NICE
ACTIMIZE

Insights Article

The Future of Information Sharing Across the Financial Crime Landscape: Is Your Organization Ready?

Introduction

It's no secret that the way the financial industry is sharing information today is outdated. Many of today's AML and fraud systems are often siloed and burdensome. When suspicious activity is found, there's limited access to data from the rest of the organization, let alone other organizations, to contextualize any red flags and confirm suspicious activity.

Meanwhile, criminals have the exact opposite situation. They're sharing intel and resources that allow them to expand their criminal operations and evade detection. They're smart and able to quickly understand and exploit vulnerabilities, and often well-funded, allowing them to utilize new technologies to aid in their money-laundering operations.

This is where information sharing, regulatory reform and advanced detection play a crucial role.

— Adam McLaughlin
Global Head of Financial Crime Strategy & Marketing, AML, NICE Actimize

Recent Developments in Financial Crime Information Sharing

Information sharing amongst financial services organizations (FSOs) to prevent crime isn't new. There have been regulatory developments with regards to private-public and private-private data sharing since the U.S. passed the Patriot Act in 2001, with the introduction of 314(b). Since then, other legislation has been introduced around the globe, providing a gateway to sharing information. This legislation includes Section 2, Article 39 of the 4th Money Laundering Directive in the EU and Chapter 2, Section 11 of the UK Criminal Finances Act 2017. The main issue with this legislation is that it's voluntary, with banks needing to jump through several hoops to share information using the legislation, resulting in the legislation hardly being used. Over the past decade, we've seen a wave of new private-public intelligence sharing partnerships being formed, starting with the Joint Money Laundering Intelligence Taskforce (JMLIT) in 2015. The map below highlights several of these recent public and private information sharing partnerships.

Map of Existing AML Private to Public Information Sharing Partnerships

These partnerships have allowed FSOs and government agencies to share information about entities or individuals under investigation, as well as share intelligence about new financial crime typologies. This improves financial crime detection by enhancing monitoring, identifying and freezing illicit assets and bringing offenders to justice in a more timely manner. A great example of this is JMLIT.

Since its inception, according to the U.K. National Crime Agency, "JMLIT has supported and developed over 500 law enforcement investigations which have directly contributed to over 130 arrests and the seizure or restraint of over £13m."

Over the same period, while private-public partnerships were opening the doors for improved information sharing, GDPR came into effect across the EU, protecting the rights of data subjects by restricting the sharing and use of personally identifiable information (PII) outside of its intended use. This has presented unique challenges for FSOs that both need to comply with current data privacy regulations, but also want to reduce their risk by cracking down on financial crime.

Challenges with Current AML Data Sharing Practices

Several limitations with our current data-sharing practices still exist that cap our effectiveness in fighting financial crime.

These limitations include:

- The majority, if not all, of the existing private-public partnerships are restricted by jurisdictional borders, resulting in them only having members from in-country public and private organizations. This continues to allow criminals to circumnavigate discovery by using bank accounts in multiple countries.
- Existing private-public partnerships are a great step in the right direction. Information sharing is much more bidirectional than it's been at any point before these partnerships existed. However, there are still areas where information sharing isn't free-flowing and bidirectional.
- Except for the U.S. with the Patriot Act Section 314(b), very few countries have taken any steps to provide a clear legal gateway for private-private AML information sharing. For the Patriot Act 314(a) and (b), the process for applying that statute is convoluted.
- With GDPR laws, what information can be shared and by what means is limited, which restricts cross-organizational sharing and leaves out potentially crucial information.
- FSOs are fined for under sharing information with authorities, however, there are no penalties for oversharing. This results in FSOs like banks, funds and exchanges filing what are often referred to as 'defensive filings' or 'defensive SARs' to ensure they are not fined later.

The Future of Financial Crime Data Sharing

The recent increase in private-public partnerships is only a first step in improving the financial crime industry's effectiveness through data sharing. In the next few years, our industry must move toward forming a consortium – a coming together of organizations to share information – to improve the industry's overall effectiveness. This is one of the only strategies that will level the playing field with that of criminals, making it critical that we take steps to make it work.

There are three key consortium models the industry could eventually pursue – the information-sharing model, detection optimization model and utility model.

The information-sharing model

The information-sharing model relies on improved information sharing through private-private and private-public partnerships. With this model, you would work with other organizations to exchange client profiles, behavioral information, suspicion information and information about newly seen typologies. Conceptually, it's one of the simplest models to start pursuing. However, for this model to be feasible, shortcomings in current data-sharing policies will need to be addressed. This includes paving a legal path for private-private information sharing and clarifying tipping off policies and suspicious activity reporting requirements.

The detection optimization model

The detection optimization model uses shared collective learning to increase the understanding of criminal behavior, optimize existing detection models and develop new typologies that keep up with changing threats. This shared collective learning can be done with non-PII data sets. Under this model, organizations that are part of the collective would share analytical findings with other organizations within the collective. This helps ensure the collective's detection systems are always up to date and always monitoring the latest threats, while eliminating legitimate behavior variations, such as increased transactional activity during seasonal holiday periods. This model will need governance processes in place to prevent inaccurate learnings from being shared and to maintain the overall effectiveness of the monitoring systems. The technology needed to implement this model is available today – organizations just need to be willing to adopt this model and work together to make it a reality.

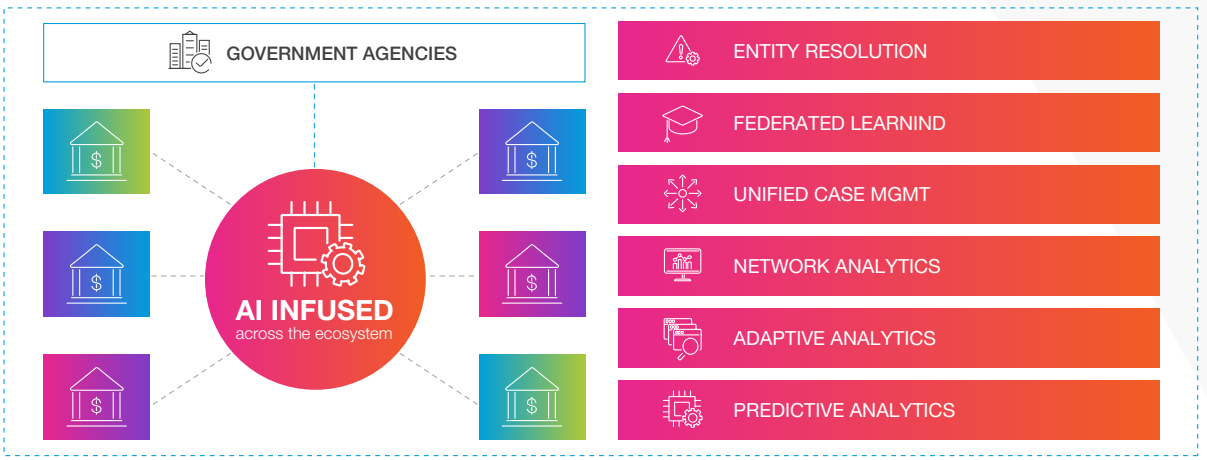
The utility model

The third and final model, the utility model, encompasses a single monitoring and detection system that evaluates activity across a network of organizations. Under a utility model, connected organizations can identify networks of connected accounts and entities, making it easier to detect criminals trying to hide across multiple organizations. This model can also be applied to KYC and screening processes. The main challenge here is extending the model beyond jurisdictional borders as regulations vary. A great example of this model is the Transaction Monitoring Netherlands (TMNL) project – a project where five of the largest banks in the Netherlands have come together to use one transaction monitoring system. This program's proof of concept started in 2021 and is the first of its kind in the world.

The Ultimate Model

All three models will play a part in helping drive toward better information sharing. Of the three consortium models, the one that would be most effective in fighting financial crime is the utility model. The utility model enables FSOs to look at a customer's behavior holistically – looking not just at the transactions that go through their entity, but also at the transaction flows across several entities. It would prevent criminals and criminal networks from using multiple accounts, across multiple organizations, with multiple distinct behaviors to avoid detection. It would also allow financial crime professionals to detect new typologies quicker, and use industry learnings collectively to fight organized criminal groups.

Utility Model Approach to Consortium for Anti-Money Laundering Information-Sharing



While this model is the ultimate model for crime detection, there are still several challenges to overcome before it can be mainstream. For this model to be successful, organizations would first need to break down silos in their organizations and place a strong emphasis on entity resolution. If we cannot resolve entities internally, we cannot expect to be able to resolve entities with other FSOs. To achieve the most effective outcome, organizations must also employ technologies such as artificial intelligence (AI) and machine learning (ML) to perform network analytics, accurately identifying suspicious activity across the network.

Steps to Prepare for Future Consortium

Before the industry can expect to increase information sharing, there must be improvements in current information sharing practices using gateways available in current legislation and solutions available in today's current technology offerings. The biggest challenge in this is breaking down organizational silos to gain a better understanding of customers and their associated risks.

Entity resolution

Entity resolution is a critical investment FSOs need to consider when preparing for a consortium. For a consortium to be effective, we as an industry must be able to link accounts owned by the same individuals with the same identifiable information together to be able to monitor each individual's behavior contextually. If this cannot be done between different lines of business, how would it be done with other banks globally? Take the following as an example – we have multiple entities with similar names, addresses, and phone numbers:

The Power of Entity Resolution

Are these entities the same individuals or are they different? If an organization is unable to understand whether these are the same entities, that organization is introducing unnecessary risk in their business any time they make a decision on these entities. They cannot be confident if they don't have all the information they need. In the event of a consortium approach, that organization is now introducing risk to all organizations involved in the consortium. Proper entity resolution should look not only at names but also at attribution data - such as addresses, phone numbers and email addresses - to help ensure there is a true and precise profile for each customer that is reflective of their real risk. Proper entity resolution enables more accurate detection by making and understanding connections across networks. With this resolution and the ability to connect two seemingly separate entities, you can leverage network analytics to monitor activity between the entities and detect abnormal behaviors that were not visible before.

In this example, we can see that all four original entities are actually connected. By resolving the entities, we can now look at Mary's risk more holistically because we can see all of her accounts and connections. We can also monitor activity across Mary's whole network to detect any potentially suspicious activity – such as the circulation of funds, structuring activity and/or burst payments to or from the corporation or the connected parties, who were not previously associated with Mary. Providing greater context to the parties and their activity dramatically improves effectiveness in the fight against financial crime.

Improving internal technology/information sharing practices

When looking to improve your current tech stack, where do you start, especially with an idea as large as consortium as the end state? FSOs must break this technology roadmap into smaller, more tangible steps to scale toward a consortium.

FSOs should aim to progress along the following stages of technology, building upon each subsequent layer:

Anti-Money Laundering (AML) Technology Layers

Independent entity-specific learning

Independent entity-specific learning is the current state of many FSOs today. In this stage, each entity within an organization operates in its silo, with little access to data from other branches. It's up to that branch, and that branch alone, to detect if a customer's behavior is suspicious. Organizations should understand the risk posed by their customers across the entire customer lifecycle. We call this Customer Lifecycle Risk Management (CLRM). Being stuck in a siloed approach, learning from a limited pool of data, makes CLRM much more difficult because FSOs have limited or no visibility of the customer's entire profile. With independent entity-specific learning, learnings from the system are more likely to be inaccurate and not sufficient to manage the risk posed by the customer, as the learnings are based on a limited set of information and do not look across the entire customer lifecycle.

Federated learning

Federated learning uses machine learning and multiple data sets from across multiple organizations to train and optimize models being used to monitor and detect money laundering, helping to investigate more financial crime. This stage of technology allows an organization to retain control of its independent detection system but benefit from collective learning across multiple connected systems. This is an easy to implement, accessible technology that uses shared learning to benefit the collective. By sharing model performance, the collective can ensure all systems are detecting the right threats and are optimized to ensure they are always performing at their best.

Intelligence level investigations

Intelligence level investigations take federated learning one step further. At this technology level, we move from just ensuring detection systems are optimized in detecting suspicious behavior to including 'normal' deviations in behavior in the analysis. This further enhances the accuracy of detection systems because we look at how this normal behavior changes based on current events, seasonal variations and life changes. Christmas and Hannukah gift shopping are good examples of seasonal variations that need to be accounted for. Leveraging AI and machine learning becomes especially important at this technology level. Ideally, organizations at this level would share normal and abnormal behavior intelligence changes across industry, which would help all organizations operate with always-optimized detection models.

Suspicious entity sharing

Suspicious entity sharing is the stage of technology development where an organization moves from just identifying suspicious behavior to working with other financial service organizations to determine if they too are investigating the same entities. Suspicious entity sharing enables our industry to come together to deliver more accurate decisions and escalate appropriate SARs more quickly. It does this by compounding an action, that may not be categorized as suspicious in one account, with the client's behavior across multiple cross-institutional accounts, potentially turning this non-suspicious event into a suspicious event. It's important to note that, at this stage of development, FSOs are not necessarily sharing all transaction information for all clients.

Cross-financial institution networks

In the final and most advanced technology layer, data is consolidated from several FSOs and analyzed together in one place. Creating this centralized view allows networks of transactions and counterparties to be monitored with significant accuracy, increasing visibility into the circulation of funds across multiple organizations. This improves the effectiveness of identifying organized crime groups and truly suspicious activity, while preventing criminals from hiding their illicit activity by crossing borders or opening accounts across multiple organizations, potentially with synthetic IDs or using mules. It is the ultimate end state in terms of financial crime prevention technology and ideal for finally turning the tide against criminals. This approach could be applied at a jurisdictional or cross-jurisdictional level. The more organizations that connect to a network, the more effective that the cross-institutional network will be.

The key for most organizations today will be to focus on moving one step up the technology ladder and, by using technology to break down internal silos, work toward a single view of the customer and their risk. By doing this, organizations will progress in terms of preparation for a consortium approach in a scalable way.

SEE HOW NICE ACTIMIZE CAN HELP >
