Choosing a detection and investigation solution for financial crime

5 key considerations for selecting the technology that's best for you

LINKURIOUS

Index

LINKURIOUS

Introduction

Financial institutions, governmental agencies and other organizations working to counter fraud, money laundering, corruption, and other financial crime today depend on large sets of heterogeneous data to detect and investigate suspicious activity. The legacy systems many organizations still use often struggle to efficiently pinpoint anomalies within the data.

False negatives continue to be a problem when using legacy systems, leaving too much criminal activity undetected.

A major challenge that has emerged is a high level of false positives—up to 95%[1] in AML use cases. The result is that most of investigators' efforts end up concentrated on non-fraudulent or otherwise non-criminal activity, wasting human and financial resources. On the other hand, false negatives continue to be a problem when using legacy systems, leaving too much criminal activity undetected. In the case of fraud in particular, this can result in very large financial losses: according to the ACFE, the average loss per fraud case against businesses is $1.78 million.[2]

This white paper explores in detail the key characteristics of effective detection and investigation solutions. Broken down into several criteria, we examine the capabilities, strengths, and weaknesses of different types of anti-financial crime solutions. Whether you're looking to add network analysis capabilities to your existing stack, or looking to roll out a full new financial crime detection and investigation solution, this guide will help you more clearly navigate the technology landscape and help you identify which tools are best suited to your needs.

With a large market offer that includes emerging technologies, this guide looks at the main points of consideration and comparison. What criteria should you use to decide if certain technologies or product features meet your team's needs? What questions should you be asking about your tech stack as you decide what to add or replace?

This guide explores in depth the performance criteria of financial crime investigation solutions for five key categories:

- → **Detection of suspicious networks**
- → **Ability to adapt to changing needs**
- → **Integration with 3rd party tools**
- → **Cost of ownership**
- → **Exploration performance**

[1] https://www.reuters.com/article/bc-finreg-laundering-detecting-idUSKCN1GP2NV

[2] https://www.acfe.com/about-the-acfe/newsroom-for-media/press-releases/press-release-detail?s=2022-RTTN-launch

The 5 key criteria for choosing an anti-financial crime solution

Detection of suspicious networks

Financial crime detection is dependent on networks. Criminals work in organized groups, laundered money is transferred through complex webs of bank accounts and financial vehicles, and chasing down fraudsters can involve navigating through webs of hundreds of accounts or pieces of personally identifiable information to find the connections.

Detection solutions have historically made it possible to set up detection and aggregation rules relating to a single entity, such as a person, a transaction or a company. These are considered “simple” rules. Criminals have been able to structure their activities in such a way as to make them undetectable if considered as isolated signals, since simple rules focus on single entities. For this reason, conventional approaches still fail to automatically detect suspicious networks.

More recently, various solutions have sought to improve the performance of simple rules using machine learning. But only newer techniques based on graph analytics can natively detect suspicious networks.

Network detection categories

No network detection

These solutions can only detect isolated entities, not networks. Tracking down links within the data is possible, but more distant connections become exponentially slower to detect.

Network detection based on graph rules

These solutions rely on graph technology, which is built to work natively on networked data. They go well beyond first-degree relationships and can analyze entire networks. They can directly detect suspicious networks, and also correlate those networks to show if one network is actually part of a larger one. This can be done in near real time with graphs of billions of entities.

Ability to adapt rules to changing needs

Fraud and money laundering schemes are constantly evolving as criminals, often working in professionalized groups, devise new ways to bypass existing rules and defense systems. In this context, organizations need to be able to create new rules or otherwise adapt the solution to new threats or new business needs.

Different solutions leave the customer with varying degrees of autonomy to set up or adjust rules and alerts and to integrate new data. Some detection rules are standardized and pre-configured within the solution, meaning they cannot be changed. Inflexible rules will be of limited usefulness in a shifting financial crime landscape.

The time to close the loop when there's a new threat and flexibility in creating rules depends various factors.

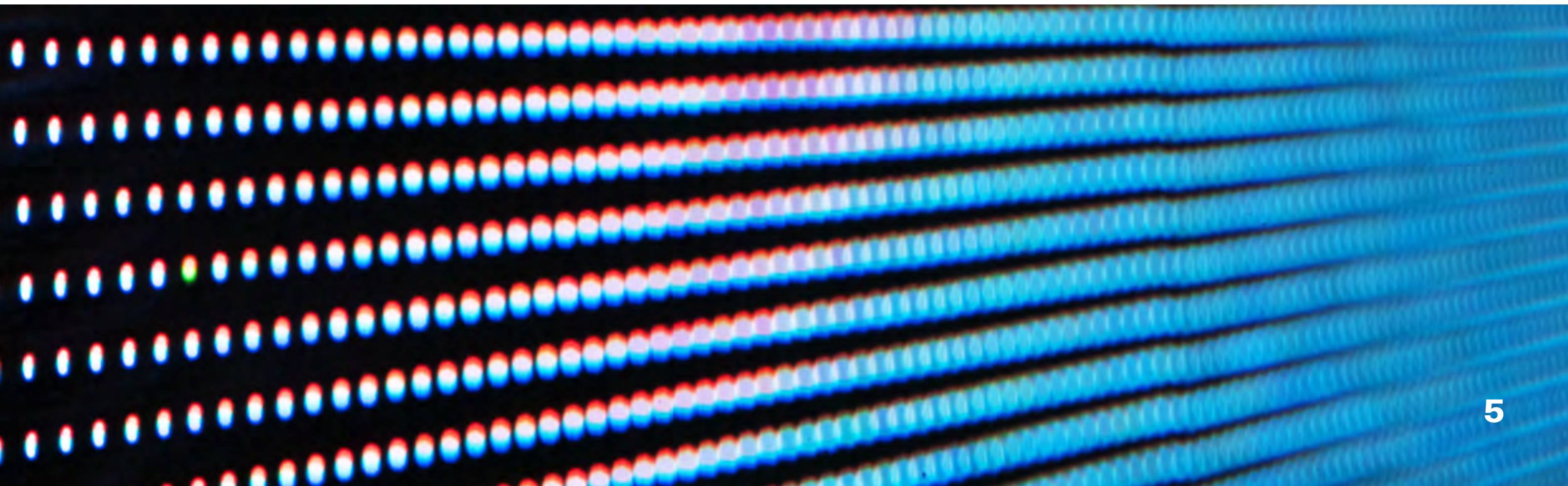
Rule adaptability

Hard-coded rules

Customized rules are created for the customer's use case and are implemented by developers or consultants. They require a query language like SQL, which is challenging to write. These rules cannot be easily changed on the client's side without external intervention, slowing down the adaptation time.

Configurable rules

Rules can be independently configured by the end user. Graph databases natively provide an easy to master and powerful graph query language (Cypher or Gremlin) that allows you to describe real-life patterns. A solution natively based on graph technology will provide the most flexibility.



Integration with third-party tools

Financial institutions use multiple sources for detection and investigation. Compliance regulations around politically exposed persons or sanctioned entities require specialized solutions like sanctions lists or compliance databases, for example.

Many financial institutions and other organizations have also invested money and human resources in setting up tools like scoring engines, case management systems, reporting tools, etc.

Integration capabilities are therefore paramount both for cost management and to effectively counter financial crime. Solutions that facilitate integration can also be less costly in maintenance time and from a financial point of view in the long run. But not all solutions are equal in their ability to integrate with different pieces of an anti-financial crime tech stack.

Integration categories

No integration

Some solutions come entirely packaged together. They simply cannot integrate data from external sources or alerts, cases, etc. from other systems.

Integration through proprietary connectors

Some solutions can be integrated with a set list of screening solutions, compliance databases, etc. through proprietary connectors, allowing some flexibility, but still with significant limitations.

Full integration

The most flexible and adaptable solutions can be integrated with screening solutions, case management systems, reporting tools, compliance databases, etc. This type of solution lets you easily fill in any gaps in your detection and investigation systems.

Cost of ownership

As compliance rules tighten and financial crime threats become more complex, the resources organizations invest in anti-financial crime solutions have tended to increase. An important consideration for any piece of your tech stack is the global cost of ownership.

The total cost of ownership includes the costs that go beyond the initial implementation of a solution.

Evaluating cost of ownership

How much support from the vendor and/or consultants is needed for set-up and maintenance?

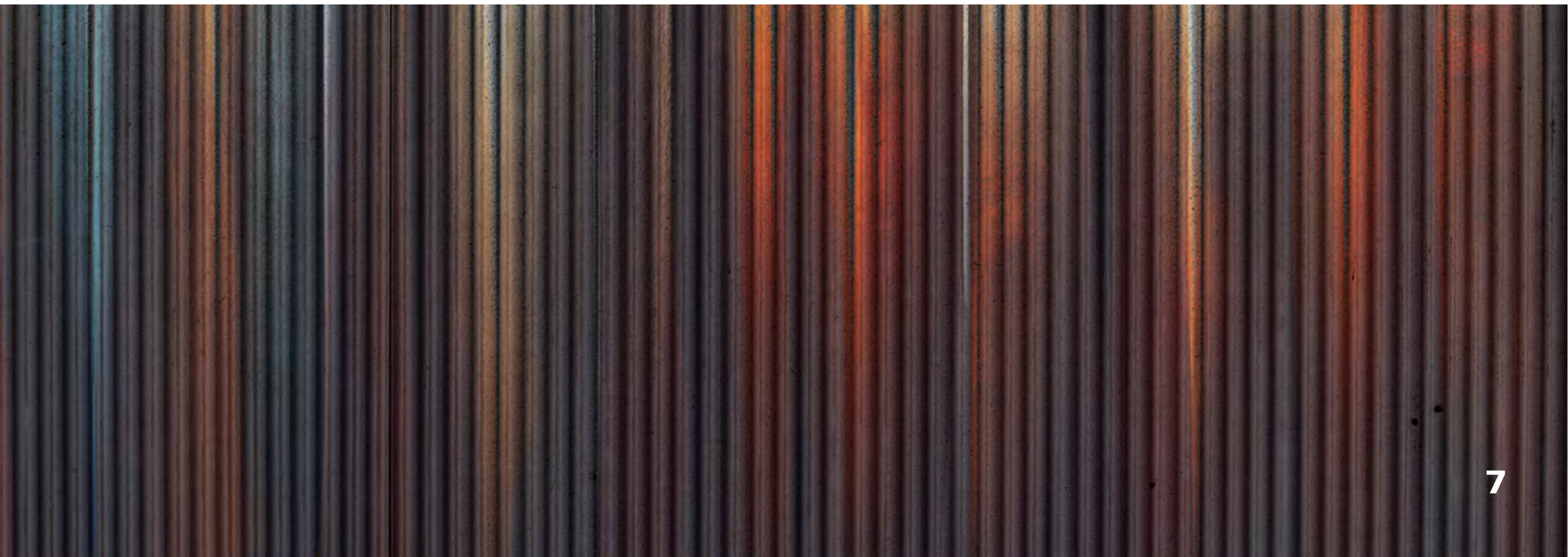
Solutions vary in how flexible they are to set up, modify, integrate with other tools, etc. The more autonomy the end-user has, and the less external support the tool requires, the easier it is to manage the cost of ownership.

How flexible are the detection models?

In addition to impacting the speed of deployment of a solution, data model flexibility has an impact on cost. Flexible detection models that can be set up directly by end-users (such as native graph models) generate fewer costs than detection models that require intervention by vendors or consultants.

How complex is the underlying infrastructure?

Software architectures based on a combination of relational databases and other tools such as Spark, Hadoop, or ElasticSearch are more complex than graph database-native architectures. The latter therefore tends to require less time and resources to manage.



Data exploration performance and UX

Historically, investigation solutions have provided limited tools for data exploration based on tabular interfaces. But as with detection of suspicious networks, the ability for analysts to effectively explore their data depends largely on how the solution performs on link analysis. More effective data exploration translates to faster decision making, from case triage all the way through investigation.

As for the technical performance of solutions, this depends on the ability to perform network visualization and analysis. Graph-native solutions can return results almost immediately. Solutions that are built on relational databases, on the other hand, can take seconds or dozens of seconds to return a result since non-graph native network visualization and analysis comes at a high computational cost.

Finally, the user experience is also an important consideration. Many solutions require technical expertise to access advanced network analysis. Others just offer limited, surface-level capabilities for data exploration. The solutions with the best user experience are graph native and are accessible to both technical and non-technical users. They enable the visualization and exploration of large networks thanks to graph analytics and a powerful UX. These tools can be used to perform routine analysis as well as more advanced data exploration in complex investigations.

Evaluating cost of ownership

No network exploration tools

Some solutions offer visualizations that resemble networks but do not actually offer any exploration capabilities.

Limited network exploration

Some solutions offer a view of an entity and its nearby network that is static or difficult to explore, either because of performance limitations or lack of exploration tools.

Advanced network exploration

Based on native graph technology, these solutions offer full network exploration capabilities with fast performance. Some tools offering advanced network exploration also have intuitive user interfaces that enable exploration by both technical and non-technical users.

Key questions for solution evaluation

As you evaluate the strengths and weaknesses of your current detection and investigation solution(s), here is a list of questions to ask yourself. These can help pin down where the gaps are in your current system, and what you'll need to effectively fill them.

- **What specific actions do I need to accomplish with my anti-financial crime system?**
- **Are any of these actions missing within the technology I'm using today? Is the technology I'm using underperforming on any of these actions?**
- **Is my detection system based on simple rules?**
- **Does my detection system detect single entities or does it detect entire networks?**
- **Does my detection system utilize AI?**
- **Do I depend on vendors or consultants to implement detection and correlation models?**
- **Can I autonomously define and implement new detection rules?**
- **Do my detection and investigation tools integrate with third-party tools such as other detection or screening solutions?**
- **Do I have access to contextual information as I triage alerts and build cases?**

About Linkurious

Linkurious provides the next generation of financial crime detection and investigation solutions. Simply powerful and powerfully simple, Linkurious technology helps teams of analysts and investigators in Global 2000 companies, government agencies, and non-profit organizations to prevent even the most sophisticated criminal networks from slipping through the cracks.

Linkurious Enterprise

Linkurious Enterprise is a powerful yet intuitive end-to-end financial crime investigation platform that uses powerful graph analytics to enhance each step of the investigation process, from detection to case management. Linkurious Enterprise provides both technical and non-technical users with a deep understanding of relationships and context to drive better decision making.

No matter how large or complex your data, Linkurious Enterprise can help you accelerate your investigations and outsmart savvy fraudsters and money launderers.

Linkurious Enterprise delivers key benefits to financial crime leaders:

- **Improve detection** with a 360° view of your data, stop advanced fraud and money laundering tactics that other solutions fail to signal.

- **Faster investigations,** with a flexible and powerful visual interface to navigate through data in one comprehensive view.

- **Easily manage workflows from end to end** to increase efficiency and diminish the number of triage cases by prioritizing and consolidating cases.

Linkurious Enterprise also makes graph data available to use with legacy tools. It can function as your go-to investigation platform, or can be layered into existing financial crime solutions to improve alerts and investigations.

Learn more