LICENSED FOR INDIVIDUAL USE ONLY

The Top Trends Shaping Anti-Money Laundering In 2020

Robotic Process Automation, Cryptocurrencies, Real-Time Detection, And KYC Processes Gain Importance

by Andras Cser
August 10, 2020

Why Read This Report

With new real-time transactions gaining popularity and new legalized product markets (such as cannabis) emerging, anti-money-laundering (AML) regulations are getting tougher and more complex. This report highlights the top trends in AML for know your customer, watchlist management, screening, and transaction monitoring case management and provides guidance how anti-money laundering and fraud management pros should respond.

Key Takeaways

Third-Party Data Integration Is Driving AML Deployments

Your decisions are only as good as the data you base them on. We increasingly see firms using productized vendor integration between their AML solution and third-party watchlists, and also device ID and IP address reputation hotlists, to deliver better decision support.

AML And Fraud Case Management Are Slowly Unifying

Firms face pressure to unify AML and fraud case management to reduce the costs of data integration, model development, and investigative labor. Since AML and fraud management both use pattern and behavioral anomaly identification, it makes sense to break down their operational silos and establish a unified fraud plus AML strategy (FRAML).

Handling AML Risk Scoring Models Is Getting Harder And Attracting More Scrutiny

Today's financial institutions (FIs) have to maintain an agile and explainable process for continually improving their models. Lifecycle of model development has to be explicitly supported by AML solutions from the ground up.

This PDF is only licensed for individual use when downloaded from forrester.com or reprints.forrester.com. All other distribution prohibited.

The Top Trends Shaping Anti-Money Laundering In 2020

Robotic Process Automation, Cryptocurrencies, Real-Time Detection, And KYC Processes Gain Importance

by Andras Cser
with Merritt Maxim, Benjamin Corey, and Peggy Dostie
August 10, 2020

Table Of Contents

Related Research Documents

The Forrester Wave™: Anti-Money Laundering Solutions, Q3 2019

The Forrester Wave™: Enterprise Fraud Management, Q3 2018

The Security Of Cryptocurrencies

Share reports with colleagues. Enhance your membership with Research Share.

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

© 2020 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

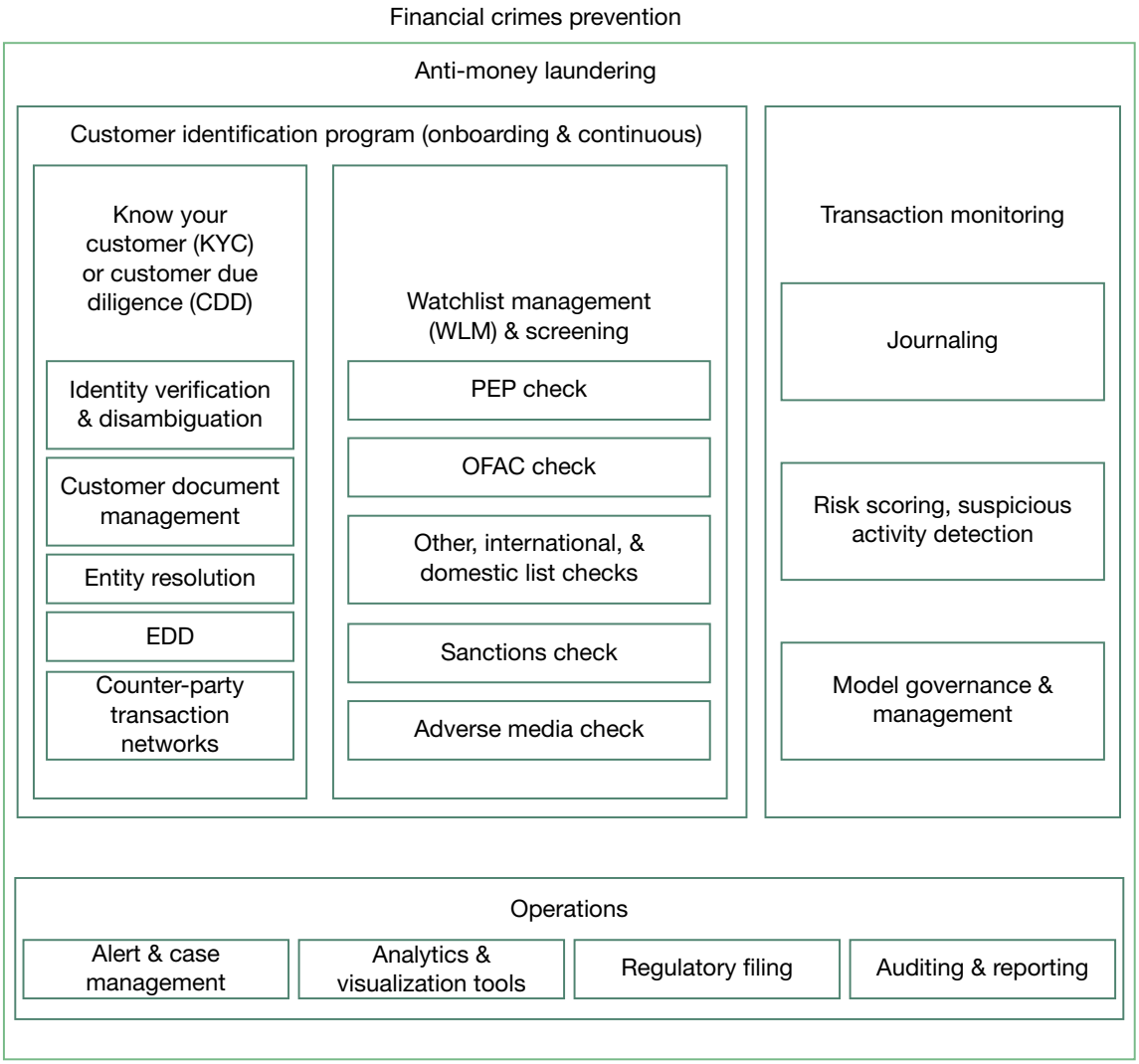
Regulations And Online Customer Acquisition Drive AML Expansion

Preventing and reporting money-laundering activities is a key issue for financial institutions, insurers, gaming and gambling organizations, utilities, and telecoms, especially during periods of economic and budgetary constraints such as today's. Forrester expects that, in the next three to four years, firms that enable customers to create an account and store and move money in and out of that account will have to comply with AML regulations in their appropriate jurisdiction. In this document, we highlight the most relevant trends impacting the entire process and tool set of AML, looking at know your customer (KYC), customer due diligence (CDD), watchlist management and screening, transaction monitoring, and operations (including alert and case management) (see Figure 1). The projected expansion of AML is occurring because:

- **Effective AML regimes contribute to brand reputation and protection.** Ensuring that your firm has a solid AML program is fundamental to securing and maintaining your brand reputation. AML failures result in regulatory fines, sanctions, negative media attention, tarnished brand reputation, defecting customers, and loss of trust from banks you work with for wire transfer.
- **Regulators are creating more-complex compliance regulations at breakneck speeds.** The list of mandates related to AML is getting longer every year. Regulators are responding to and keeping up with an increasing number and sophistication of money-laundering schemes. New AML regulations effective January 10, 2020 mandate that new kinds of organizations, beyond traditional financial services, must perform AML activities.[1]
- **Increasing online customer acquisition is requiring more-efficient KYC processes.** In the current global economic downturn, increased online consumer engagement places a heavy burden on fast, frictionless, and low-cost KYC and customer due diligence (CDD) operations, watchlist management, and screening. Firms must maintain effective AML risk scoring and case management to meet the increased customer acquisition without making significant investments in additional human analysts and investigators.
- **New payment transaction types allow money launderers to apply smarter schemes.** The adoption of peer-to-peer payments via Google Pay, PayPal, PopMoney, SquareCash, Venmo, Xoom, Zelle, etc. complicates tracing funds and catching money-laundering activities. Cryptocurrency payments are on the rise — along with related money-laundering activity.[2] This allows money launderers to employ covert new account opening, layering and structuring schemes to facilitate faster and less detectable money laundering.
- **Data integration woes still impair AML responsiveness and tooling.** Financial institutions and other firms subject to AML regulations struggle to integrate their internal and external transactional and security data sources into the AML solution. Data schema limitations of AML solutions often mean that FIs use considerable IT and development resources to transform data from transactional and security to be usable in the AML solution. This is not only expensive but also limits the company's ability to perform real-time AML checks because they have to wait for the nightly data import and consolidation batch to complete.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 1 Anatomy Of AML Programs



Online Physical Document Verification Transforms KYC And CDD

Our interviewees estimate that, on average, they see a 10% to 15% increase in online new account registrations compared to a year ago. This places a significant burden and responsibility on the institution's KYC, CDD, and watchlist management (WLM) processes.

CDD/ECDD Requirements Force AML Pros To Expand Their Thinking On Identity Verification

CDD processes are mandated by regulators and force FIs and other firms to conduct detailed inquiries into the identity data of all their prospective customers.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Identity resolution cuts down the number of duplicate customer registrations.** Having a complete picture about a new customer starts with resolving their identity. This means looking for other similarly sounding customer names that your company already knows about to determine if the registrant, by mistake or deliberately, wants to open a new, unrelated account, which should be merged with the original account. If there are duplicate registrations or the newly registered customer name is too similar to an already existing customer name, your AML department needs to be notified automatically, or if needed, manually investigate these issues. Identity resolution solutions such as Amperity, Axciom, and Infutor improve not only registration but also existing customer data quality.[3]
- **FIs increasingly use IDV based on phone, email, social and physical document data.** Once the bank disambiguates its applicant's identity, it has to perform identity verification (also known as vetting and proofing); this ensures that the FI knows precisely who it's dealing with. Identity verification (IDV) helps with preventing stolen and synthetic identity theft. While legacy and expensive IDV methods based on credit file headers (Experian, Equifax, and TransUnion) still reign supreme, our interviewees indicated that more and more they are testing IDV based on phone number, email, device ID reputation, as well as behavioral biometrics.[4] Accuity, Mitek, Onfido, Trulio, and others provide solutions that allow for physical document verification online (scan document, take selfie, compare). IDV solutions also allow integration with B2B merchant onboarding processes and provide identity linkage graphs to connect identities on multiple application forms.
- **Behavioral biometrics and device ID expose linkages between people and machines.** Behavioral biometrics solutions (BehavioSec, Biocatch, Shape Security, etc.) look at the patterns of keystrokes, mouse movements, clicks, mobile screen swipes, etc. during a user's completion of an application form to provide signals whether the application is fraudulent or legitimate. Why? Because fraudsters, copying data from a spreadsheet, may have to think about the gender or date of birth of a stolen identity, while legitimate users have no trouble remembering these personally identifiable data attributes. FIs also increasingly use device ID reputation and linkages from vendors such as Kount, LexisNexis, or TransUnion to understand if a fraudster is completing hundreds of applications using the same desktop or mobile device.[5]
- **Identifying falsified account statements revolutionizes document management.** For a long time, document management (collecting, scanning, storing and retaining customer documents, such as ID cards, proof of address utility bills, credit card statements, etc.) has been an arduous process that merely checked a compliance box. We now see FIs demanding that document management solutions they use in the AML regime provide intelligent and speedy optical character recognition, link analysis, and fraudulent document identification. We also see vendors that traditionally scan physical documents expanding into mobile app-based document capture and biometric authentication such as facial print.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

WLM And Screening Can Only Cope With More Transaction Types When Using AI

WLM and screening refer to downloading, filtering, distributing internally, updating, and otherwise operationally managing public or commercial lists of politically exposed persons and entities that fall under the scrutiny of the Office of Foreign Asset Control (OFAC) and adverse media lists. Screening allows FIs to see if their prospective and existing customers are named in those watchlists and consequently refuse service, conduct enhanced customer due diligence (ECDD), or report the prospective customer to the proper authorities.

- **Productized third-party list source integration.** To improve the accuracy of decisions based on watchlist data, all AML vendors have planned AML product roadmap updates to include integration from more watchlists and their updates from Accuity, Bank of England, ComplyAdvantage, Dow Jones, LexisNexis, OFAC, Refinitiv, Thomson Reuters, and others. Integrations should provide fuss-free use, filtering and merging of entities on the lists into a cohesive and repeatably updateable, regression-tested set of watchlists. FIs often mention that they need to filter watchlists based on geographical requirements and internal lines of business. Many AML vendors also plan to support more national currencies and languages.
- **Refining matching algorithms using AI and natural language processing (NLP).** We are seeing vendors adding capabilities for real-time, artificial intelligence (supervised and unsupervised learning) algorithm-backed matching applicants' names to watchlist elements. Solutions support integrating open source risk scoring models such as H2O.ai, Octave, SciPy, R, etc.). NLP algorithms also help with fuzzy matches or names transliterated between non-Latin alphabets and Latin alphabets. Visualization, link analysis of watchlist data (even before link analysis of transaction monitoring data) also greatly helps to preventively identify and protect against money launders at application/registration time.
- **Support for more types of transactions.** As ACH, Fedwire, peer-to-peer payments, the EU's SEPA, and SWIFT payment transaction volumes grow, auditors and regulators are requiring that FIs provide direct support for these transactions. Real-time payments, increasingly the norm worldwide, put excessive strain on existing screening systems' performance and stability; as a result, AML vendors such as FICO and Verafin now offer cloud-based, elastically scalable screening processes to deal with this surge.

Model Governance And Explainability Dominate Transaction Monitoring

Transaction monitoring ensures that FI can meet regulators' mandates to risk score, identify, investigate, and, if necessary, block customers' transactions. We identified the following trends in this area:

- **Governance requirements tighten.** Regulators and auditors are pressing for model governance: The FI's risk scoring model developers and AML hosting vendors have to create a well-documented process for designing, testing, implementing and rolling back models. This includes exact descriptions and version control for: 1) model parameters; 2) model algorithm selections; 3)

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

model validation; 4) supervised or semi-supervised model training documentation; and 5) expected and realized model performance changes/improvements. OCC 201-12 and ECB both mandate model governance, and Forrester expects scrutiny to increase in this area.[6] Agile model building (updating models once a week or on an as-needed basis) is also increasing — requiring strict model governance and software development lifecycle (SDLC) processes and tools.

- **Models show AI/ML improvements and can segment customers in real-time.** Risk scoring in a post-rules modeling world requires a plethora of risk scoring AI algorithms (supervised, semi-supervised and unsupervised), including Bayesian, K-means clustering, Logistic regression, Neural networks, XGBoost, etc. These algorithms all feast on large data quantities, both monetary/payment and contextual data.[7] Due to the explosion of cloud-offered AML solutions, vendors can now see much more data across their entire customer base, which leads to dramatic improvements in model performance. Alongside model improvements, AML solutions now can dynamically segment and resegment customer populations using AI algorithms — a great help for reducing overall customer friction.
- **Real-time and cryptocurrency payments mandate dynamic transaction risk scoring.** AML vendors are feverishly creating models that can: 1) cover new style, peer-to-peer payments such as Venmo, Xoom, and Zelle and 2) risk score transactions in real time. (Sometimes real-time responses hinge on the platform's ability to process them.) It's important to build entity link networks based on past transactions with implicit entity risk scores. It helps with real-time transaction risk scoring. These entity link features have been a longer-term, more ambitious customer requirement, and we finally see vendors responding to them.
- **Better AI model explainability.** Regulator-imposed model governance, reducing overall customer friction, and empowering AML investigators and analysts require that FIs are able to explain risk scoring and decisions that models make. This is relatively easy for rules-based systems, but with machine learning, and especially unsupervised machine learning clustering algorithms, explainability causes a lot of headaches. To help, FIs and AML vendors offer scaffolding models, which are predominantly rules-based, simplified models that loosely map the risk scores of unsupervised models. These scaffolding models provide reason codes for the decisions of unsupervised models.
- **AML ontologies and taxonomies are taking shape and becoming available.** Traditionally, every organization maintained its own (largely oral-history-based) AML and fraud taxonomies consisting of the various known methods used by known money launderers and fraudsters. This approach is obviously incomplete and limits the FI to only being aware of schemes it previously encountered — making detection of new unknown-to-the-bank schemes very difficult. Vendors are taking heed and are planning to provide productized and regularly managed databases and/or cloud repositories of new money laundering and fraud taxonomies and patterns.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Case Management And Operations Converge For AML And EFM

Case management is the process of repeatably dealing with high-risk transactions, investigation, follow-up, regulatory filing, dashboarding, and reporting. Forrester's clients report that providing human analysts and investigators with an easy-to-use and intuitive case management system can improve case management efficiencies by 15% to 20%. To support improved case management, we see client requirements and vendors' roadmap plans including the following:

- **A single case management system for AML and fraud management.** Converging fraud and AML (FRAML for short) is a common trend today. FIs see high cross-correlation between the two areas; usually fraud precedes money-laundering activities and is very often committed by the same individuals. FRAML allows for a single-pane-of-glass view across all cases (obviously making sure that fraud analysts can't tip off customers about ongoing AML investigations). We see vendors improving SAR reporting by adding enhanced and automated evidence-gathering methods and enabling cross-jurisdictional SAR filing.
- **Prioritizing alerts automatically and focusing on the top 5%.** With AML investigation, FIs have to focus on the highest-risk and highest-impact transactions. We see firms increasingly requiring automatic, ongoing, and AI-based prioritization of alerts and cases in their case management platforms to help with automatic alert prioritization (i.e., focusing on the top 5% alerts). This also helps improve investigator efficiencies: A North American bank reported a 17% reduction in average case handling times after implementing automatic alert prioritization in its queues. An automated alert suppression engine for marking all similar but false positive alerts can also dramatically improve detection rates and investigator efficiency.
- **Homomorphic encryption in investigation used between banks.** FIs can achieve increased accuracy and speed of AML investigation by sharing entity and transaction dates among them. The biggest roadblock here has traditionally been privacy and the Bank Secrecy Act regulations prohibiting direct customer PII data sharing with any external organizations. As a result, FIs are now interested in homomorphic encryption of data used in the investigation process. Allowing investigators to perform search, sort, and filter operations on the bank's own and other banks' encrypted entity and transactional information helps with faster identification of money-laundering activities. We are starting to see Duality and Enveil provide functionality for homomorphic encryption to support this use case.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Recommendations

Integrate Once, Communicate Often

Failing to improve your firm's AML regime can expose it to regulatory fines, sanctions, and even higher levels of fraud. In today's complex and online-first environment, where faceless registration and application is the norm, it's important that you:

- **Do data integration and data sharing once.** Disparate, siloed line-of-business AML solutions require more data integration and investigative labor; they're also inaccurate. S&R and AML pros should coordinate and unify efforts to build on existing and create new unified data ingestion methods for as few AML suites as possible. At a minimum, create an internal sharing database with tight access (read/write) controls to disseminate hotlists about known money launderers' identities.
- **Ease investigators' pain with robotic process automation (RPA).** While not always a systemic solution, RPA solutions such as Blueprism and WorkFusion offer significant cost savings since they automate menial, repetitive tasks predominantly in case management. RPA solutions can also speed up the data integration process and provide data connectivity to hitherto hard-to-get-to data sources (e.g., mainframe and iSeries).
- **Supply as much alert and case context to investigators on one screen as possible.** Solutions are getting much better at being able to customize case management screens to include map information, link analysis, predictively recommended other cases to look at or to investigate. Having a single-pane-of-glass view of transactions and entities reduces the likelihood of investigators missing important case details.
- **Converge fraud management and AML operations.** A North American regional bank told us that it embarked on the journey of tearing down legacy EFM and AML silos by simply colocating investigators and providing them with a common instant messaging platform. This bank told us the communication between EFM and AML investigators greatly improves efficiency as fraud very often accompanies money-laundering activity. Using a unified case management system and sharing modeling techniques also improves AML operations' efficiency and accuracy.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

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 iOS and Android.
Stay ahead of your competition no matter where you are.

Supplemental Material

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

ACI
BAE
BehavioSec
CipherTrace
Elliptic.io
Featurespace
Feedzai
FICO
IdentityMind
NICE

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Endnotes

[1] Source: Chris Jewers, "Immediate action required to meet new AML legislation," Accountancy Age, January 3, 2020 (https://www.accountancyage.com/2020/01/03/immediate-action-required-to-meet-new-aml-legislation/).

[2] Source: "CM Network Data Charts," Coin Metrics (https://coinmetrics.io/charts/#assets=btc).

[3] See the Forrester report "Now Tech: Identity Resolution, Q3 2018."

[4] See the Forrester report "Top Trends Shaping Identity Verification (IDV) In 2018."

[5] It is also important to recognize that privacy regulations (GDPR, CCPA, etc.) may explicitly prohibit using device IDs and IP addresses for any other purpose than fraud management and AML. See the Forrester report "The Forrester Wave™: Risk-Based Authentication, Q2 2020".

[6] Source: Andrew Li, "The Importance of AML Model Governance and Validation," ACAMS (http://files.acams.org/pdfs/2016/The_Importance_of_AML_Model_Governance_A_Li.pdf) and "Anti-money laundering," ECB Banking Supervision (https://www.bankingsupervision.europa.eu/banking/tasks/anti-moneylaundering/html/index.en.html).

[7] Source: "How Do I Get Started?" Machine Learning Mastery (https://machinelearningmastery.com/start-here/) and Jason Brownlee, "A Gentle Introduction to XGBoost for Applied Machine Learning," Machine Learning Mastery, April 22, 2020 (https://machinelearningmastery.com/gentle-introduction-xgboost-applied-machine-learning/).

See the Forrester report "Stop Billions In Fraud Losses With Machine Learning."

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

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

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

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.