FORRESTER®

Vendor Landscape: Anti-Money-Laundering Solutions, 2017

Digital Innovation And Stricter Regulations Reinvigorate The AML Market

by Andras Cser and Nick Hayes
March 29, 2017 | Updated: April 20, 2017

Why Read This Report

Due to recent global terrorist attacks; corporate corruption; and worsening illicit markets such as drugs, guns, and human trafficking; governments realize the importance of countering criminal and extremist financing. Although anti-money-laundering (AML) regulations have become much stricter, new digital payment options such as peer-to-peer payments, digital wallet, and virtual currencies have made compliance incredibly difficult. This report uncovers the vendor landscape of AML solution providers for transaction monitoring and watchlist management for S&R professionals.

Key Takeaways

Avoid Point Products, Prioritize Complete Solutions
Since AML is a complex and mandatory compliance-related activity, it's important to select a solution that allows for end-to-end governance, including the areas of know your customer (KYC), customer due diligence (CDD), watchlist management (WLM), transaction monitoring (TXM), and operations (visualization, reporting, etc.).

Expect Regulations To Force Better Risk Model Management Practices
Regulators increasingly want to understand how you came to your risk scoring conclusions and want to see repeatable processes and automatic risk scoring model management activities. To satisfy these requirements, AML solutions have to provide risk scoring model versioning and proofing and documented model improvement strategies.

Vendor Landscape: Anti-Money-Laundering Solutions, 2017

Digital Innovation And Stricter Regulations Reinvigorate The AML Market

by Andras Cser and Nick Hayes

with Stephanie Balaouras, Salvatore Schiano, and Peggy Dostie

March 29, 2017 | Updated: April 20, 2017

Table Of Contents

Related Research Documents

Build Digital Risk Insight

The Forrester Wave™: Enterprise Fraud Management, Q1 2016

TechRadar™: Risk Management, Q4 2015

FOR SECURITY & RISK PROFESSIONALS

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

March 29, 2017 | Updated: April 20, 2017

Financial Crime And Corporate Opacity Thrust AML Front And Center

Anti-money-laundering (AML) programs take on even greater importance today for all companies that facilitate meaningful financial transactions for consumer and corporate customers. Due to rapid digital innovation, this includes an increasing number of bank and nonbank financial institutions (NBFIs), such as money service businesses (MSBs), electronic commerce (eCommerce) and auction systems, virtual currencies, mobile payment and digital wallet services, and peer-to-peer (P2P) lending and crowdfunding services. Risk management professionals must oversee related financial activities for AML purposes today because:

› **Organized crime's and extremist groups' financial schemes are more sophisticated.** Global expansion and the diversification of payments make it easier to conduct international commerce, trade assets, manage money movements — and launder money. The United Nations Office on Drugs and Crime (UNODC) estimates that between US$1 trillion and US$2 trillion is laundered globally each year.[1] And less than 1% of the proceeds are seized or frozen.[2] In fact, even global investors managing over $740 billion in assets — while typically advocates of less regulation, not more — recently petitioned the US Congress to pass tougher rules to condemn terrorism financing and make financial obfuscation more difficult.[3]

› **It's hellish to keep pace with exponentially rising data volume and velocity.** The growing number of methods and channels for conducting financial transactions means relevant data resides in more systems and proliferates more rapidly. In turn, this makes data aggregation and integration, along with sound data governance and risk management practices, even more cumbersome. Technology management, compliance, and data scientists must work in tandem to incorporate advanced tactics that provide holistic context while simultaneously establishing and enforcing proper rules for data authoring, tuning, and validation.

› **Regulatory scrutiny is stricter and more comprehensive.** Regulatory bodies worldwide continue to add AML mandates and enforce them more aggressively. Within the past year alone, the US Financial Crimes Enforcement Network (FinCEN) issued new customer due diligence (CDD) obligations and increased statutory penalties for various Bank Secrecy Act (BSA) violations; the European Commission amended and brought forward the transposition date of its Fourth AML Directive (AMLD4) to January 1, 2017; the New York Department of Financial Services (NYADFS) issued final antiterrorism transaction monitoring and filtering program regulation; and the UK introduces a new Criminal Finance Bill in October 2017.[4] The respective penalties can be massive. For example, Western Union agreed to pay $586 million for turning a blind eye as criminals used its service for money laundering.[5]

› **Expanding vendor and business partner ecosystems further AML complexity.** Demanding performance goals increasingly push businesses to expand into new markets and offer new products and services to a greater number of customers. To execute effectively on their expansion

FOR SECURITY & RISK PROFESSIONALS

March 29, 2017 | Updated: April 20, 2017

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

plans, organizations cultivate an ecosystem of strategic partners and other third parties. The combination of rapid expansion of regions, products, customers, and third parties greatly enhances the complexity of AML activities.
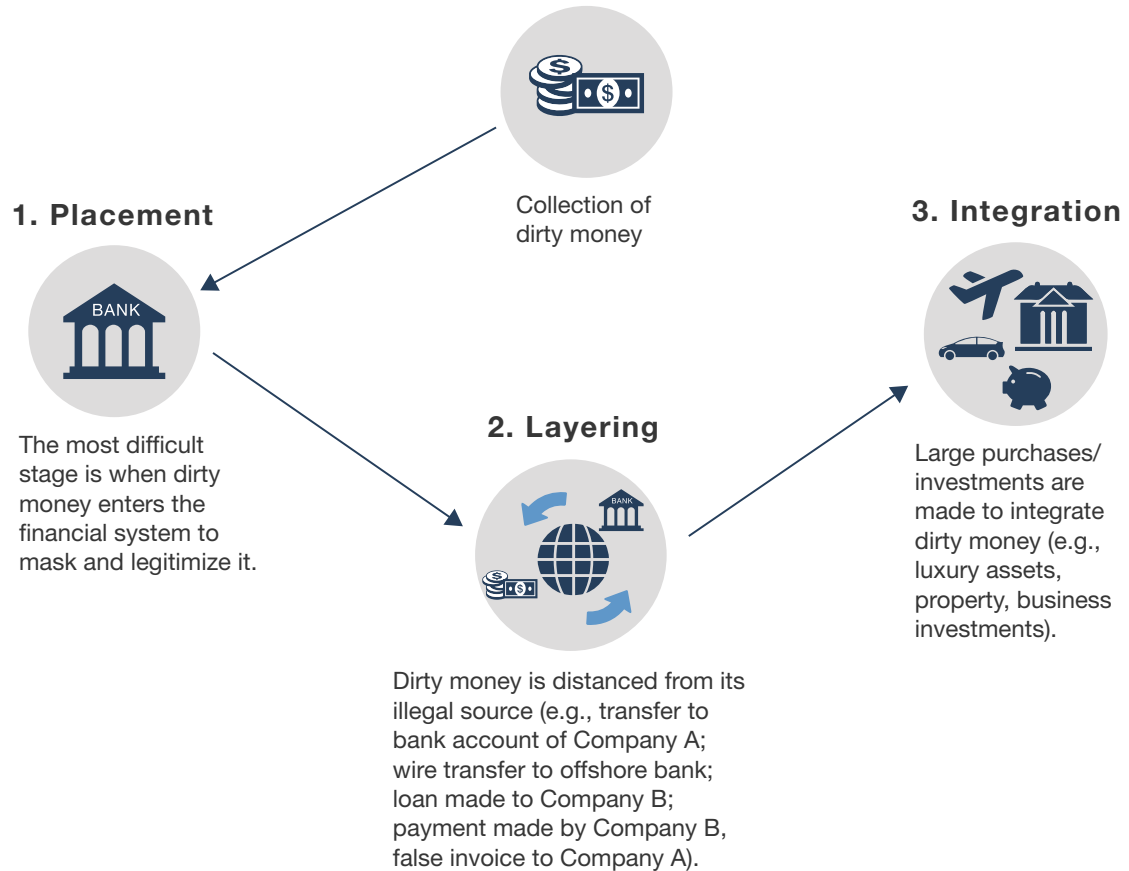
› **Reputational damage due to AML issues can be catastrophic.** In today's unstable and terror-fraught world, cutting funding sources of terrorists and other criminal groups is more than a compliance obligation: It helps save human lives. Effective AML programs deter corporate corruption, human trafficking, illicit drugs and weapons trades, and authoritarian government regimes, just to name a few. However, when firms fail to take their AML obligations seriously, it can cast doubt on their integrity and severely damage reputation and public goodwill. For instance, BNP Paribas' stock price fell 12% over the course of six months in anticipation of what turned into a record $9 billion penalty for violating US sanctions.[6] Companies that don't take proactive AML measures to prevent criminal financing risk turning into corporate pariahs in the public's eye.

AML Techniques Grow More Advanced But Still Rely On Three Core Actions

Despite the new digital payment tools and currencies upending legacy approaches to AML, the core, underlying tactics of money laundering remain the same. According to the United Nations Office on Drugs and Crime (UNODC), money laundering is still a dynamic, three-stage process requiring: 1) "placement," moving money to disassociate with primary criminals; 2) "layering," further obfuscation of dirty money linkages; and 3) "integration," legitimizing the money for the criminals' use (see Figure 1).[7] Since this fundamental scheme remains intact, AML leaders should aim to modernize existing AML tools and tactics first, before considering new models or approaches.

FOR SECURITY & RISK PROFESSIONALS

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

March 29, 2017 | Updated: April 20, 2017

FIGURE 1 A Typical Money-Laundering Scheme Has Three Phases

1. Placement

Collection of
dirty money

3. Integration

The most difficult
stage is when dirty
money enters the
financial system to
mask and legitimize it.

2. Layering

Large purchases/
investments are
made to integrate
dirty money (e.g.,
luxury assets,
property, business
investments).

Dirty money is distanced from its
illegal source (e.g., transfer to
bank account of Company A;
wire transfer to offshore bank;
loan made to Company B;
payment made by Company B,
false invoice to Company A).

Conduct AML Vendor Selection With A Holistic AML Architecture

Many AML solutions are aging, inflexible, and expensive to maintain, and produce high false-positive
rates. This results in costly overhead, risk visibility gaps, program inefficiencies, and a prolonged and
diminished customer transaction experience. However, switching or adopting new AML technologies
is no easy task either. They're complex and costly implementations that require extensive systems and
data integration; ongoing authoring, tuning, and testing of risk management models and procedures;
alignment to numerous regulations and geographic jurisdictions; and strict data protection and access
controls.[8] To select the right AML technologies to improve your program, consider the broader financial
crimes prevention and risk management architecture within which AML sits, including (see Figure 2):

› **Customer identification and due diligence for KYC and CDD purposes.** Whom you allow
to interact and transact with your firm has a huge impact on how well you can intercept money
laundering and terrorist financing and meet compliance regulations. KYC and CDD involve: 1)
identity verification and disambiguation; 2) collecting and archiving customer documentation, such

FOR SECURITY & RISK PROFESSIONALS

March 29, 2017 | Updated: April 20, 2017

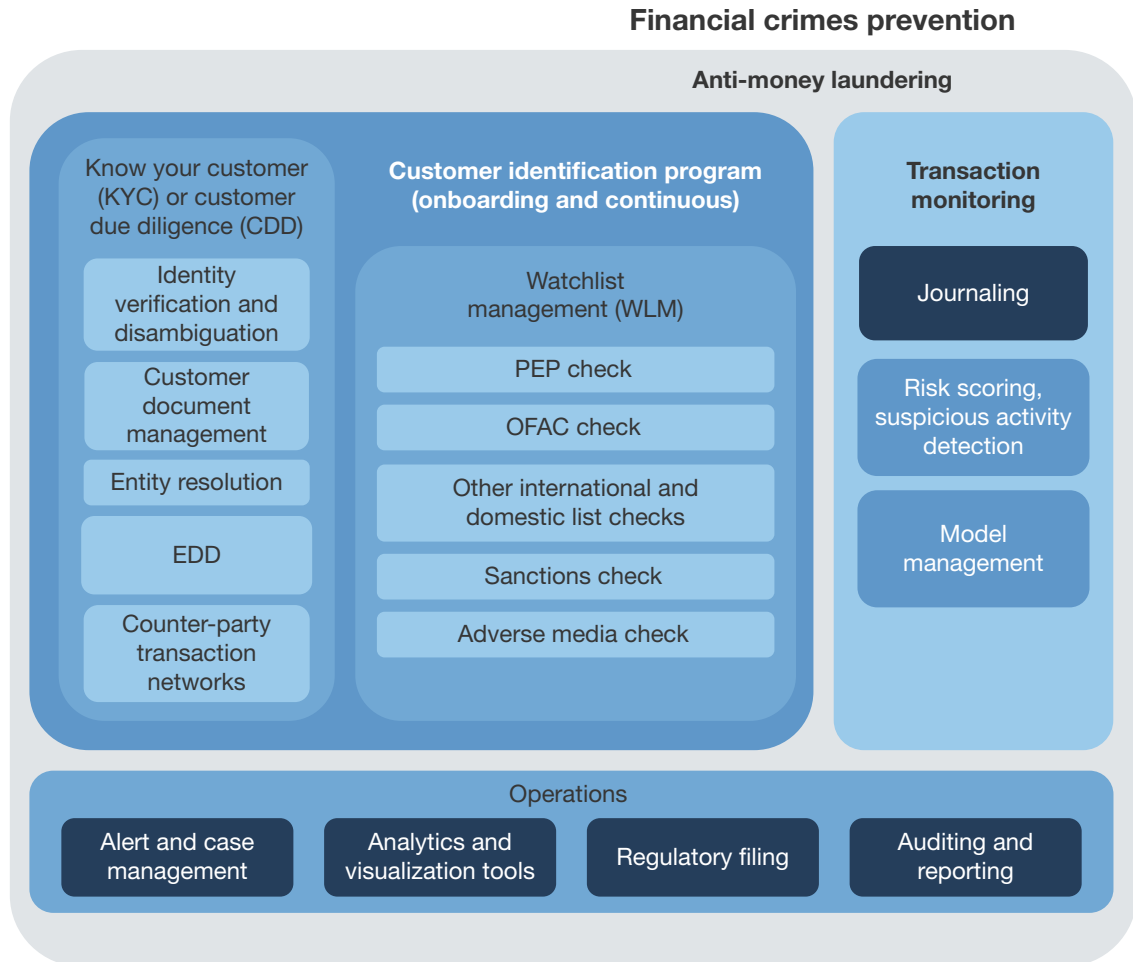**Vendor Landscape: Anti-Money-Laundering Solutions, 2017**
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

as copies of ID cards, proof of address, etc.; 3) entity resolution (resolving inadvertent or deliberate variances in name spellings); 4) enhanced due diligence (more-extensive checks for customers at high AML risk); and 5) counter-party transaction networks (understanding the whole ecosystem and path of transactions).

› **Watchlist management (WLM) to screen government and proprietary sanctions lists.** During onboarding and in transactions, you have to understand if a customer entity or identity: 1) is on a politically exposed persons (PEP) list; 2) is on the Office of Foreign Asset Control (OFAC) list; 3) is on other international and domestic lists; 4) is subject to sanctions; or 5) has been covered adversely by the media. WLM is tricky: It has to ensure that all AML system components can efficiently and effectively crosscheck potential and existing customer identities in the firm's systems against relevant sanctions lists, based on region, language, regulation, etc. In the US, KYC and WLM are part of firms' Customer Identification Program (CIP).

› **Transaction monitoring (TXM) for real-time risk scoring, alerts, and interdiction.** For in-scope transactions, such as account openings, payments, deposits, or insurance claims, TXM performs: 1) journaling (creating a paper trail of every transaction in the AML system); 2) risk scoring and suspicious activity detection (creating a risk score for transactions, using rules, machine learning, and statistical algorithms); and 3) risk scoring model management, maintenance, verification, and audit — mandatory in most AML regimes.[9] Transaction monitoring looks for suspicious patterns of activities, such as too much or too little activity in an account or excessive cross-border transactions, and ensures the firm has an ongoing risk assessment framework for all transactions.

› **Operations to ensure consistent process, reporting, and compliance.** Operations is a collection of tools and processes that make the entire AML process a repeatable, auditable and well-governed activity. Components of operations include: 1) alert and case management (role-based routing, analyzing, investigating, following up on suspicious activities in a structured manner); 2) analytics and visualization tools that allow investigators to peek into complex transactional flows, entity profiles, and relationships; 3) regulatory filing (submitting defensible and well-investigated Suspicious Activity Reports [SARs]); and 4) auditing and reporting for internal and external auditors and industry regulators.

FOR SECURITY & RISK PROFESSIONALS

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

March 29, 2017 | Updated: April 20, 2017

FIGURE 2 AML Taxonomy Diagram

Financial crimes prevention

Anti-money laundering

Know your customer (KYC) or customer due diligence (CDD)
- Identity verification and disambiguation
- Customer document management
- Entity resolution
- EDD
- Counter-party transaction networks

Customer identification program (onboarding and continuous)
- Watchlist management (WLM)
- PEP check
- OFAC check
- Other international and domestic list checks
- Sanctions check
- Adverse media check

Transaction monitoring
- Journaling
- Risk scoring, suspicious activity detection
- Model management

Operations
- Alert and case management
- Analytics and visualization tools
- Regulatory filing
- Auditing and reporting

AML Suites And Analytical Investigation Tools Vie For Attention

The AML market is fairly mature (see Figure 3). Vendors such as BAE Systems, FICO TONBELLER, Fiserv, NICE Actimize, Uncharted, and SAS provide complete solutions with holistic transaction monitoring. Attivio and OutsideIQ and other analytics engines that monitor and analyze AML activity rely on other tools for process management and cross-functional team coordination. Meanwhile, IdentityMind predominantly offers digital identity verification data services (e.g., name, address, SSN, or IP geolocation) (see Figure 4). Forrester uncovered an AML market in which:

› **Attivio offers analytics tools for AML investigation and reporting.** The vendor's solution creates a unified semantic compliance catalog across internal and external sources (including web-accessible applications), using file traversing, content enrichment, and indexing technology native to the vendor's data unification platform. The focus of the on-premises-only solution is on

FOR SECURITY & RISK PROFESSIONALS

March 29, 2017 | Updated: April 20, 2017

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

payment transactions, and it does not perform transaction risk scoring. Instead, it provides AML investigators with tools for evidence gathering and narrative reporting.[10] The solution integrates with procedural workflow and generates pertinent case evidence, supporting audit, review, and machine learning for its transaction alerting models.

› **BAE Systems offers a complete AML solution for banking and insurance.** The anti-money-laundering solution ingests customer, product, and transactional data, together with supplementary reference information and external watchlist data, and builds profiles of financial and nonfinancial activity across the entire customer base. Automated AML risk scoring uses rules, statistical models, social network analysis, fuzzy matching, and entity resolution to alert activity involving money laundering. The solution is available as on-premises and SaaS, has no own watchlists (but natively integrates with customer-provided and third-party data sources), and, in Forrester's opinion, has a high price tag: Forrester estimates average deal sizes between $500,000 and $750,000 perpetual.[11]

› **FICO TONBELLER has a large, mainly European customer base.** The solution is grouped into three tiers: 1) Siron configuration; 2) Siron database, with Siron scoring connected to the core banking system; and 3) Siron analysis application (case management and regulatory filing). It has one of the largest install bases of solutions we reviewed (1,200 customer organizations). The solution is available as on-premises and SaaS, and it requires that clients transform transaction data from their business systems to Siron's data schema. It has strong integration with watchlist data providers such as Dow Jones, LexisNexis Risk Solutions, and World-Check. Forrester expects that the vendor will deepen technical integration and analytics best practices sharing between its AML and enterprise fraud management solutions.

› **Fiserv comes with an extensive connector set to third-party data sources.** The all-around solution provides transaction monitoring, watchlist filtering, alert and case management, and regulatory and managerial reporting. Risk scoring uses behavioral analysis and predictive modeling for money laundering and terrorist financing detection and mitigation. Real time WLM uses fuzzy and Soundex algorithms. The solution includes integrated alert and case management and regulatory reporting. Risk scoring offers only unsupervised but no supervised training. Forrester's clients mention that the on-premises-only solution is complex and can be costly to implement in production. The solution has a large hosted and on-premises install base of 300 customer organizations.

› **IdentityMind provides eDNA — a shared electronic human profile data service.** The solution provides investigators with a complete understanding of the identity behind transactions — it extracts identity parameters from the transaction and correlates it across all clients. It also aggregates financial behaviors, identity validation, affiliation and affinity, and other values in a "reputation" concept yielding an overall assessment of the identity behind the transaction. All services are available through a restful API. The solution is SaaS only, provides case management but no coverage for insurance transactions or own unsupervised machine learning. Forrester estimates average deal sizes at $30,000 to $50,000 per year. The solution has a medium sized install base of 80 to 100 organizations.

FOR SECURITY & RISK PROFESSIONALS

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

March 29, 2017 | Updated: April 20, 2017

› **NICE Actimize has a large mindshare.** The solution has coverage for analytics-based detection, alerting, workflow processing, and reporting of suspicious activity. The solution is available both as on-premises and SaaS. It mandates the vendor's data model schema — so customers have to transform their own transactional data to the vendor's data model for risk scoring as the solution provides no external data aggregation. The install base of the on-premises solution is 240 to 260 organizations, while the SaaS solution, launched in Q2 2016, has fewer than five customers in production.[12] The solution has a large mindshare with Forrester's clients.

› **OutsideIQ offers a machine-learning-based risk scoring platform with data integration.** DDIQ is a risk-based cognitive computing platform that combines automation with the skills of a human researcher to uncover and analyze regulatory risks of a subject by looking at all available public data about a subject while preparing auditable reports. The predominantly SaaS solution has no watchlist management and a relatively small install base of an estimated 50 to 70 organizations. Vendor claims SOC2 compliance. The solution is entirely based on machine learning algorithms and does not require or provide features for rules-based risk scoring.

› **SAS provides AML for banking and insurance firms.** The solution provides entity resolution and fuzzy matching to integrate customer and transaction data from numerous data sources to create a single view of party risk. The solution has rules, anomaly detection, predictive analytics, and entity link analysis to compare a subject's activity with their historical profile. KYC information, peer groups, risk rating, and watchlist matching provide more accurate coverage and identify persons, organizations, or high-risk jurisdictions that represent regulatory risks. The solution does not provide its own watchlist data (it integrates with major providers), and Forrester customers find the solution costly to implement. Forrester estimates the install base of the on-premises solution to be 140 to 150 organizations and the SaaS solution to be three to six organizations.

› **Uncharted's Influent offers data visualization and social network analytics.** The solution is especially designed to analyze and display transaction volume and temporal patterns. It can ingest and fuse data from disparate sources. The on-premises-only solution (SaaS planned) does not have watchlist management, transaction monitoring, or case management.[13] The vendor has no implementation services partners; Forrester estimates the vendor's annual revenues from Influent to be between $500,000 and $1 million. Customers can also use the solution outside of AML for other investigation (fraud management, cyberthreat incident response, etc.).

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

FIGURE 3 AML Vendor Solution Comparison

The spreadsheet associated with this figure contains additional data.

Out of the box, the vendor solution on its own supports:	Attivio	BAE Systems	FICO	TONBELLER	Fiserv	IdentityMind	NICE Actimize	OutsideIQ	SAS	Uncharted
Transaction monitoring and risk scoring		●	●	●	●	●	●	●	●	
Multitenancy		●	●		●	●	●	●	●	
Sanctions and PEP screening data			●		●	●				
Investigator feedback to tune risk scoring via ML	●	●	●			●	●	●		
Payment transactions risk scoring	●	●	●		●	●	●		●	
Insurance transactions risk scoring		●	●		●		●		●	
Case management		●	●		●	●	●		●	
Rules in transaction risk scoring is exposed to customers	●	●	●		●		●		●	
Unsupervised ML is exposed to customers	●	●					●	●		
Supervised ML is exposed to customers	●	●			●	●	●			
Watchlist filtering functionality		●	●		●	●	●	●	●	
Entity resolution		●				●	●	●	●	●
Social network and link analysis		●	●			●		●	●	●
Predefined bidirectional data connectors			●		●		●		●	

Legend

| | Vendor's solution does not support | | Support is partial or via partnership (see detailed XLS) | ● | Vendor's solution supports this |

FOR SECURITY & RISK PROFESSIONALS

March 29, 2017 | Updated: April 20, 2017

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

FIGURE 4 AML Vendor Landscape

The spreadsheet associated with this figure contains additional data.

Forrester estimates are highlighted in green.

AML	Attivio	BAE Systems	FICO TONBELLER	Fiserv
Top services partners	N/A	N/A	ACC, Bank Verlag, Bateleur Consulting, B&F Soft, Blitz, ELAM, Fasyl, IMTF, NetBit, Printec, RD Tex, Vitalis	N/A
Average deal size	$300K to $450K perpetual	$500K to $750K perpetual (excluding sanctions, PEP, CDD)	$400K to $500K perpetual	$600K to $750K perpetual (excluding sanctions, PEP, CDD)

AML	IdentityMind	NICE Actimize	OutsideIQ	SAS	Uncharted
Top services partners	Augur, Ethoca, Experian, Mitek	Deloitte, Genpact, PwC	Exiger, Genpact, Intellect Design, Pega	Accenture, Capgemini, Zencos	N/A
Average deal size	$30K to $50K a year	$100K to $400K a year	$250K a year	$250K-$350K for midsized institutions	$40K to $50K a year

On-premises	Attivio	BAE Systems	FICO TONBELLER	Fiserv	IdentityMind	NICE Actimize
Pricing	$100 to $150 per investigator a year	$100 to $150 per investigator a year	Based on the size of the balance sheet and number of accounts/transactions	Based on the size of the balance sheet of the customer	N/A	Average deal size: $100K to $500K perpetual
Customers in production	10 to 15	160 to 180	1,200	300	0 to 5	240 to 260
Revenue	$500K to $1M a year	$15M to $20M/year	$20M to $25M a year	$20M to $25M a year	$100K to $500K/year	$50M to $100M/year

FOR SECURITY & RISK PROFESSIONALS

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

March 29, 2017 | Updated: April 20, 2017

FIGURE 4 AML Vendor Landscape (Cont.)

On-premises	OutsideIQ	SAS	Uncharted
Pricing	N/A	Licensing based on assets under management for financial institutions. (The first year system fees range from $200K for a $10B asset institution to $1.5M for a trillion dollar asset institution.)	$5K a year per user, plus configuration and integration
Customers in production	0 to 5	140 to 150	3 to 5
Revenue	N/A	$45M to $48M a year	$500K to $1M a year

SaaS	Attivio	BAE Systems	FICO TONBELLER	Fiserv	IdentityMind	NICE Actimize	OutsideIQ
Pricing	No SaaS solution	$100 to $150 per investiga-tor a year	SaaS solution commercialized — pricing unavailable	No SaaS solution	AML: 3-8c/txn KYC: 50-250c/txn	Value based: client size and usage (# of accounts)	$20 a year per user
Customers in production	N/A	3 to 5	10	N/A	80 to 100	1 to 5	50 to 70
Revenue	N/A	$1M to $2M/year	$1M to $2M a year	N/A	$3M to $5M a year	$500K to $1M a year	$700K to $1M/year

SaaS	SAS	Uncharted
Pricing	Based on assets under management for financial institutions. The average subscription cost is $100K per year.	No SaaS solution. Forrester expects planned SaaS solution pricing: $5K a year per user, plus configuration.
Customers in production	3 to 6	N/A
Revenue	$4M to $5M a year	N/A

FOR SECURITY & RISK PROFESSIONALS

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

March 29, 2017 | Updated: April 20, 2017

Recommendations

Synergize Your Data Between Fraud Management, GRC, And AML

AML implementations usually take 12 to 18 months to complete their first phase, even at organizations with previously established and operationalized AML governance programs. Beyond proper scoping, to ensure a successful AML implementation, risk management pros need to:

› **Synergize with other compliance and fraud initiatives.** Many times, other departments (fraud management, information security, marketing, compliance, GRC, lines of business) already have set up (costly) data integration between business transaction processing systems and their platforms. Redoing all the implementation work is wasted effort: Try to synergize and build on results of these teams — even if you can't reuse their risk scoring methodologies. Identifying data requirements and standardizing implementation methods early (i.e., using generic data collection connectors, avoiding excessive customization) definitely helps with the data integration process.

› **Combine rules and machine learning in risk scoring — and focus on explanations.** Unlike fraud management, AML is all about explaining to regulators and auditors why you came to a certain disposition of a transaction.[14] When filing a Suspicious Activity Report on a client or transaction, you must have all your evidence lined up and explanations ready for auditors, regulators, and law enforcement. Forrester's interviewees mention that solutions that purely do machine learning or statistical risk scoring don't always do a good job of explaining the risk score to the investigator or analyst. A better strategy is to use rules-based methods (augmented with visual investigation tools) to be sure to reduce the number of false positives. Tuning the solution to cope with transaction volumes is critical.

› **Hire AML analysts with investigative and financial services backgrounds.** Good AML governance demands not only deploying top-notch AML solutions but also vetting and hiring the right AML investigative talent. AML analysts have to be efficient in gathering, reviewing, and linking vast amounts of client information to confirm suspicious activity. Training AML analysts is not easy: It takes anywhere from 18 to 24 months of peer and supervisor coaching for a newly hired analyst to become fully productive. Analysts need to be able to write informative SARs that tell a comprehensive story to the law enforcement agency reading the SAR. Finally, analysts need to be familiar with constantly changing regulations, expectations, and typologies. They need to attend financial crime training not only internally but externally to keep up with the changing landscape of threats and regulations.

FOR SECURITY & RISK PROFESSIONALS

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

March 29, 2017 | Updated: April 20, 2017

New Payment Types Will Raise AML Costs

Criminals will use any product or service where there is an opportunity to move and launder money. In the next 18 to 24 months, Forrester expects that:

› **More and more regulations will be forthcoming.** In the wake of recent terrorist attacks, as regulators such as FinCEN, OCC, CESF, BaFin, FMA, EU, and many more see criminal activity getting smarter and more digital-savvy, they will tighten existing regulations and legislate and enforce new ones. Forrester expects that as the number of regulations increases the complexity, and initial and ongoing costs of maintaining AML solutions will also increase by 15% to 25%.

› **Criminals will quickly target new channels, catching most firms off guard.** As new types of peer-to-peer payments (P2PP) and digital wallets (DW) become the norm, banks and insurance carriers have to add these types of payments and channels to their existing AML management regimes. Banks will also have to pay close attention to new incomes coming from recently legalized marijuana sales. As a result, all firms face huge reputational risks and higher fines in case of deficiencies in money laundering prevention and fulfilling compliance obligations (such as the KYC principle). Firms with immature AML schemes (for example, firms in the insurance and eCommerce verticals) may be slow to react to this change.

› **Vendors that include new data sources will come out on top.** Beyond identity verification, vendors such as IdentityMind and LexisNexis Risk Solutions will offer a broader set of data sources based on phone number, device identities, etc. Many of the government sanctions lists are well known and commonplace for all AML solutions (e.g., OFAC, United Nations Security Council, etc.), but there are other proprietary data sets, such as Dow Jones Watchlist, LexisNexis Risk Solutions WorldCompliance, and Thomson Reuters World-Check, as well as social media and negative news monitoring that complement existing sources and add further risk context. To include and enrich these new data sources, vendors such as Fiserv, IdentityMind, and LexisNexis Risk Solutions will provide better AML detection rates and will increase their market share.

› **AML will incorporate advanced data analytics, risk visualizations, and simulations.** To optimize AML data, some vendors such as OutsideIQ can already apply sophisticated data science techniques to augment risk context, such as automated data flow analysis, social network analysis, machine learning, and data clustering. AML vendors with cutting edge analytics and investigation capabilities (e.g., Attivio and OutsideIQ) may leap forward, while legacy AML vendors, such as Fiserv or NICE Actimize, will have to revamp their legacy AML solutions to keep up.

FOR SECURITY & RISK PROFESSIONALS

March 29, 2017 | Updated: April 20, 2017

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Supplemental Material

Online Resource

The underlying spreadsheets detailing the tables in Figure 3 and 4 are available online. Please click "Save" in the upper right hand corner of the figure to download the Microsoft Excel spreadsheet.

Endnotes

[1] Source: "Money-Laundering and Globalization," United Nations Office on Drugs and Crime (https://www.unodc.org/unodc/en/money-laundering/globalization.html).

[2] Source: "Illicit money: how much is out there?" United Nations Office on Drugs and Crime, October 25, 2011 (https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html).

[3] Source: "Chancing It: How secret company ownership is a risk to investors," Global Witness, September 7, 2016 (https://www.globalwitness.org/en/reports/chancing-it/).

FOR SECURITY & RISK PROFESSIONALS

Vendor Landscape: Anti-Money-Laundering Solutions, 2017
Digital Innovation And Stricter Regulations Reinvigorate The AML Market

March 29, 2017 | Updated: April 20, 2017

[4] Source: Melissa R. H. Hall and Ignacio A. Sandoval, "Bank Secrecy Act Violations Now Come with Significantly Higher Penalties," The National Law Review, June 30, 2016 (http://www.natlawreview.com/article/bank-secrecy-act-violations-now-come-significantly-higher-penalties).

Source: Patricia Taylor, "The Fourth EU Anti-Money Laundering Directive – Impact on Investment Funds," William Fry, October 7, 2016 (http://www.williamfry.com/newsandinsights/news-article/2016/10/07/the-fourth-eu-anti-money-laundering-directive-impact-on-investment-funds).

Source: Ben Dipietro, "The Morning Risk Report: New York Law Adds Teeth to Federal AML Oversight," The Wall Street Journal, January 24, 2017 (http://blogs.wsj.com/riskandcompliance/2017/01/24/the-morning-risk-report-new-york-law-adds-teeth-to-federal-aml-oversight/).

Source: Emma Rumney, "UK plans renewed effort to eliminate its role in global corruption," Public Finance International, November 4, 2016 (http://www.publicfinanceinternational.org/news/2016/11/uk-criminal-finance-bill-could-be-most-significant-30-years).

[5] Source: Joel Schectman and Diane Bartz, "Western Union admits to aiding wire fraud, to pay $586 million," Reuters, January 20, 2017 (http://www.reuters.com/article/us-usa-western-union-settlement-idUSKBN1532RL).

[6] Source: Mark Thompson and Evan Perez, "BNP Paribas to pay nearly $9 billion penalty," CNN Money, July 1, 2014 (http://money.cnn.com/2014/06/30/investing/bnp-paribas-sanctions-fine/).

[7] Source: "The Money-Laundering Cycle," United Nations Office on Drugs and Crime (https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html).

[8] AML regulations usually override privacy requirements. Most countries' laws stipulate that data used for AML cannot be shared, is accessed only on a need-to-know-basis in the firm, and cannot be used for marketing purposes.

[9] Most vendors offer their own professional services or partnerships with system integrators to create, augment, and manage statistical models and supervised and unsupervised machine learning algorithms for risk scoring.

[10] Note that Attivio partners with NICE systems for providing end-to-end AML solutions.

[11] As with other vendors, customization for compliance may introduce great variability to total project costs.

[12] Collaborating with these initial customers, NICE Actimize intends to develop data adapters for core banking solutions.

[13] However, the solution provides integrations for these areas.

[14] In fraud management, false positives usually decrease revenues and drive customers away from you, but, unlike in AML, there is no permanent negative record or SAR that can impact someone's life.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

› Core research and tools
› Data and analytics
› Peer collaboration
› Analyst engagement
› Consulting
› Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals	**Technology Management Professionals**	**Technology Industry Professionals**
CMO	CIO	Analyst Relations
B2B Marketing	Application Development & Delivery	
B2C Marketing	Enterprise Architecture	
Customer Experience	Infrastructure & Operations	
Customer Insights	› Security & Risk	
eBusiness & Channel Strategy	Sourcing & Vendor Management	

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.