Why you need an end-to-end solution for risk and fraud investigations

WHITE PAPER

THOMSON REUTERS®

More than ever, businesses are under siege. And the battle is only going to get more intense.

The problem is risk.

Specifically, the dangers of customers and vendors that aren't who they say they are. If an organization can't thoroughly screen a potential customer or vendor for risk, it could be making itself vulnerable not only to fraud but also to legal liabilities. It could be at risk of lost revenue, lost customers, and damage to a company's reputation that can take a long time to repair. It could even be in danger of shutting down.

If your title is chief risk officer or another position where you're overseeing efforts in areas such as anti-money laundering (AML), know your customer (KYC), or customer due diligence (CDD), you know this all too well. You might also be unsure what more you can do to identify and minimize the risks that are coming your way. You might be finding that the mix of tools and processes that you and your team use to uncover information on potential customers and vendors has become rather clunky. It requires too much of your people's time, and time has become particularly precious given the increasing workload and the increasing difficulty in finding hires with the right skill sets. Risk models are often being applied inconsistently, even by the same staff members.

What are the risks to you and the business you work for? You're undoubtedly well aware of them. Customers or vendors that appeared to be trustworthy when you began working with them may prove to be bad actors that leave invoices unpaid or prepaid orders unfilled.

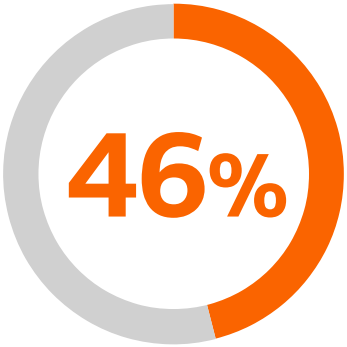
And with transactions and data largely digitized, what appeared to be a solid, reliable business relationship could turn into a skillfully nefarious scheme to embezzle thousands of dollars in financing or products from your organization. All this means that your organization is facing perils like never before — and that you're wrestling with worries and sleepless nights.

Whatever the type of organization you're helping to protect, minimizing risk is essential to its lasting growth and its reputation. From identity verification and risk assessment as you onboard clients and vendors, to the continuous evaluation and investigation of revealed concerns within existing business relationships, it is mission critical to cover the needs across all your risk-based review requirements.

What can you do to improve the odds of your organization's financial survival? What you may be needing is a single end-to-end solution that allows you and your team to handle all the phases and activities involved in assessing and managing risk — onboarding customers and vendors, monitoring their transactions, and investigating any suspicious activities that your monitoring might reveal.

In this white paper, we will focus largely on the risk and fraud management challenges facing financial institutions, which are under particular pressure to prevent fraudulent activity and confirm the identities of individuals and businesses seeking to open accounts. But most businesses are facing many of the same potential dangers.

The 2022 Global Economic Crime and Fraud Survey released by PwC reported that



of the organizations surveyed experienced some form of fraud or other economic crime over the past two years.

Standard operating procedure and taking the "digital journey"

The dangers of customer and vendor fraud are huge and undeniable. Just to name one statistical source: The 2022 Global Economic Crime and Fraud Survey released by Big Four accounting and professional services firm PwC reported that 46% of the organizations surveyed experienced some form of fraud or other economic crime over the past two years. These crimes include asset misappropriation, supply chain fraud, and fraudulent activity associated with procurement and accounting.

According to the survey, 52% of companies with annual revenue over $10 billion experienced fraudulent activity; for businesses under $100 million in revenue, that figure is lower but still significant (38%). Nearly every business sector — manufacturing, healthcare, technology, retail, energy, and of course financial services — has been victimized by bad actors. And often, those fraudsters are people and companies those businesses thought they could trust. As the PwC survey also noted:

- 43% of "the most disruptive or serious fraud" that surveyed organizations experienced were perpetrated externally, while 31% came from internal sources and 26% resulted from a collusion between external and internal actors
- Of those external perpetrators, 29% were customers, 20% were vendors, 12% were shared service providers, and 10% were consultants
- Among financial services businesses, 44% of fraud came from customers

In other words, the need to conduct risk and fraud assessment of any customer or vendor remains crucial. But how can you find the most current, most thorough information?

Let's start with financial services. Larger financial institutions often follow several steps, each with its own team and workflows. In many cases, each of the following steps is handled by a single team:

- Account onboarding departments, which focuses on verifying potential customers' identities
- A fraud team that monitors and investigates any account activity that looks suspicious
- A financial intelligence unit that handles deeper investigations

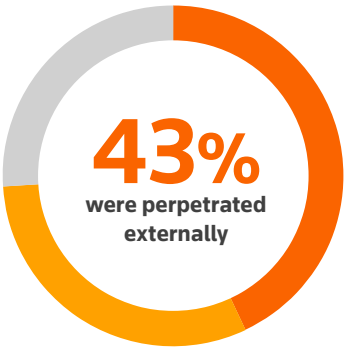
These teams make use of data gleaned from sanction checks, background research in public records, negative news/adverse media reports, and court records searches. Many might be using digital platforms that provide access to each particular type of data. But many of them continue to rely heavily on "manual" approaches — entering names of potential or existing customers and vendors into search engines such as Google, then visiting every website that might have relevant data. Not only is this approach time-consuming, it also can result in inconsistent, unreliable results. In addition, those who are handling this work are often overwhelmed and don't always have time to do complete, proper, and thorough due diligence. And what's more, these teams are often siloed and not sharing information that they all could find useful.

What these banks, credit unions, and financial services companies need are greater efficiencies in knowing their customers and spotting potential risk. That's also true of many other types of businesses that need to protect themselves from bad actors.

For the past decade or so, businesses of all kinds have been working to make their operations more and more digital, at least as much as possible. Management consultants often refer to this as "the digital journey." Of course, businesses have become more digital, using web-based transactions, chatbots and other online customer service providers, and so on. But when it comes to risk and fraud, finding and using a complete digital solution has been more challenging.

And that is why organizations may require an end-to-end solution. Yours may well be one of them.

Of "the most disruptive or serious fraud" that surveyed organizations experienced:



31%
came from internal sources

26%
from a collusion between external and internal actors

What is an "end-to-end" approach?

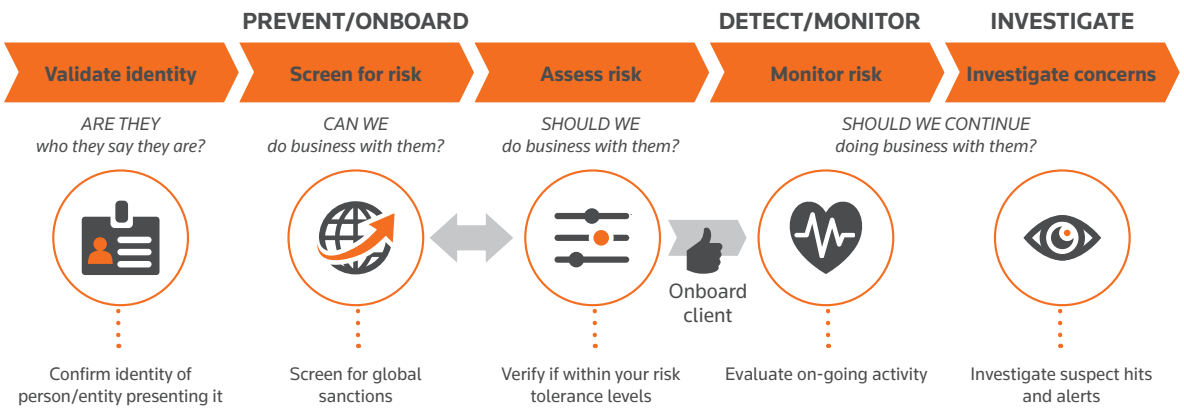
An end-to-end solution would include onboarding, monitoring, and investigating all possible sources of risk throughout all phases of a customer or vendor relationship to assess and manage that risk. For financial institutions, for instance, an end-to-end solution will initiate a thorough vetting before onboarding, then continue to monitor any relevant data as soon as a customer opens a bank, crypto, or online brokerage account. The solution also would support everything a bank, credit union, brokerage, or other financial services provider needs to conduct compliance activities or identify any potential fraud, such as money laundering, that may occur many months after the customer is onboarded. It would continue to monitor or investigate any red flags that an account holder might run up the flagpole.

This end-to-end approach is being offered by Thomson Reuters® with its Risk & Fraud Solutions portfolio that brings together several digital risk and fraud discovery and management tools. The centerpiece is CLEAR, a cloud-based public-records database-searching set of tools that automates processes for collecting and analyzing thousands of state and federal data sets. CLEAR allows organizations to conduct deep investigative research and create reports on potential customers and vendors.

Popular CLEAR tools include:

- ID Confirm, which validates that identities exist by searching across numerous data sources
- Risk Inform, which allows an organization to quickly assess risk and uncover synthetic identities
- Adverse Media with Sanctions, which uncovers negative news coverage plus sanctions, politically exposed persons, and state-owned entities for a potential or current customer or business that raises concerns, including the possibility of financial crime

The graphic below illustrates how this creates an end-to-end approach, from verifying the identity of a client, customer, or vendor, through onboarding, risk assessment and monitoring, and investigating potential problems:



Thomson Reuters Risk & Fraud Solutions establishes consistent risk models that are based on the specific criteria an organization sets up. This gives a financial institution or other business the capability to adjust these risk models as the market, regulations, and other issues change.

What's more, all of these tools are automated, using AI-powered analytics that can sort through massive amounts of online data. Artificial intelligence technologies allow you to quickly examine and report on multiple data points, including transaction and user history and account-holder geography, current activity, and account events. AI's machine-learning capabilities allow the suite to continuously learn and identify new and evolving fraud trends and risk levels, integrating an organization's proprietary data with public records.

As a result, users don't need to conduct validation, assessment, and monitoring "by hand"— that is, by calling up each online data source. Instead, the suite uses CLEAR capabilities to organize usable data on a customizable dashboard.

This adds efficiency in identification confirmation, risk assessment, and investigations. This means that routine matters can be handled quickly, and high-risk accounts can be flagged consistently and clearly so they get the time and attention needed.

Improved processes ensure compliance and allow for clearer reporting to regulators. Those added efficiencies allow it to facilitate increased business by allowing companies to respond to customers quickly. The idea is to start with good data, then apply consistent rules decided by that financial institution or other business.

What constitutes "good" or "reliable" data? This is a complex and crucial issue. The quality of an organization's decision-making processes is inextricably linked to the quality of its data. In the recently released 2022 Thomson Reuters Anti-Money Laundering Insights Survey, financial services industry respondents were asked how satisfied and confident they were with the accuracy of data acquired from their primary data providers. In general, the answer was "not very."

In a sense, you could compare it to milk that you buy at the supermarket. The bottle or carton includes a sell-by date to let you know it's fresh and hasn't spoiled. The difficulty with the data that many risk-detection software programs deliver is that it can't guarantee freshness. These programs typically timestamp the information with the date that they retrieve it (or upload to their programs), when in fact, that data could be years old.

By contrast, the Thomson Reuters Risk & Fraud Solutions are designed to deliver transparent data. In other words, it identifies the specific source of the data, including the exact date it was posted by that source. This allows you and your team the ability to evaluate that data and compare it with other (perhaps troubling) data you've uncovered about the potential vendor or customer. And once a customer is onboarded, you can monitor the relationship for any worrisome activity that requires investigation. Financial institutions, for instance, can be alerted if an account holder suddenly begins sending numerous overseas wire transfers.

You can look upon Risk Inform and Adverse Media as "instant insight tools," identifying risks as soon as they appear. When the person or entity of a questionable transaction needs to be investigated, an organization needs to look beyond its own data to public information that might reveal a sketchy history or questionable recent activity.

It's also worth noting that many financial institutions have substantially more risk in their portfolio than they realize or have accounted for. In general, banks (and perhaps other organizations) want to know only what they're tasked with knowing. For instance, bank regulators may not require financial institutions to look beyond the individual or a company ownership's when evaluating the risk of onboarding an account. Might there be other problems in that individual's or owner's extended family? A bank, credit union, or brokerage may wish to focus only on what might be the immediate risk.

In such cases, CLEAR Risk Inform can be configured so that the organization has a set template for a consistent data-discovery process. This allows a financial institution (or other business) to focus on the types of data it wants to uncover — for instance, by narrowing down a data search for bankruptcies by a set time period.

This past May, Forrester published an ROI study on the cost savings and benefits that businesses gained by using CLEAR ID Confirm and CLEAR Risk Inform, two of the key tools in the Thomson Reuters Risk & Fraud Solutions suite. Among the CLEAR users interviewed in the study, Forrester reported that using CLEAR resulted in 40% more efficient identity confirmation and 40% more efficient risk assessment, as well as easier investigation of high-risk accounts and improved processes to ensure compliance. Forrester respondents also cited additional business from faster customer onboarding and thus a higher level of customer service.

Doing your own due diligence

Thomson Reuters Risk & Fraud Solutions is continuing to add new tools. Most recently, the CLEAR suite now allows organizations to conduct global business research and investigations of international customers and vendors. As larger U.S. financial institutions and many American businesses (both large and small) expand their overseas markets, this capability can be crucial for sorting through the complexities of data across numerous countries.

In sum, Thomson Reuters Risk & Fraud Solutions provides the most complete research and investigation toolbox currently available. And for organizations seeking to reduce the number of vendors they work with; Thomson Reuters can offer a single vendor.

Could you and your financial institution or business benefit from an automated, end-to-end approach to verifying potential customers and vendors and monitoring any signs of fraud they might be evincing after they're onboarded? You can learn more by investigating Thomson Reuters Risk & Fraud Solutions at **tr.com/risk-fraud**.

Thomson Reuters is not a consumer reporting agency and none of its services or the data contained therein constitute a 'consumer report' as such term is defined in the Federal Fair Credit Reporting Act (FCRA), 15 U.S.C. sec. 1681 et seq. The data provided to you may not be used as a factor in consumer debt collection decisioning, establishing a consumer's eligibility for credit, insurance, employment, government benefits, or housing, or for any other purpose authorized under the FCRA. By accessing one of our services, you agree not to use the service or data for any purpose authorized under the FCRA or in relation to taking an adverse action relating to a consumer application.

THOMSON REUTERS®