datos INSIGHTS

February 2024

Identity Risk Management: Orchestration as the Key to Collective Risk Intelligence

Charles Subrt

Prepared for:

ALLOY

February 2024

Identity Risk Management: Orchestration as the Key to Collective Risk Intelligence

Charles Subrt

Table of Contents

List of Figures

Executive Summary

The customer identity profile comprises many solutions, tools, and data sets, but current approaches to identity risk management have hamstrung financial institutions (FIs). This white paper explores why new and innovative approaches can better connect anti-money laundering (AML) compliance, anti-fraud, and credit-decisioning risk tools within a common infrastructure so FIs can integrate and harness an increasing volume of data more effectively, construct more complete identity profiles, and cultivate more meaningful and collective risk intelligence.

The key findings from this paper follow:

- **Effective identity risk management is hard:** Conducting and maintaining appropriate identity risk management has traditionally been an endeavor that most FIs have struggled to master and bring together in a versatile, dynamic, and sustainable manner. As the volume of risk-relevant customer information continues to expand, legacy approaches to Know Your Customer (KYC) and identity stymie many institutions in their ability to harness the data and build holistic pictures of customers and their risk.

- **Executing an orchestrated identity risk management ecosystem is imperative:** Without fully integrated systems and data sources, a lack of holistic enterprise views of customer identity often leads to insufficient customer risk appreciation, siloed organizational decision-making, and inadequate outcomes while creating operational lag and resource misallocation. Transforming customer information into actionable risk intelligence requires a more cohesive organizational strategy and an orchestrated technology infrastructure so FIs can bring together the current patchwork of processes, systems, and data that support identity risk management.

- **The benefits of integrating the right orchestration tools are abundant:** Orchestration can bring together the underlying data and systems into a more integrated ecosystem, facilitating the ingestion and analysis of risk-relevant data and cultivating enriched risk intelligence. These technologies can promote regulatory compliance and vibrant risk management practices across the customer life cycle. In addition, cross-functional benefits can be achieved, which improves organizational economics and the customer experience when it is most delicate—at the beginning of the relationship.

Introduction

Managing identity across the end-to-end customer life cycle is a foundational pillar for all FIs as they attempt to balance myriad strategic yet perhaps conflicting priorities: delivering seamless onboarding and ongoing customer experiences and growing revenue while achieving strong risk management and regulatory compliance, operational efficiency, and cost management. Customers expect faster and frictionless experiences, but FIs must perform appropriate due diligence and other risk-mitigation activities to manage their fraud, AML compliance, and credit risks appropriately. Doing so becomes even more critical and complex as firms onboard and sustain relationships with business entities.

Yet, current approaches to identity risk management have hindered FIs in achieving an optimal balance of their strategic objectives. Over time, firms have deployed a patchwork of solutions, tools, and data sets to assemble customer information and build a customer identity and risk profile. Moreover, the responsibility for identity risk management has often been largely fragmented and decentralized, with key roles and accountabilities spread across various business, operational, and risk functions. As a result, FIs have had to devote significant operational resources to these activities.

This white paper explores why FIs need new and innovative approaches to connect compliance, fraud, and credit risk tools within a common infrastructure so they can integrate and harness an increasing volume of data more effectively, construct more complete identity profiles, and cultivate more meaningful and collective risk intelligence. A more integrated technology infrastructure underpinning identity risk management can enable firms to become more proactive and agile in adapting to an evolving threat landscape while delivering better experiences across the customer journey.

Methodology

The insights supporting this white paper are based on ongoing Datos Insights research as well as interviews and surveys conducted in 2023 with financial crime risk practitioners at financial organizations.

Mastering Identity: The Holy Grail of Risk Management

In today's fast-paced and increasingly digital world, establishing dynamic, integrated, and cohesive identity risk management has become more critical than ever, as it supports almost every other aspect of an organization's ecosystem. Not only should FIs know to whom they are providing products and services, but they must also ascertain their customers' ongoing risk, vigorously scrutinize their behavior, and respond appropriately to mitigate potential risks. By building holistic pictures of customer identity and risk, firms can drive more effective risk management and regulatory compliance while taking on more profitable but higher-risk customers (Figure 1).

Figure 1: Mastering Identity Risk Management

Source: Datos Insights

Effective Identity Risk Management Is Hard

Conducting and maintaining appropriate identity risk management has traditionally been an endeavor that most FIs have struggled to master or bring together in a versatile, dynamic, and sustainable manner. The volume of risk-relevant customer information continues to expand, particularly with the introduction of nontraditional data sets, such as

geolocation data and device and behavior analytics. Hence, legacy approaches to KYC and identity hinder many institutions' ability to harness diverse customer data and sufficiently build holistic pictures of customers and their risk levels. Unreliable risk assessments can allow higher risks and reportable suspicious activity to go hidden while driving needless friction for good customers.

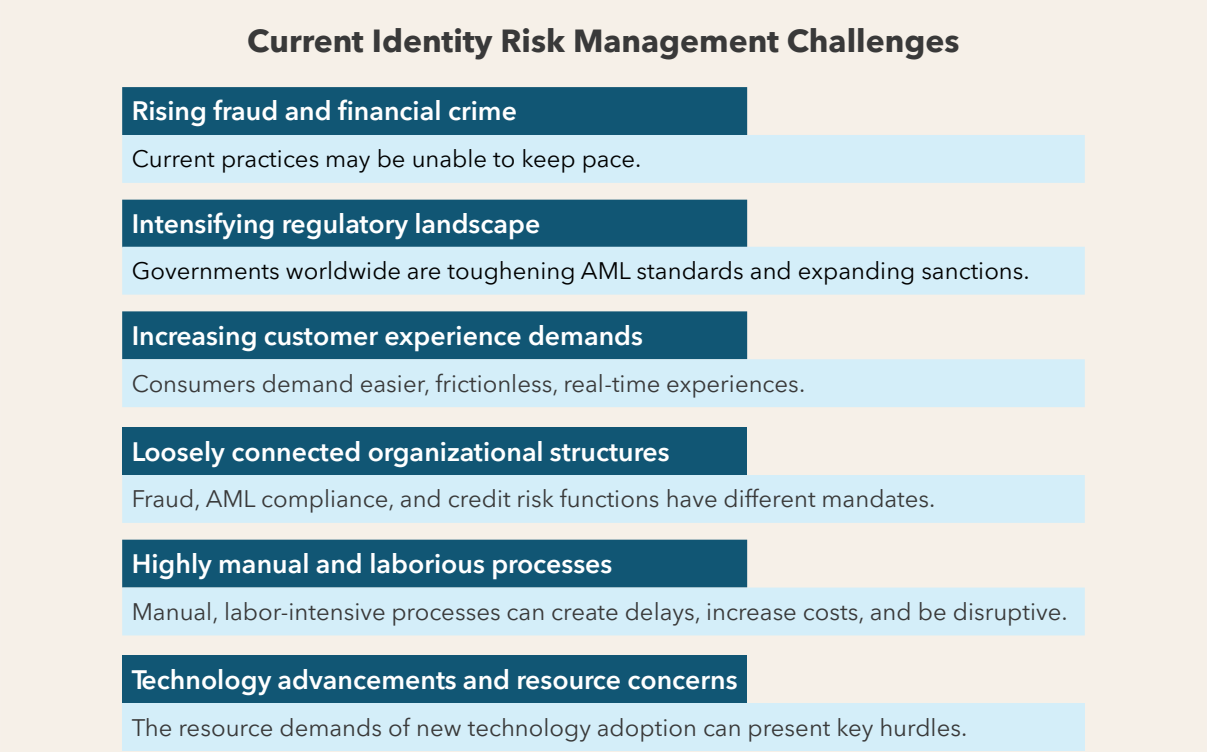
Starting with onboarding and acceptance and extending throughout the customer life cycle, FIs must conduct ongoing risk-based KYC and due diligence on all individual and business applicants and customers. This includes corporations, trusts, partnerships, and other legal entities. When conducting Know Your Business (KYB) on corporate customers, FIs are expected to also ascertain and conduct KYC on the individuals with an ownership share or control, management, or direction of the business entity—i.e., the ultimate beneficial owners (UBOs). Regrettably, this can be a tricky pursuit, as much information or documentation, especially on UBOs, officers, directors, and other key stakeholders, is not publicly available, and individual ownership and control can often be obscured through intricate corporate layers. Business onboarding, especially onboarding large and global organizations, can be highly manual, time-intensive, and protracted. The process can often take days, weeks, or even months.

AML compliance officers may often be responsible for establishing the primary customer information requirements for regulatory compliance, but other critical risk, business, and operational functions leverage risk-relevant customer information to achieve their key mandates while servicing the customer. Numerous internal and external systems and data sources are maintained to gather, assemble, validate, and analyze critical customer information. An effective identity risk management program should bring together those functions responsible for fraud, credit, KYC/KYB, and identity verification and authentication and the policies, processes, and technologies supporting them. These functions should work together and support a cohesive and effective execution of interconnected procedures and practices, removing all silos and assembling a single customer view.

Escalating fraud and financial crime, increasing regulation, growing demands for frictionless customer experiences, and a greater urgency to operate more efficiently can often impede the successful operation of identity risk management. The lack of a unified or holistic customer view further disrupts effective risk management, causing operational inefficiencies and frustrating best efforts to promote seamless customer experiences. Moreover, there can be a disconnect and a lack of visibility and transparency into the

customer journey among different business lines as well as across business operations and risk functions (Figure 2).

Figure 2: Current Identity Risk Management Challenges



Source: Datos Insights

Rising Fraud and Financial Crime

Financial crime is flourishing as organized crime becomes more sophisticated at exploiting vulnerabilities across the financial ecosystem and hiding their true identities and unlawful activity. Criminal networks frequently use corporate structures to operate with greater anonymity. Current identity risk management practices may be unable to keep pace. Operating KYC/KYB and anti-fraud processes and workflows in silos thwarts the organizational ability to identify and stop bad actors while confidently onboarding legitimate new customers.

Intensifying Regulatory Landscape

Governments around the world are constantly evolving, toughening AML standards and expanding sanctions. Customer due diligence is often cited as a primary pain point. Many AML compliance officers worry whether they can construct complete customer risk profiles or whether ongoing monitoring is adequate. Many enforcement actions trace back to

insufficient identity management and customer risk profiling, particularly for corporate entities. Insufficient identity management can also degrade screening against sanction watch lists, leaving FIs exposed to transacting with individuals and entities subject to international sanctions.

Increasing Customer Experience Demands

Consumers are demanding easier, frictionless, and more real-time experiences. FIs are under extreme pressure to integrate friction-right controls for bad actors while delivering a seamless customer experience for legitimate customers without introducing too much risk for the organization. Poor customer experiences driven out of siloed and disconnected systems, processes, and workflows can increase applicant abandonment and erode customer loyalty.

Loosely Connected Organizational Structures

The functions responsible for managing fraud, AML compliance, and credit risks have different mandates. As such, they have diverse needs in constructing an understanding of customers and their risk profiles and what measures may be needed to manage those risks. Enterprise risk management operations become less effective and efficient, driving up long-term costs as follows:

- Streamlining legacy technologies and harnessing risk-relevant data to feed analytics have long been primary challenges for risk executives. These functions have cobbled together disparate processes, systems, and data sources, leaving underlying enterprise identify risk management frameworks fragmented, disjointed, and operationally burdensome with high technical debt. Vital data and documentation can be siloed across different business groups, functions, and loosely connected systems.

- Loosely connected systems can often lead to duplicate customer requests and inquiries, resulting in poor experiences. Moreover, organizations frequently miss the opportunities to offer customers additional complementary and value-added products and services as a result of disconnected business operations.

- A lack of a centralized customer profile impairs the ability to identify, assess, and monitor high-risk parties, accounts, and events accurately. Inferior customer intelligence can degrade financial crime monitoring, leading to too many false positives. Considerable resource time can be allocated to unnecessary alert reviews and customer due diligence activities.

Highly Manual and Laborious Processes

Highly manual and labor-intensive processes often delay processing times of onboarding and other customer-initiated requests, increase operational costs, and disrupt seamless customer experiences. Manual and repetitive processes can also lead to poor data quality, and less-than-ideal data often degrades effective risk management. Periodic reviews of accounts ensure complete, accurate, and current customer information. However, they are operationally taxing, particularly since behavior can change through the customer life cycle. Moreover, extensive KYC/KYB protocols, highly manual processes, and a lack of holistic views of customers and their risk profiles extend customer onboarding, add unnecessary friction, and frustrate applicants and customers.

Technology Advancements and Resource Concerns

Advancements in computing capabilities, automation, artificial intelligence, and cloud-based technology can uplift regulatory compliance and risk management. At the same time, they can improve operational efficiency, reduce the total cost of ownership, minimize customer friction, and support and drive organizational growth. However, the overall resource demands of adoption can present key hurdles.

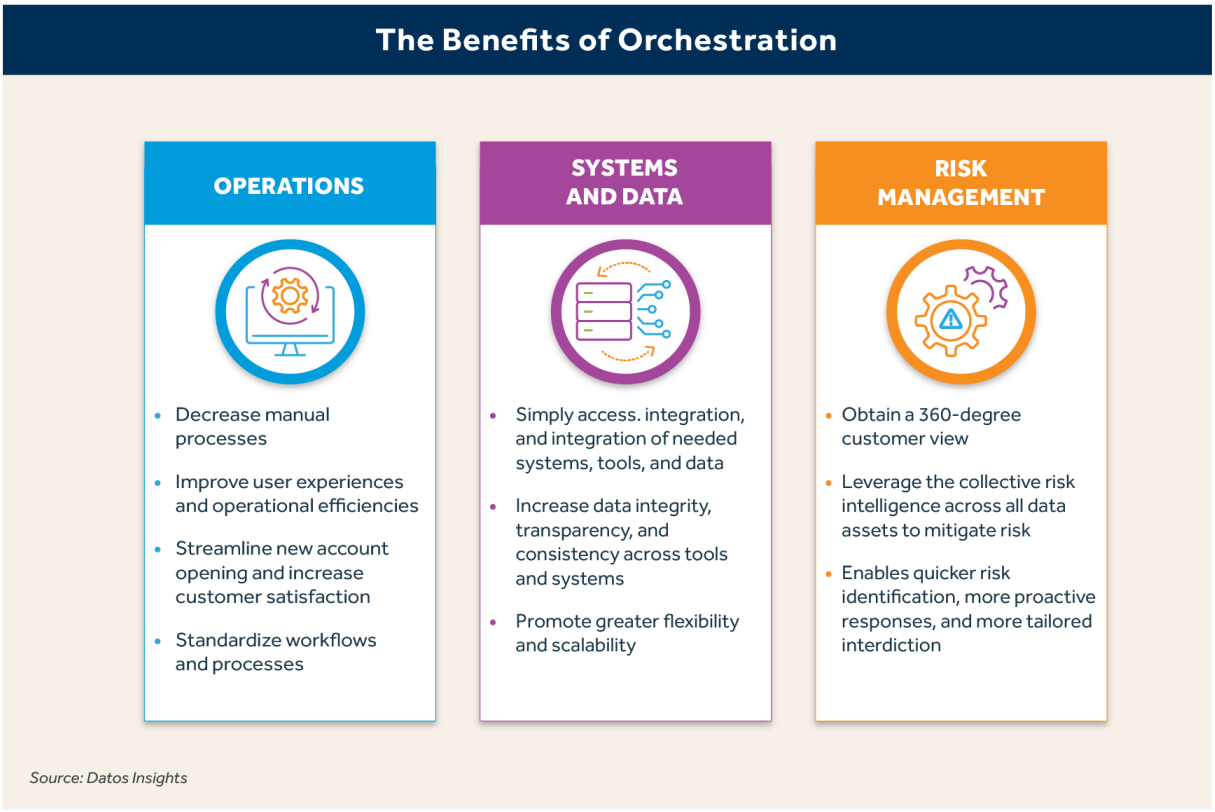
The Growing Imperative of an Orchestrated Identity Risk Model

To help mitigate the risks stemming from the increasing financial crimes and poor credit decisions, FIs must evolve how they define, construct, and manage identity across the customer journey. To transform customer information into actionable risk intelligence and one collective customer truth, FIs must commit to a more cohesive strategy and an orchestrated technology infrastructure to bring together the current patchwork of processes, systems, and data that support identity risk management.

While coordinating across risk disciplines can be challenging due to competing objectives, the commonalities can be aligned through effective orchestration. Integrating the right orchestration tools can bring together the underlying systems into a more cohesive ecosystem, facilitating the ingestion and analysis of risk-relevant data and cultivating enriched risk intelligence. These technologies can drive regulatory compliance and vibrant risk management practices across the customer life cycle. In addition, cross-functional benefits can improve organizational economics and the customer experience, especially when it is most delicate—at the beginning of the relationship.

Orchestration yields numerous benefits (Figure 3).

Figure 3: The Benefits of Orchestration



The following benefits are realized when institutions embrace a more holistic mindset to risk management and leverage the core orchestration capabilities.

- Modern APIs, built-in connectors, and other tools simplify the deployment and integration of diverse tools, technologies, and applications. They also simplify the analysis of multiple data sources and intelligence, often in different data stores and formats, and help cultivate collective and actionable risk intelligence. These benefits enable organizations to adopt the most appropriate tools and data sets more easily, allowing them to configure the identity risk management stack to fit the needs of their business operations, risk functions, and customers.

- FIs must be able to integrate digital identity data more easily and construct more holistic customer profiles to prevent more fraud losses without inserting unnecessary friction across the customer life cycle. Orchestration tools can amalgamate multiple attributes such as behavioral biometrics, device identity and reputation, mobile phone ownership, and email tenure and reputation into an enterprise risk assessment and decision-making infrastructure.

- Increased orchestration can streamline the operations and workflows of identity risk management and help navigate customers as well as internal staff through mandated protocols in a less obtrusive and more consistent manner.
- More sophisticated risk-analytic and orchestration capabilities can support regulatory compliance while minimizing customer friction. As one chief risk officer of a foreign bank expressed, "As banks, we have numerous regulations to which we must adhere, so we must have the right data, tools, and technologies to stay current and not fall behind."
- Orchestration can simplify risk decisioning throughout the customer journey. Greater access and integration of diverse risk-relevant data sets, tools, and analytics enables more agile risk identification, more proactive responses, and more tailored interdiction. FIs can make faster and more informed decisions and achieve better risk-based outcomes while optimizing operational efficiency and elevating customer experiences. For example, orchestration can facilitate the appropriate treatment of customers based on the level of risk detected and the expressed preferences of those customers.
- An orchestrated identity management program can drive higher approval rates and lower customer frustration and abandonment at onboarding while mitigating risk and reducing manual reviews and intervention. For example, orchestrated and incremental fraud and KYC/KYB screenings can streamline onboarding decisioning and prevent bad applicants from getting all the way through an account opening flow before a required decline due to a fraud detection check. In the words of one risk executive at a U.S. bank, "A quick no is better than a slow yes."
- The use of orchestration hubs alleviates the overhead and operational headaches associated with internal vendor risk management processes and reduces the ongoing vendor-management burden and expense.

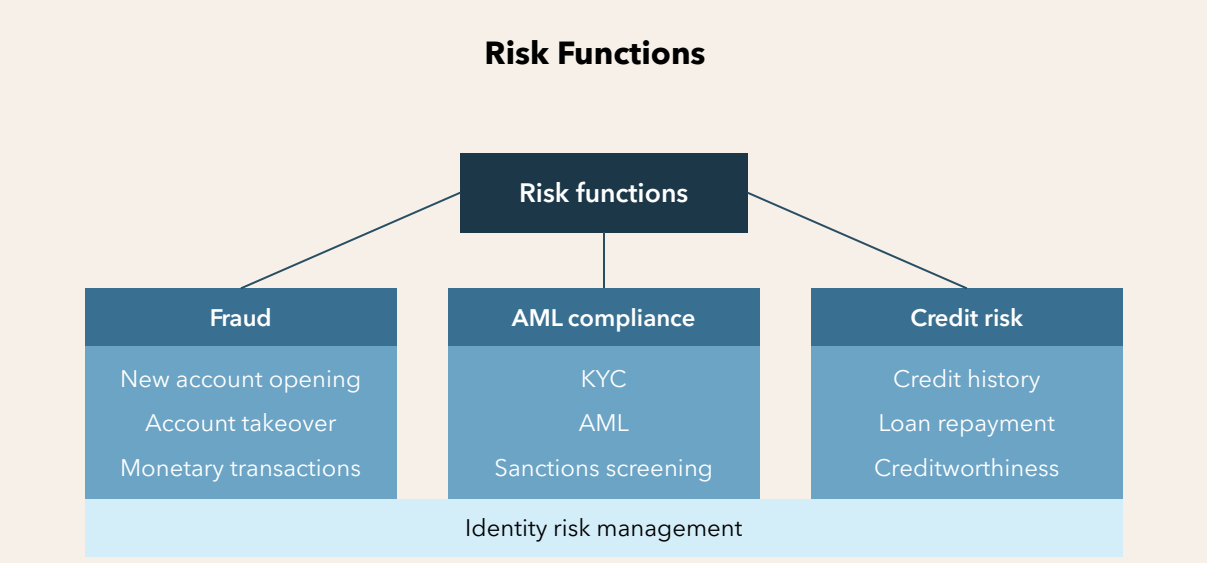
Orchestrated Identity Management: The Art of the Possible

An integrated and cohesive identity risk management ecosystem can weave together the systems, technologies, and data sets underpinning the key processes supporting the customer journey and help build holistic customer views with richer risk insights. Bringing in orchestration tools can facilitate the deployment of and integration across the different systems, ingest and analyze all internal contextual customer transaction data and external risk-relevant data, synthesize all output, and deliver faster, enriched risk intelligence. When done well, it can drive financial crime operations, risk management, and adherence to AML regulatory obligations while improving customer engagement, satisfaction, and loyalty and elevating operational efficiency.

Decentralized Risk Functions: Fraud, AML Compliance, and Credit Underwriting

Protecting the firm and the customer is a common goal for fraud, AML compliance, and credit risk functions. However, each group has a unique set of mandates and perspectives for achieving that goal (Figure 4).

Figure 4: Risk Functions



Source: Datos Insights

- **Fraud:** The primary objective of the fraud function is to reduce losses and preserve the trust relationship with customers by protecting their assets and personal and confidential information. Fraud functions tend to work in concert with IT departments and business units. They are responsible for detecting fraud across the customer journey and their financial transactions.

- **AML compliance:** AML compliance is entrusted with ensuring effective financial risk management and regulatory adherence to specific AML and KYC/KYB obligations in the jurisdictions in which the FI operates. AML compliance helps to establish the appropriate frameworks and standards for required customer information collection and validation, risk profiling, due diligence and other risk-mitigation measures, and financial crime monitoring and reporting. AML compliance is often a dedicated function, as it requires specialized subject-matter expertise as well as independence from the business.

- **Credit:** Credit risk is most commonly managed by a separate department that has sole responsibility for assessing and underwriting a customer's creditworthiness. Their objective is to ensure that the resulting credit loss rates are within a reasonable range that is consistent with the interest rate margin on the resulting receivables. The verification of the related identity is essential to ensure that the correct individual is being underwritten.

Managing fraud, compliance, and credit risk has become a constant but delicate balancing act of appropriately mitigating risk without unnecessarily disrupting customers or business growth. Some firms may align risk functions under one organizational structure or common executive leadership to foster collaboration, shared insights, and operational efficiencies. However, more often, these functions reside under separate departments with different leaders, mandates, and specializations.

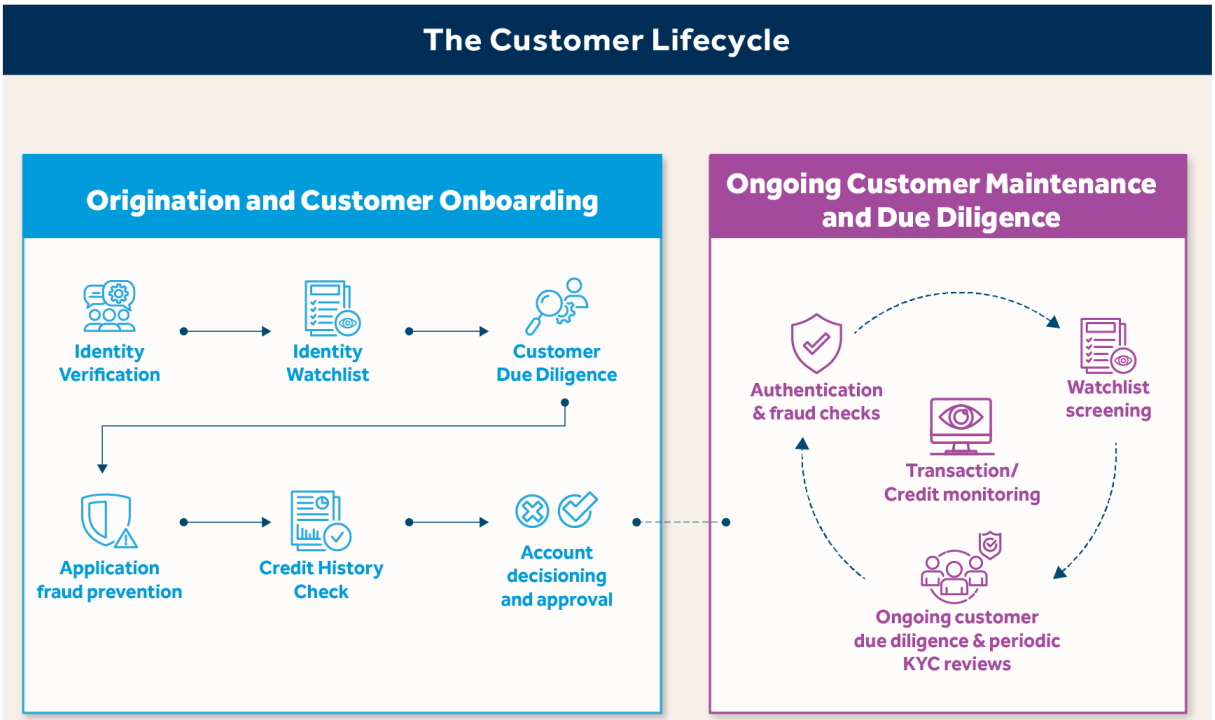
For many leaders, each risk function needs specialists with distinct skill sets and subject-matter expertise. Some leaders worry that blending these risk functions could hinder execution and decision-making by conflating their key objectives.

The Customer Journey: A Risk Perspective

Starting at onboarding and continuing throughout the customer life cycle, required customer information must be gathered and analyzed to comply with regulatory obligations as well as internal policies to inform the enterprise decision of whether to open, retain, or exit the relationship.

Business operations are typically responsible for the execution of many of the specific customer touch points and activities; fraud, AML compliance, and credit risk teams help define the key processes, data sets, and technologies supporting them. Despite having separate budgets and making separate decisions on which tools to deploy, these functions appreciate the benefits of increasing the sharing of data and tools and optimizing the end-to-end customer journey process flow (Figure 5).

Figure 5: The Customer Life Cycle



Source: Datos Insights

A patchwork of different systems, tools, and data sets supports the end-to-end customer journey. Point solutions address specific needs, but integration is necessary to maximize the benefits across multiple tools so risk functions and business operations can talk with one another and exchange data for greater visibility, more accurate detection, and lower false positives. Moreover, recognizing that legacy fraud and AML solutions may no longer be sufficient, some organizations are embedding automation and analytics to harness data more effectively and cultivate more meaningful intelligence.

Origination and Customer Onboarding

Firms take several steps during initial onboarding to collect sufficient customer information to establish identity and construct an understanding of customer risk and expected customer activity. Doing so becomes vital when building AML and fraud transaction monitoring systems and vetting future customer behavior. Most institutions perform fraud and compliance checks before completing any required credit risk underwriting:

- Customer identity can be established through documentary and nondocumentary methods. Institutions can independently compare and verify provided identity information against information gathered from reliable third-party sources.

- Applicants, customers, and counterparties, as well as incoming and ongoing payments, are screened against relevant international sanctions and prohibited lists. No further business action can be taken until all required checks have been completed and dispositioned. Checking against politically exposed-person (PEP) registers, adverse media lists, and other risk-relevant databases may also be completed to gather additional customer attributes to inform a complete risk profile.

- Customer risk profiling will often factor in a spectrum of risk-relevant attributes from multiple internal and external data sources, such as occupation or nature of business, PEP status, source of funds and wealth, geographic presence, frequency and nature of cross-border activity, and adverse media indicia. For example, cash-intensive businesses or those involved in cannabis, gambling, adult entertainment, cryptocurrency trading, or other higher-risk industries will warrant increased scrutiny. More customer information may be required to mitigate heightened risk exposure; firms may conduct additional research and investigation. FIs may elect not to onboard parties for which the risk is too high.

- Various defenses and identity verification steps are integrated into the onboarding process to look for and detect indicators of application fraud and catch fraudsters before they are onboarded. FIs have deployed different solutions leveraging behavioral biometrics, device fingerprinting, and mobile device authentication, or consortia-based suspicious identity, account abuse, and known fraudster information. Multilayered identity schemes can accelerate the application and onboarding process while extending the capacities to identify and stop application fraud, synthetic identities, and money mules.

- Depending on the nature of the business application, specific underwriting steps, including credit history checks, will be taken. Applications for business-deposit or checking accounts will not require these checks. However, applications for business loans or credit cards will require underwriting. Credit risk functions typically use commercial solutions as a starting point for creating a final credit risk solution that these functions may customize and deploy in production and acquire data from a commercial vendor to fill in blind spots in its internal data set.

Ongoing Customer Maintenance and Due Diligence

After customer onboarding, customer information and risk profiles must be kept up to date. Customer and account activity must be continuously monitored to detect changes in risk so institutions can respond timely and appropriately. Maintaining current customer information enables an organization to direct its monitoring and investigation efforts better.

Systems are in place to monitor and investigate customer transactions to detect first-party fraud, account takeovers, money laundering, terrorist financing, and other illicit conduct. The design, approach, and execution may vary across FIs, but a lack of holistic customer profiles degrades the performance of rules and models.

In servicing customer interactions and requests, authentication tools help to establish and validate customer identity by cross-checking against previously designated and internally recorded identifiers. Strong authentication protocols help to prevent account takeover fraud, build customer trust, and uplift the customer experience.

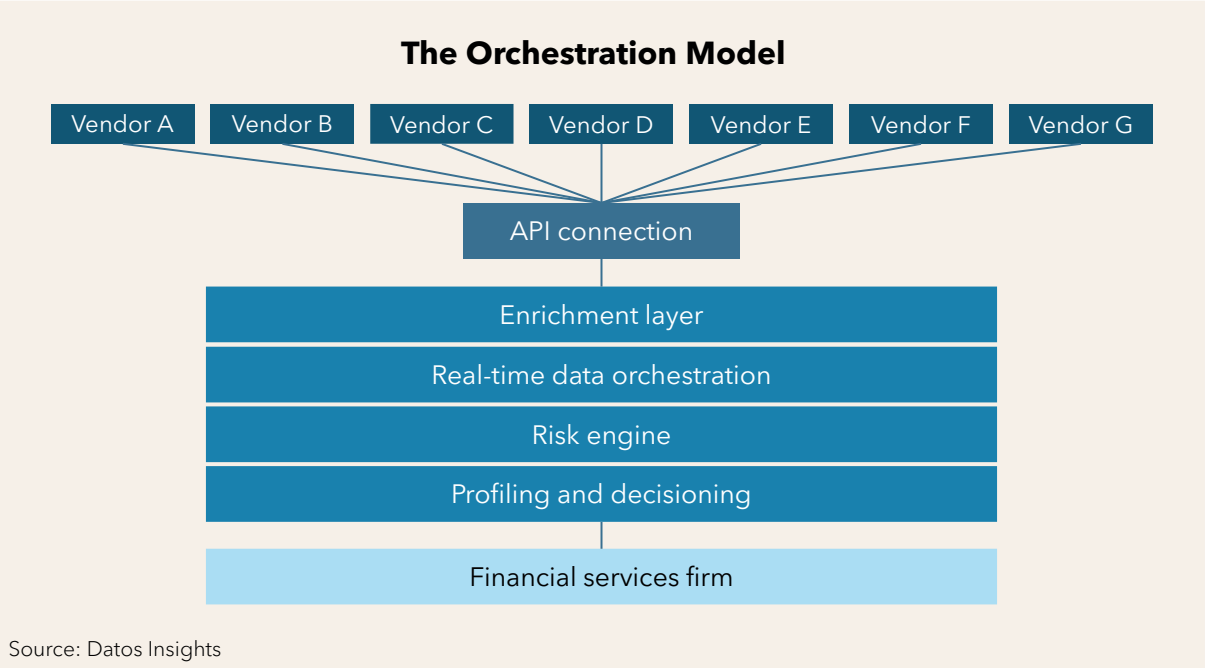
Customer accounts are reviewed periodically on a cadence based on the customer's assessed risk. These periodic reviews primarily ensure identity information is up to date as well as check actual customer activity against the expected behavior. For many institutions, these reviews are largely manual, require considerable time and resources, and can result in inaccurate or underestimated customer risk scores and leave organizations vulnerable to preventable threats.

The Orchestration Platform

Ensuring that the data gathered is comprehensive, accurate, and shared across disciplines enables each function to meet its mandates while leveraging the common data elements that support identity.

The concept of an orchestration hub delivers critical features (Figure 6).

Figure 6: The Orchestration Model



Source: Datos Insights

- **API connection:** Through one API connection, an orchestration platform can connect an end organization to numerous point solution vendors, simplifying access to fraud, authentication, KYC/KYB, AML compliance, and credit risk tools.
- **Enrichment layer:** An enrichment layer can facilitate input from external point solutions as well as optimally enable ingestion and integration of internal customer information.
- **Real-time data orchestration:** A real-time data orchestration layer ensures that each discipline can leverage common data and avoid redundant and inconsistent treatment.
- **Risk engine:** Orchestration can leverage a sophisticated risk engine that can ingest intelligence and inputs from multiple internal and external platforms and assess risk.
- **Profiling and decisioning:** Profiling and decisioning layers can perform the contextualization and direct actions on what to do next. Automatic risk-driven triggers such as stepped-up authentication and account freezes can be defined and woven across the customer life cycle.

Data Enrichment, Elevated Contextualization, and Operational Efficiency

Firms realize that fraud, compliance, and credit risk systems contain vital risk-relevant data. Disconnected tools and systems and a lack of visibility across systems impede quick and fully informed decisioning. Translating disparate information into actionable risk intelligence demands a multidimensional customer view built on high-quality data linked together and enriched from multiple internal and external sources. Contextualizing the customer risk journey can often deliver faster risk decisioning, higher approval rates, decreased fraud, less manual effort as well as higher customer satisfaction and loyalty.

Orchestrated technology can enable businesses to become much more agile in the face of evolving threats. Harnessing data into intelligence for effective monitoring, detection, and investigation has been a primary challenge for FIs. Orchestration tools facilitate the integration of advanced analytics, machine learning models, and other technologies that can bring diverse data sets together in an enriched state and deliver much contextual intelligence that can streamline onboarding as well as many facets of ongoing AML compliance and fraud prevention. This can yield sharper financial crime detection and investigation, driving more informed decision-making and better overall outcomes.

Orchestration brings a tighter technology footprint that enables a greater volume of structured and unstructured data to be consumed and combined for accurate, holistic views of the customer and risk. Significant third-party sourced information can further enrich an organization's internal data:

- Firms will be able to leverage their existing knowledge of client behavior to tailor stepped-up authentication decisions down to the customer level. The decision to insert friction will no longer be the product of an if-then rule. Instead, it will factor in the customer's past behaviors to determine whether friction is appropriate.
- The AML compliance team will be able to monitor negative media sources of small businesses. At the same time, the credit risk function will be able to access that intelligence to improve credit decisioning.

Orchestration can promote greater data integrity and consistency by ensuring that the data gathered is more comprehensive, accurate, and shared across disciplines. This enables each risk and business function to meet its mandates while leveraging the common data elements that support identity and avoid redundancy and inconsistency. As certain data sources and systems become less relevant, outdated, or obsolete, required

data changes can be recognized more easily and quickly so that organizations can ensure appropriate assessment and make any required substitution.

Sharing systems across business lines and operations can minimize duplicative requests for similar customer information and streamline the customer experience. New data sources can be identified and ingested into the end-to-end customer life cycle ecosystem.

Many risk executives value the idea of being able to "plug and play" the most appropriate point solutions quickly when a business need or use case arises. A CEO at a global payment processor referenced the fact that, though point solutions address specific needs, integration and orchestration are necessary to maximize the benefits across multiple tools so the tools can talk to each other and share data for greater visibility, higher fraud detection, and lower false positives.

Not only can an orchestration platform enable companies to integrate additional technologies quickly as needed, but it can also theoretically streamline the technology evaluation stage by facilitating value tests among vendors with competitive capabilities without requiring business-line executives to wait in line for internal IT resources. As many organizations are looking to improve their onboarding systems and the checks available within them, they are constantly evaluating current tools to make sure they are performing well, as well as exploring new solutions coming to market. The orchestration capability can also help with cost management by enabling the selective use of external vendors based on data-driven decisions.

Progress Toward an Orchestrated Identity Risk Model

Transforming identity risk management into a more cohesive and orchestrated ecosystem is becoming a necessity for FIs. In the words of many fraud risk executives, FIs are constantly striving to minimize the friction for the 99% of customers who are legitimate while still being able to find the 1% who are not.

This delicate balance requires a faster and sharper intelligence that comes from a cohesive and orchestrated identity risk ecosystem. However, without fully integrated systems or centralized data sources, many FIs lack holistic enterprise views of customer identity. This often leads to insufficient customer risk appreciation, siloed decision-making, and poor outcomes while creating operational lag and resource misallocation.

Implementing a true orchestration identity risk management framework is not a simple task. It is best achieved through a phased approach:

- **Obtain a complete understanding of the needs of each stakeholder throughout the customer journey:** This should include a full inventory of the patchwork of policies, solutions, tools, and data sets that support the collection and synthesis of customer information in building a complete identity and risk profile.
- **Build a long-term strategy to augment, replace, and integrate technology across the mandates of the different risk functions:** An orchestrated yet modular approach enables organizations to identify the necessary tools and data sources and put them together in the way they deem appropriate.
- **Strike a balance among strategic objectives:** Objectives include mitigating risk, reducing expense, optimizing revenue, and maintaining regulatory compliance.
- **Start small and build upon early success to drive to a full suite of orchestrated identity capabilities:** A key benefit of an orchestrated approach is the ability to scale as needed and add and remove building blocks as you learn and progress.

When executed properly, orchestration can drive financial crime prevention, detection, and investigation, adherence to AML regulatory obligations, and risk management while facilitating the onboarding process, improving customer engagement, satisfaction, and loyalty, and elevating operational efficiency.

About Alloy

Alloy solves the identity risk problem for companies that offer financial products. Today, over 500 banks and fintechs turn to Alloy's end-to-end identity risk management platform to take control of fraud, credit, and compliance risks, and grow with confidence. Founded in 2015, Alloy is powering the delivery of great financial products to more customers around the world.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author information

Charles Subrt

csubrt@datos-insights.com