolation of individual FIs to fund their paydays. Why use one bank when you can hide activity across ten of them?

Here are examples that help illustrate the problem of searching for financial crime in a silo:

Micro-Structuring

John is a customer at National Bank. Every week he deposits:

- $3000 in cash at the Main Branch ATM

Nothing particularly unusual; business is going good for John. At one point the bank’s transaction monitoring software generated a low risk alert on his activity. After a quick look at his history, the investigator saw nothing warranting an investigation and moved on to other higher risk alerts assigned to her. The team at National Bank has never opened an investigative case on John.
Of course, there is a good chance they would be concerned if they knew every week he also deposited:

- $4000 in cash at Your Regional CU
- $4500 in cash at Skyline Horizon Bank

That puts John’s cash deposit activity, across three FIs, at $11,500 per week. Clearly, John is structuring his activity across multiple FIs to avoid suspicion and reporting. The problem is, stuck in institutional silos, none of the FIs have any sense of the larger picture.

What is he really doing here? Why is he structuring deposits to move this kind of money every week?

**Common Wire Receiver**

Structuring cash deposits is only the start of the risk that surrounds John. In addition to the cash deposits, John transfers $10,000 from each of the three FIs to multiple accounts at Red, White and Blue Bank in Manhattan each month.

What none of these FIs know is that John is just one part of a much larger team of criminals. In addition to John, who is moving $30,000 per month in total, there are four other individuals also structuring cash deposits and wiring money to the same accounts at Red, White and Blue Bank.
Strength in Numbers
Fighting Financial Crime with the Power of Cross-Institutional Detection & Collaboration

What happens to the money once it is received at Red, White and Blue Bank? None of the FIs has any way of knowing. If only they knew the money is being wired to overseas accounts in Turkey, Armenia, and Azerbaijan; alarm bells would be ringing very loudly.

These examples illustrate how the majority of today’s AML and fraud detection technology has reached a limit in terms of its ability to help stop financial crime. If an FI cannot detect the presence of cross-institutional criminal activity or work with other institutions to share relevant information, how can they stop it? Spoiler alert: they can’t.

The new approach
Traditionally, FIs were restricted to a limited view of their customer’s activity. Within the silo of an individual institution it is nearly impossible to truly know your customer. To make things even more difficult, many FIs not only are restricted to an institutional silo, their efforts to detect financial crime are further hampered by internal, departmental silos. The left hand is unaware of what the right hand is doing.

Today’s criminal enterprises recognize these struggles. In addition to spreading their activity across multiple transaction channels, they are manipulating multiple FIs to facilitate their criminal activities. Investigators are left wondering — am I seeing the full picture or only a small slice of what this person is doing? An incredible amount of time is then spent on what often turns out to be unnecessary investigation. In a 2016 Wall Street Journal article entitled, “Losing Count: US Terror Rules Drive Money Underground”, Jaikumar Ramaswamy, a Bank of America Corp. compliance executive and former federal prosecutor, touched on this frustration, “I’m surprised at how much of my time is spent not focusing on the guilty but chasing the innocent.”

Fortunately, technology provides an avenue to combat this trend. Unlike what many of our grade school teachers told us, the time has come to get our heads into the cloud.

Over the past five years, cloud computing has experienced incredible growth and continued momentum. The significance of this technological progression on financial crime fighting is enormous.

Cloud technology provides a powerful means of breaking out of restrictive silos and, in turn, enables a new way of thinking about how to successfully protect against today’s financial criminal. As criminals break away from single institution attacks and execute their schemes across multiple FIs it is no longer effective to analyze data in isolation.

Enter FRAMLx: Cross-institutional analysis and collaboration
What is FRAMLx?
As discussed, the industry has reached a limit regarding what can be found when confined to analyzing data within four-walled silos. Today’s criminals know this and have made the necessary adjustments to remain undetected — while making away with more money than ever before. Enter Verafin’s FRAMLx (the x standing for cross-institution) solution.
FRAMLx is the next evolution in financial crime detection. This game-changing innovation leverages the advantages of Verafin’s cloud environment, the Verafin Cloud. Since being introduced in 2009, over 1300 FIs have migrated their customer data into the Verafin Cloud. Every day, in the cloud environment, Verafin analyzes over 100 million transactions for FIs with over $1 trillion in collective assets.

With FRAMLx, Verafin applies advanced, behavior-based analytics to cross-institutional data. While an institution’s specific data remains private at all times, FIs are alerted to patterns of unusual activity affecting multiple institutions. It then provides the means to collaborate directly with other similarly affected institutions.

**Verafin FRAMLx Alert Example**

**The growth of cross-institutional collaboration via 314(b)**

Advanced data analysis and the resulting alerts are just one part of the FRAMLx advantage. The other is collaboration, providing investigators with the ability to work one-to-one with colleagues at other FIs to gather vital insight into a much larger picture of their customer’s activity.

Section 314(b) of the *USA PATRIOT Act*, passed by Congress and signed into law on October 26, 2001, provides FIs with a powerful ability in the fight against financial crime. Once registered with FinCEN, FIs can share information with “safe harbor” from civil liability to the “full extent provided in subsection 314(b) of Public Law 107-56 [the *USA PATRIOT Act*].”

Jennifer Shasky Calvery, Director at FinCEN, spoke to the importance of 314(b) collaboration and the intersection between fraud, money laundering, and terrorist financing in her remarks to the Securities Industry and Financial Markets Association Anti-Money Laundering and Financial Crimes Conference in 2014. “[S]haring information between financial institutions is also critical. The 314(b) safe harbor provisions permit financial institutions to share information under
the 314(b) program as it relates to transactions involving proceeds of suspected fraud and other specified unlawful activities (SUAs), the predicate offenses for money laundering, if the financial institution suspects there is a nexus between the suspected fraud or other SUA and possible money laundering or terrorist financing activity. And I can tell you as a former money laundering prosecutor who has handled several fraud related money laundering cases, anytime you have funds that you suspect are related to fraud in or moving through your financial institution, you should also be suspicious that transactions made with those funds may involve money laundering."

Since 2002, FinCEN has received over 19,500 SARs that explicitly reference the sharing or attempted sharing of information — the number is even more remarkable considering "an undetermined number of SARs may also have been filed as a result of the filing institution's involvement in a 314(b) communication, even though there is no specific mention of 314(b) in the SAR narratives." (FinCEN's 2013 SAR Activity Review – Issue 23)

The FRAMLxchange Secure 314(b) Collaboration Network

The FRAMLxchange network is registered with FinCEN for 314(b) information sharing as an association of financial institutions.

Verafin FRAMLx Collaboration Example

A 314(b)-registered FI can join the FRAMLxchange network at any time. The FRAMLxchange Secure 314(b) Collaboration Network enables registered investigators to share information using collaboration tools available within the secure Verafin application environment.

"Information available to the financial institutions via 314(b) allows the financial institutions the opportunity to more effectively investigate potential suspects and their activities. Financial institutions that participate in the process, as well as law enforcement agencies, benefit from the increased collaboration and information sharing that the FRAMLxchange network provides."
Strength in Numbers
Fighting Financial Crime with the Power of Cross-Institutional Detection & Collaboration

enforcement that see SARs filed by one or both institutions, can obtain a more comprehensive picture of the subject's accounts, funding mechanisms, and activities. With the enhanced information available to institutions that participate in the 314(b) process, institutions can make better informed decisions and strengthen their compliance efforts.” (FinCEN's 2013 SAR Activity Review – Issue 23)

FRAMLx: How it works

Analysis and alerts

Every day customer data (transactional and non-transactional) from over 1300 FIs across the country is uploaded into Verafin’s secure cloud environment. With FRAMLx, each FI’s data remains private.

Profile information (Tax ID and other identifiable factors) is examined for matches. For example, John (SSN: 123-22-1234) at National Bank is the same person as Jon (SSN: 123-22-1234) at Your Regional CU due to an SSN match. Once multiple instances of a person are found, they are analyzed to determine if they have alerts or unusual activity across multiple FIs.

If unusual activity is discovered, an alert is generated at the FI where that person is a customer. From this alert, a user can start a collaboration with the 314(b) contact at the other FI. Through collaboration, a user can discover the information necessary for them to make the best decision on how to proceed.

A FRAMLx alert will generate at an FI if a shared customer is performing unusual activity at another institution on the FRAMLxchange network.

- **No information, beyond the fact that the customer is performing unusual activity at the other FI(s), is automatically shared in the alert.** Information is only shared voluntarily via collaboration. No institution has access to another institution's data.

- **Collaboration is private and strictly one-to-one.** For example, if ABC Bank collaborates with XYZ Bank, only ABC Bank and XYZ Bank can see that conversation. It is not visible to any other member of the FRAMLxchange network.

Collaboration: Fighting Crime, Together

Collaboration is a vital component in the fight against financial crime. Removed from an institutional silo, investigators collaborating with peers across the FRAMLxchange network can choose to share new and important customer data. This results in more thorough and effective investigations, greater efficiency, and improved decision making. It is important to note that FRAMLx facilitates teamwork amongst peers — no information is shared automatically. A FRAMLxchange member only shares the information they voluntarily choose to through one-to-one collaboration.
Within the Verafin application, a FRAMLxchange member can exchange messages with any other FRAMLxchange member or 314(b)-registered contact. There are a number of ways to initiate a collaboration:

- **FRAMLx alert.** This option is available if Verafin is analyzing an FI’s customer data. A FRAMLx alert generates on a customer based on unusual patterns of activity across FIs. The alert provides the contact information for the other FIs that share the relevant customer. With a mouse click, a user can ask for more information on the customer and their activity.

- **Wire and/or ACH activity.** This option is available if Verafin is analyzing an FI’s customer data. Users can collaborate about a particular wire or ACH transfer with the FIs involved in those transactions.

- **Any place within Verafin.** A user can start a collaboration with any other 314(b)-registered contact at any time. If that contact is not already a FRAMLxchange member, they will be sent an email asking them to join the FRAMLxchange. The email also indicates a new collaboration is waiting for them.

Collaborations between FRAMLxchange members are not visible to the rest of the network. While a collaboration can be sent to any 314(b)-registered contact, that person can only view the collaboration by joining the network. The Verafin application scans the 314(b) list numerous times daily to ensure the creation, sending, and receipt of messages are strictly restricted to participants at 314(b)-registered FIs.

As an added benefit, every collaboration is logged and reportable for auditing purposes. Numerous automated collaboration reports are also available.
Strength in Numbers
Fighting Financial Crime with the Power of Cross-Institutional Detection & Collaboration

Security

All FI data is securely housed in the Verafin Cloud environment, where integrity and confidentiality are strictly maintained. Security features of the Verafin Cloud include:

- **Encryption at rest**: The Verafin Cloud infrastructure is maintained in a secured Tier IV Gold facility where FI data is encrypted and securely stored.

- **Encryption in transit**: All file transfers to the Verafin Cloud use NIST-certified secure file transfer encryption, teamed with Transport Layer Security (TLS) and Advanced Encryption Standard 21 (AES) 256-bit encryption on trusted channels, and are protected by firewalls that are locked-down to only authorized customer networks or environments. Access to the Verafin application is facilitated through secure HTTP (HTTPS) connections based on unique customer usernames and passwords for authorized personnel only.

- **24 / 7 / 365 monitoring**: The Verafin Cloud and its data are monitored 24/7/365, which ensures threat management is in place. An intrusion detection system (IDS) and a security information event management (SIEM) system continuously monitor for anomalous activities.

- **Backups and disaster recovery**: All data in the Verafin Cloud is regularly backed up to a disaster recovery (DR) environment. Data is replicated on an hourly and nightly basis between the production environment of the Verafin Cloud and the DR center (separate from the physical storage location of the production data). Verafin’s Disaster Recovery Plan (DRP) outlines both the recovery time objective (RTO) and recovery point objective (RPO), and Verafin performs regular testing of this DRP to verify recovery times and the integrity of customer data.

The real-world power of FRAMLx

Faced with today’s sophisticated financial criminal, FRAMLx and cross-institutional collaboration are essential tools.

Becky Robertson, Senior Vice President / Director of AML Compliance at South State Bank, offered her thoughts on the benefits her institution is experiencing. “It’s an incredibly powerful tool. FRAMLx takes the guesswork out of our investigations. When we see an alert, we know right away this is a person we need to look into. We don’t have to waste time digging around, trying to figure out who to contact for more information. And the information we share gives both our institutions a view of our mutual customer we could never achieve without working together.”

Using FRAMLx and the collaboration opportunities provided by the FRAMLxchange network, FIs have an incredible opportunity to stop financial crime and improve investigative efficiencies.
Thinking back to the examples (Micro-Structuring and Common Wire Receiver) shared earlier, let’s consider another example — this time with FRAMLx available to the FIs:

Jane, the BSA & Risk Officer at Carolina Sunset FCU, is reviewing her FRAML alerts in Verafin and notices a high risk FRAMLx alert on George Raymond. George is a 22 year old Plumber and a customer of the bank for 2 years.

Reviewing the alert evidence, she sees that George is a potential Risky Entity. Jane knows this means another FI on the FRAMLxchange has dealt with George and categorized his activity as unusual. She scrolls to the alert’s Transaction section and sees a $9000 deposit. Checking the Behavior section of the alert, Jane sees that in George’s two years as a customer, he has never made a single deposit for more than $2500.

Jane next checks the Institutions section of the alert. This section shows her the names of the other two FIs (and the verified 314(b) contact names) that have had dealings with George and caused the FRAMLx alert to generate.

She clicks the Collaborate icon for TX Members FCU, the first FI in the list, and types her message:

```
Hi, I’m contacting you to request information about potentially suspicious activity.

Customer Name: George Raymond
SSN: 709-00-5566
Activity: $9000 deposit on May 13, 2016

We are investigating a customer of ours named George Raymond. He made a highly unusual (for him) deposit yesterday. It appears he is also a customer at your bank.

Can you tell me any of the following about George:
Do you have any BSA/AML concerns?
Are there any unusual transactions?

Thank you.
```

14-May-2016 14:53:09 - Jane Stacks

She sends the collaboration message to TX Members FCU and then sends a similar message to Golden Gate Bridge Bank, the second FI in the list.

Later that afternoon, Jane receives a response from Kelly at TX Members FCU,

```
Jane,

George was a customer here. He had a loan with us and was behind on his payments.

He withdrew most of the loan and disappeared. We made multiple attempts to contact him. Yesterday, based on his activity, we closed the case we had open on him.
```

14-May-2016 15:08:15 - Kelly Rivara
Concerned, Jane responds to Kelly,

Thanks Kelly.
That is helpful. In the two years he has been a customer here, he never made a deposit anywhere near this amount.
Now he has applied for a loan to purchase a car from a man named Thomas Jenkins. The unusual deposit, followed by a loan request feels very suspicious, so the info you provided is very timely.

Minutes after sending her message, Kelly responds,

Now, that’s very interesting.
I had a look after reading your message and it appears we have a case open on a Thomas Jenkins (SSN: 123-00-0987).
We thought we might have to charge it off but then a woman named Mary Jackson paid it off.

With this information, Jane has what she needs to open a case in Verafin and files a Suspicious Activity Report (SAR) with FinCEN.

The story outlined above is based on a real-life loan fraud ring discovered by multiple FRAMLxchange members collaborating in Verafin.

The size and scope of this crime ring is staggering, with more affected FIs being discovered regularly.

Here is a quick overview of the numbers, as they stand today, to help illustrate the scale of this criminal enterprise:

- 137 collaborations
- 29 FIs
- 16 Risky Entities
- 10 states

Even more alarming, these numbers may only represent a piece of an even larger scheme — it is unknown how many institutions, not currently collaborating in the FRAMLxchange network, are victims of this criminal activity.
Joining FRAMLxchange

There are two ways a 314(b)-registered FI can join the FRAMLxchange and collaborate with other members of the network:

- Go to https://framlxchange.verafin.com/ and complete the sign up process.
- Receive an invitation from a 314(b)-registered Verafin user and follow the steps outlined in the invitation.

There are a number of benefits to joining the FRAMLxchange network, including:

- **No data integration required.** There is no data export or import, or IT resources required to access or use FRAMLxchange.
- **Connect with peers.** FRAMLxchange creates a network of peers collaborating to improve investigations and decision-making.
- **Secure and compliant.** Verafin’s secure application environment assures confidentiality, processing integrity, security, and privacy. Four-times daily scanning and verification of the 314(b) list ensures that FRAMLxchange members are valid, registered 314(b) contacts at all times.
- **Comprehensive audit trail.** All collaborations are logged and reports can be easily created for all 314(b) requests and responses.

Conclusion

Analyzing data within the confines of an institutional silo is problematic and limiting in today’s environment as criminal enterprises stretch their activity far and wide. FRAMLx and collaboration via the FRAMLxchange network help you strengthen your customer knowledge and improve the efficiency of your investigations into potentially suspicious activity.

This forward-looking technology helps FIs break free of their restricted view of customer activity. Verafin’s advanced cross-institutional analytics empower a network of collaborators to work together. The result is criminals can no longer hide their unlawful activity by manipulating multiple FIs.

“Before FRAMLx, collaboration was like fishing in the dark. We’re more likely to send a request now. Unless I saw suspicious activity between accounts, I didn’t know if a member only had an account at our institution versus any other institutions,” describes Kris Ockenfels, BSA Compliance Officer at University of Iowa Community Credit Union. “With FRAMLx, I get the 314(b) contact at the other institution and I know that they have our member at their institution, so it’s relevant to ask them to share information.”

In the fight against money laundering, terrorism, and the fraud tied to these criminal offenses, FRAMLx is a significant step ahead.