2017 THOMSON REUTERS US ANTI-MONEY LAUNDERING INSIGHTS REPORT

ACAMS® | Advancing Financial Crime Professionals Worldwide®

THOMSON REUTERS®

CONTENTS

EXECUTIVE SUMMARY

The U.S. anti-money laundering (AML) regime has undergone radical change driven by shifting economic sanctions' targets, new ultimate beneficial owner (UBO) data-reporting demands and cyber-enabled crime. Thomson Reuters conducted a survey of 438 AML compliance leaders connected with the Association of Certified Anti-Money Laundering Specialists (ACAMS) to understand how U.S. financial institutions (FIs) are responding to regulatory disruption in an evolving-threat landscape.

Over the last year, FIs have had to perform sweeping overhauls of their customer screening, monitoring and reporting processes courtesy of the U.S. Treasury's Office of Foreign Asset Control (OFAC). Changing OFAC priorities have significantly impacted operations for 53 percent of survey respondents who regularly engage in sanctions screening. Specifically, the Obama administration's easing of sanctions against Iran, Cuba, Burma and Sudan, coupled with its levying of new penalties against certain Russian entities for their alleged role in 2016 election meddling, have complicated geopolitical agendas, sending FIs scrambling to adjust.

Additionally, the Trump administration's recent directives against the Venezuelan government and third-party countries that support North Korea add more challenges to the OFAC obstacle course. President Trump also has signaled a desire to relax the enforcement of Foreign Corrupt Practices Act (FCPA) laws, sowing further regulatory confusion.

$800 billion to $2 trillion laundered every year

Beyond shifting FCPA and sanctions guidance, the 2016 Customer Due Diligence (CDD) and UBO final rules enacted by the Financial Crimes Enforcement Network (FinCEN) present more challenges for FIs. Now covered FIs, including depository institutions, broker-dealers, mutual funds and futures commission merchants, have until May 11, 2018 to comply with a more onerous regulatory framework for verifying customers and the UBOs of legal entity accounts.

Most significantly, FIs need to incorporate UBO data collection into their standard CDD processes to identify any stakeholder who owns 25 percent or more of a legal entity, and develop consistent risk-based procedures for collecting beneficial ownership information.

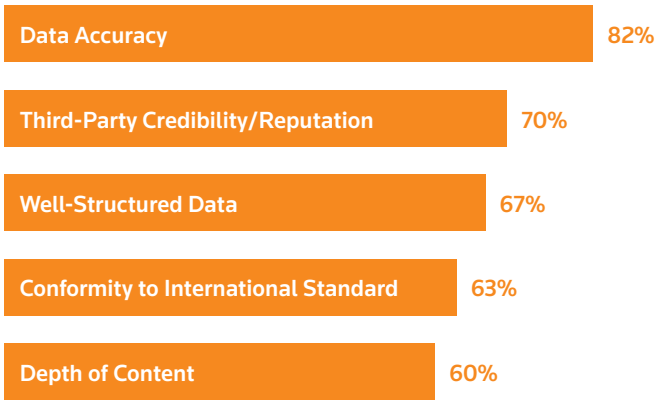
According to the survey, 89 percent of organizations currently verify UBO information directly from the customer. But 58 percent of survey participants cite the inability to validate UBO data as their greatest operating challenge. In fact, only three in five survey respondents stated they are confident their organizations will be able to comply with FinCEN's new rules by the 2018 deadline.

Illustrating the post-final rules enforcement zeitgeist is the $17-million fine issued by the Financial Industry Regulatory Authority – the largest money laundering penalty ever issued by the agency – against a major broker dealer in May 2016. More staggering is the $184 million civil penalty assessed by FinCEN in January against one of the world's most prominent money service businesses (MSBs). FinCEN penalized the delinquent MSB because it failed "to implement and maintain an effective risk-based AML program" and delayed the filing of suspicious activity reports (SARs).

While filing timely and accurate SARs is important, this enforcement action underscores a much larger systemic dysfunction in SAR reporting; risk analysts are overwhelmingly blind to the accuracy of generated alerts. **Seventy-one percent and 78 percent of survey respondents said they did not know how many of their SARs were false positives and false negatives, respectively.** This blind spot may be correlated to potentially outdated screening parameters programmed into transaction monitoring systems. Curiously, the survey revealed that multiple deposits into an account, which can indicate transaction structuring, are the second most frequent trigger for alerts, as indicated by 53 percent of respondents.

It should come as no surprise that 86 percent of survey respondents said that transaction details were always included in SARs, but only 45 percent provide additional identifiers not included in required fields. Perhaps the inclusion of alternative identifiers like customer IP addresses, email addresses and phone numbers, as noted by FinCEN's October 2016 cyber-risk advisory, could help improve SAR reporting accuracy and mitigate the risk of enforcement action. **Regardless, a broken SAR paradigm may be the reason 33 percent of survey participants are considering new processes to reduce AML risk. Chief among these processes is the adoption of automated regulatory technology (regtech) to verify customer identities and better qualify transaction risks.**

According to the survey, 64 percent of survey respondents continuously monitor their customers with automated AML and CDD systems. However, only 39 percent use an automated system to manage screening, workflow and records management. Additionally, the split between organizations that use a third-party regtech vendor to collect AML/CDD information versus those that manage customer screening internally is fairly even at 51 percent and 49 percent, respectively. For FIs that use a third-party to aggregate AML/CDD, the following five factors were listed as most important by at least six in ten respondents:

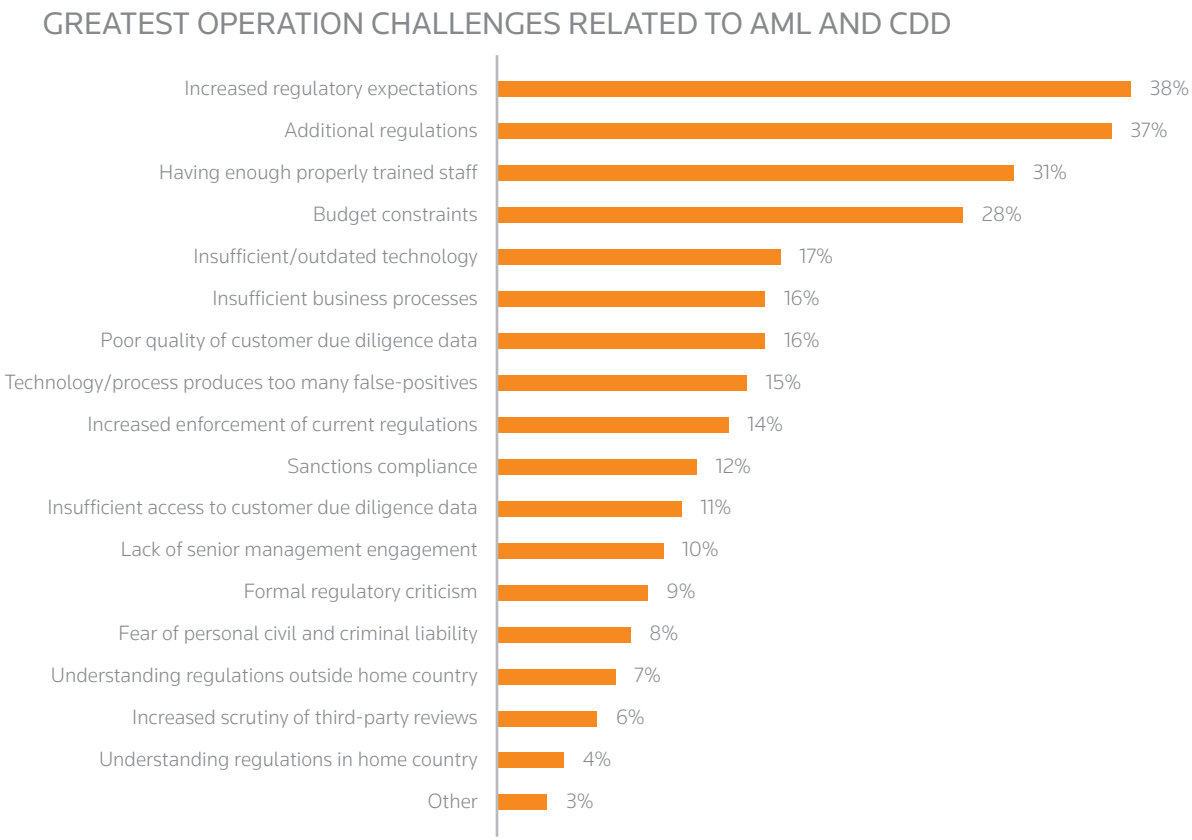


The 2017 Thomson Reuters U.S. Anti-Money Laundering Insights Report analyzes the survey findings, providing a data-driven framework for AML professionals to make better operational and budgetary decisions. The latter is key as 72 percent of survey participants did not know their organizations' dedicated budget for AML/CDD screening. However, the broader goal is to help U.S. institutions stem the estimated $800 billion to $2 trillion laundered every year by the global financial industry, often making it an unwitting financier for terrorist networks, drug cartels and other criminal groups that threaten national security.

CHALLENGES AND TRENDS

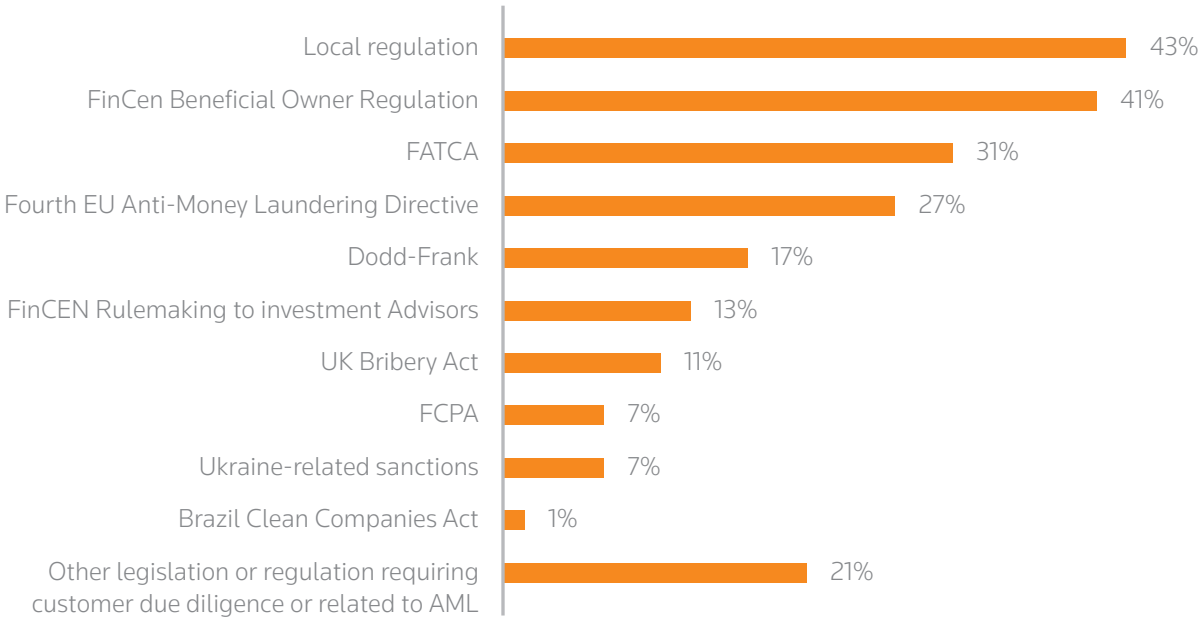
Respondents said the greatest operational challenges stemmed from increased regulations, a lack of properly trained staff and budget constraints. Surprisingly, local regulation was most frequently cited as being the biggest driver of heightened compliance workload. This trend may correspond to participating financial institutions (FIs) having significant operating hubs in New York, where the state's financial regulator enacted its Final Anti-Terrorism Transaction Monitoring and Filtering Program Regulation on Jan. 1, 2017.

The top four operational challenges for survey respondents were: increased regulatory expectations (38%); additional regulations (37%); having enough properly trained staff (31%) and budget constraints (28%).



By decree of New York's Department of Financial Services (DFS), regulated institutions and regulated non-bank institutions now have to implement and maintain a risk-based transaction monitoring and filtering program. This initiative includes continuous documentation that specifies the parameters of transaction monitoring, any modifications to these rules and the results of stress tests that audit the effectiveness of risk screening controls.

REGULATIONS CONTRIBUTING TO WORKLOAD



The five regulations most frequently cited for compounding workload include: local regulation (43 percent); FinCEN beneficial owner regulation (41%); FATCA (31%); Fourth EU AML Directive (27%); and other legislation (21%).

Additionally, Part 504, as the DFS rule is more commonly known, requires regulated entities to incorporate filtering systems that intercept transactions prohibited by federal trade sanctions. This local regulatory apparatus further reduces FIs' margin for error, as they attempt to adapt to a transitioning and increasingly complex OFAC regime.

The last onus of the Part 504 ruling is the obligatory annual board resolution or senior officer compliance finding, which must be submitted to the DFS superintendent by April 15 of each year. Now, every regulated entity has to keep all "records, schedules and data supporting adoption of the board resolution or senior officer compliance finding for a period of five years." [1]

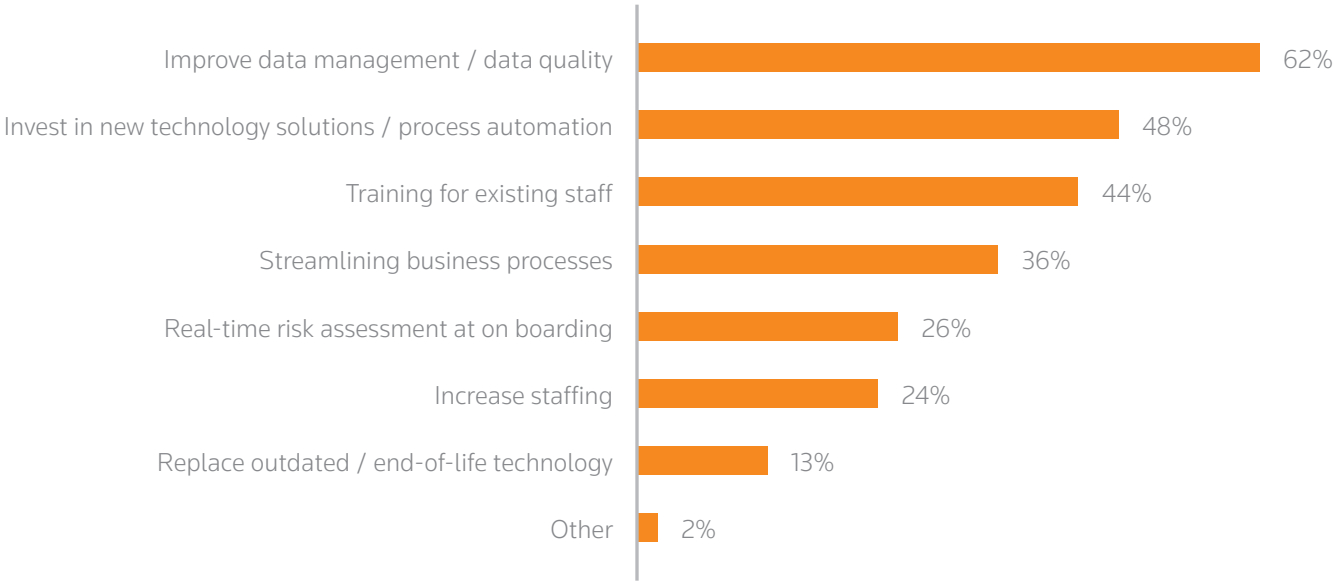
Predictably, the second regulation most frequently cited as contributing to additional workload was FinCEN's UBO reforms. But FIs need only to collect the UBO data, and this activity can be rolled into normal CDD processes. With most survey respondents (37%) already collecting UBO data between the 1 percent to 24 percent threshold, the new requirement should actually allow them to relax their legal entity screening controls.

But given the growing enforcement power of local regulatory regimes, and their heightened scrutiny over transaction monitoring systems, it should come as no surprise that most survey respondents cited data management/quality and investing in new technologies as their top priorities for AML and CDD in the next 12 months.

[1] http://www.dfs.ny.gov/about/press/pr1606301.htm

The top three AML and CDD priorities cited by participants were: improving data management and data quality (62%); investing in new technology and process automation (48%); and training existing staff (44%).

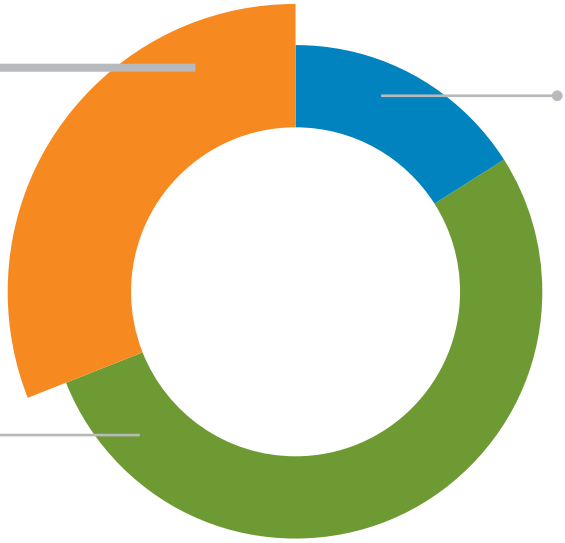
AML AND CDD PRIORITIES FOR THE NEXT 12 MONTHS



REGULATORY ENFORCEMENT ACTIONS

31%

Of respondents have experienced an AML/CDD enforcement action



16%

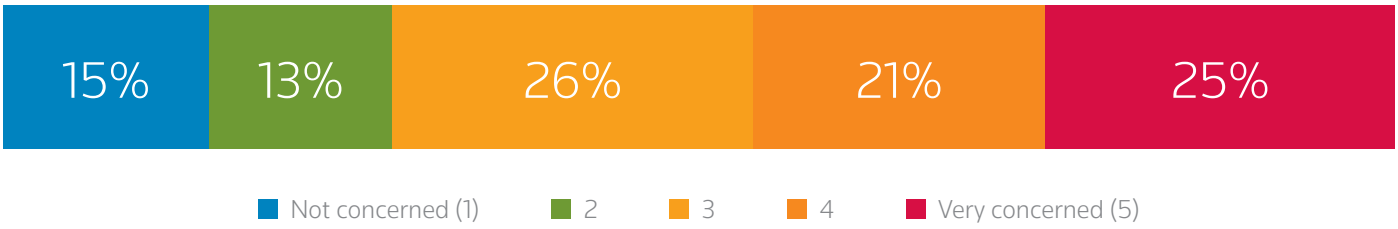
Don't know

53%

Have not experienced regulatory action

Forty-six percent of respondents noted they are concerned (21%) or very concerned (25%) about personal, civil or criminal liability, while 28 percent said that liability was not a concern.

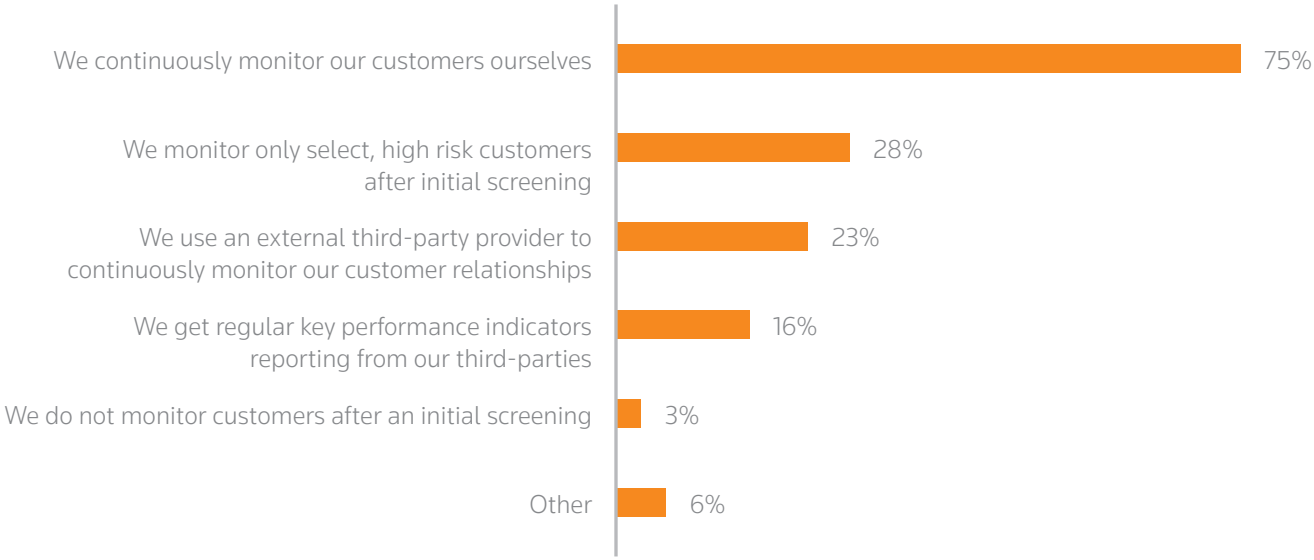
CONCERNS ABOUT PERSONAL CIVIL AND CRIMINAL LIABILITY



DUE DILIGENCE AND AML PROCESSES

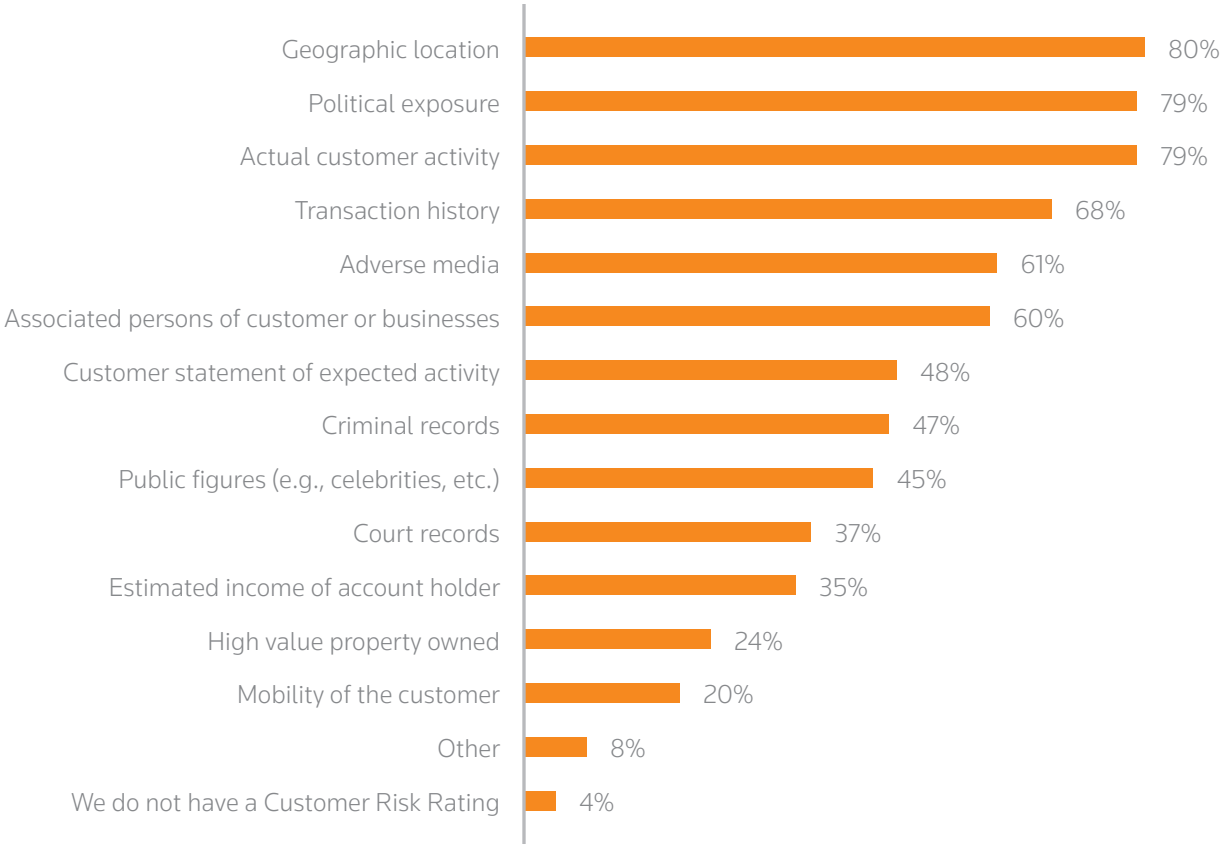
The survey revealed that the majority (64%) of institutions are following the best practice of continually monitoring and screening their customers. But about a quarter perform the initial screening at the start of client engagement. Of the respondents who continually screen their customers, 75 percent do so internally, while 23 percent use a third-party provider.

MONITORING CUSTOMERS POST-SCREENING



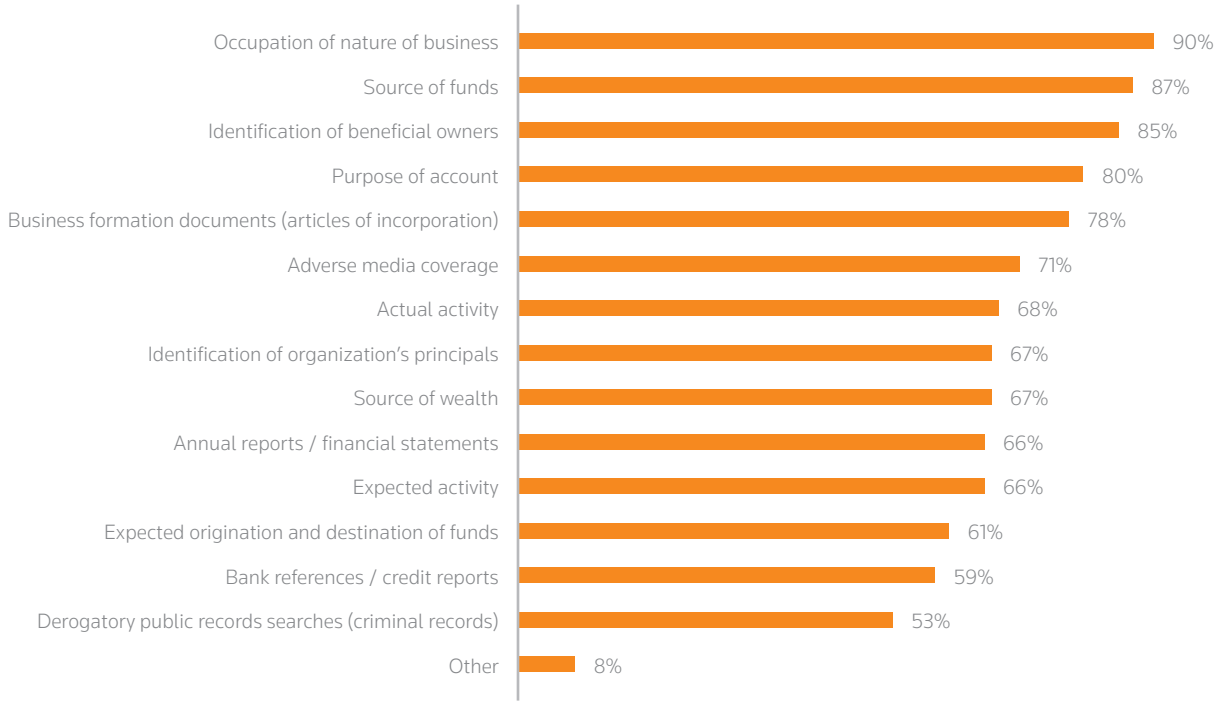
The top five data points factored into customer risk-ratings are: geographic location (80%); political exposure (79%); actual customer activity (79%); transaction history (68%); and adverse media (61%). Shifting regulatory attitudes toward FCPA enforcement may reduce the risk priority of politically exposed persons (PEPs) from certain jurisdictions in the years to come.

DEVELOPING CUSTOMER RISK RATINGS

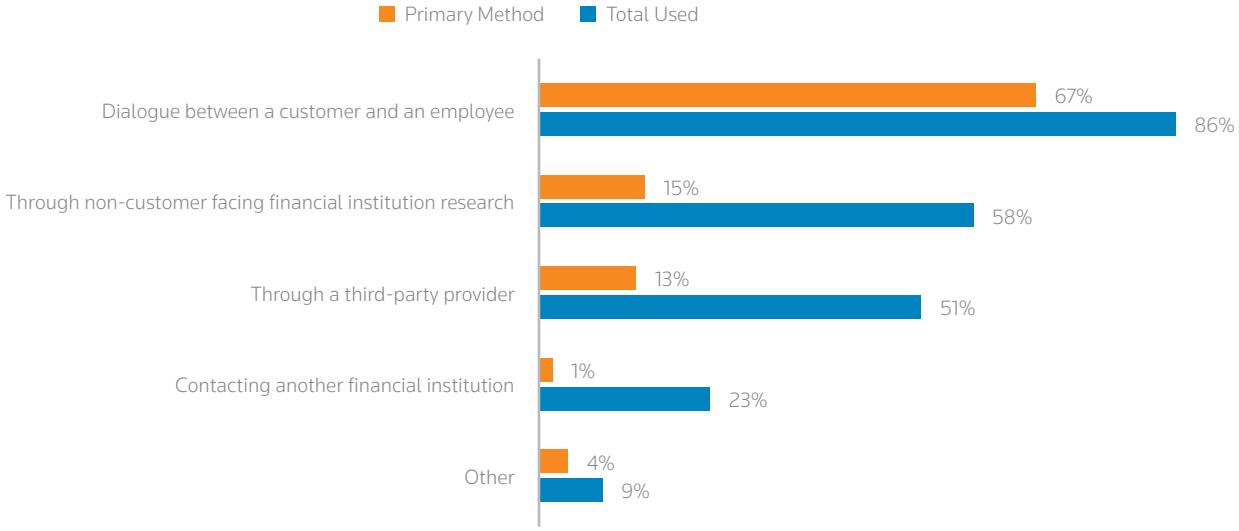


The most common CDD information collected includes: occupation or nature of business (90%); source of funds (87%); identification of beneficial owners (85%); and purpose of account (80%). But the majority of respondents (86%) said they rely on direct dialogue with the customer to gather AML/CDD information. But only 58 percent and 51 percent verified AML/CDD data through non-customer-facing financial institution, or by using a third-party service, respectively. If FIs are serious about curbing financial crime, these percentages need to increase. Self-reported customer profiles cannot be taken at face value, and must be cross-referenced with external AML databases.

TYPES OF INFORMATION COLLECTED FOR CDD

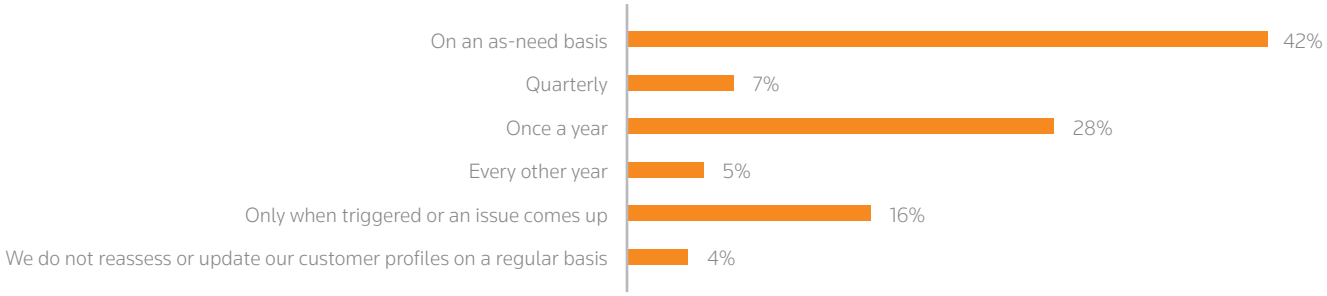


GATHERING AML/CDD INFORMATION



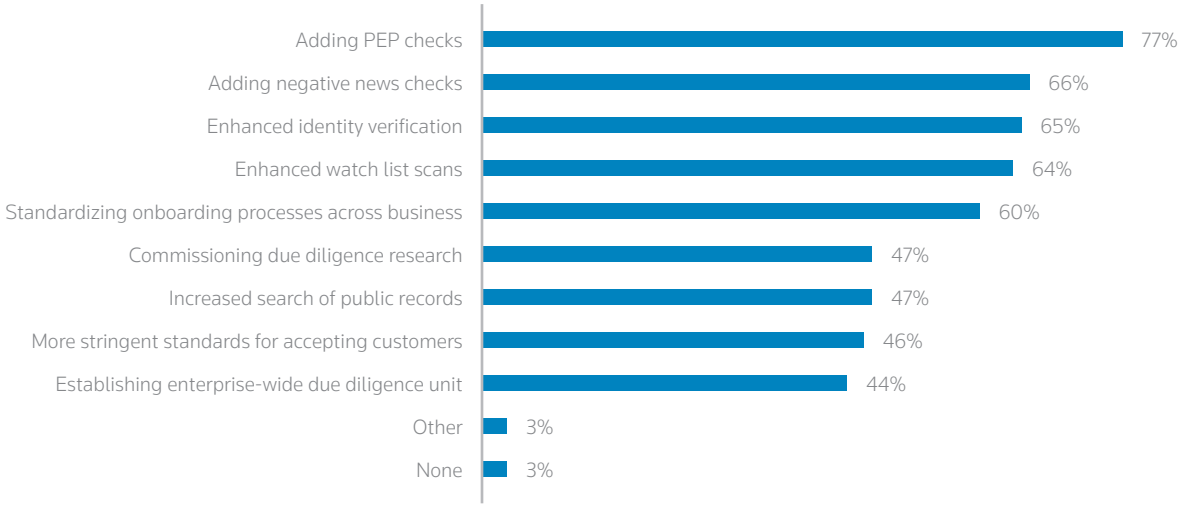
On the topic of customer reassessments, most participants said they re-evaluate clients on an as-needed basis (42%), while 28 percent conduct reassessments once a year and 16 percent do so only when triggered or an issue arises. Unusual activity (92%) and new know your customer (KYC) information (82%) were the most common triggers for customer reassessments.

FREQUENCY OF REASSESSING CUSTOMER PROFILES



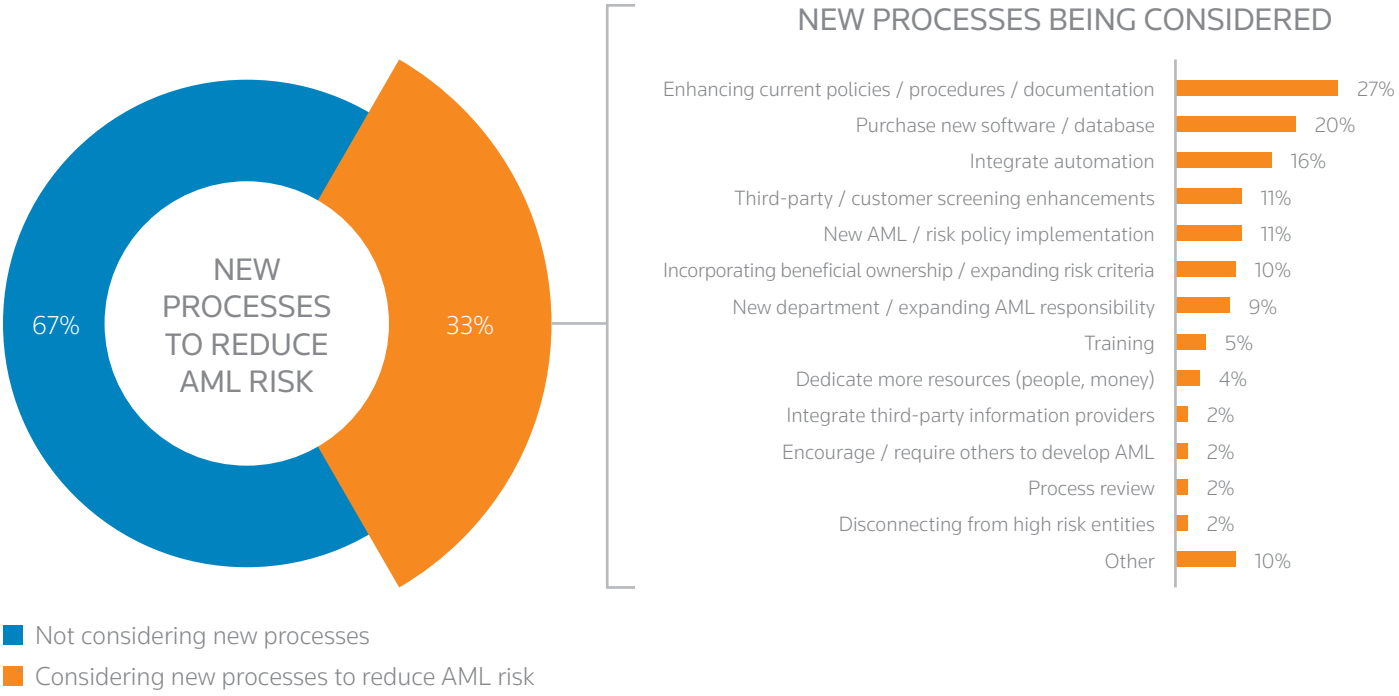
Meanwhile, to mitigate AML risk, respondents said the most widely adopted industry standards were: PEP checks (77%); adverse media checks (66%); enhanced identity verification (65%); enhanced watch list scans (64%); and standardized onboarding processes (60%). Again, shifting FCPA enforcement guidance may reduce the significance of certain PEPs in AML-risk screening. In the coming year, enhanced identity management, watch list scans and the standardization of onboarding processes are likely to become more vital to AML risk management.

STANDARD MEASURES TO REDUCE AML RISK



Surprisingly, only a third of participants said their organizations are considering new processes to mitigate AML risks. This is problematic because local regulatory regimes like New York's DFS and federal entities like FinCEN are raising the bar for transaction monitoring and data reporting. More stringent regulatory expectations demand a more sophisticated and technology-driven approach to managing AML risk.

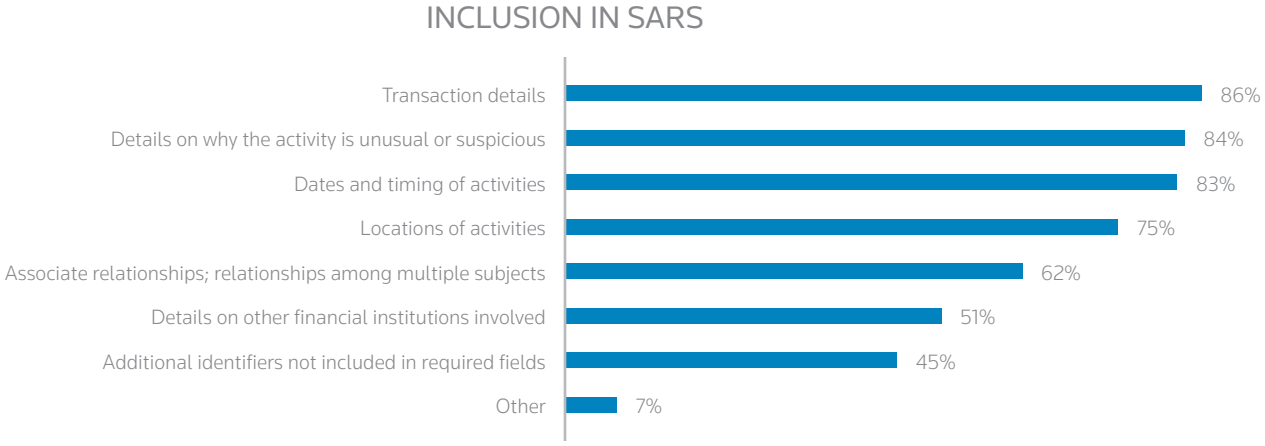
Despite the onerous demands of Part 504 regulations and FinCEN's October 2016 cyber-risk advisory, which requires FIs to capture alternative data like IP addresses, email addresses and telephone numbers in SARs, the majority of FIs do not seem to recognize that new processes are needed to confront emerging threats.



Nowhere are new processes more needed than in SAR generation, which represents a major blind spot for risk analysts. Not only were 68 percent of participants unaware of how many SARs they filed last year, but the overwhelming majority did not know many of these alerts were false positives (71%) and false negatives (78%), respectively.

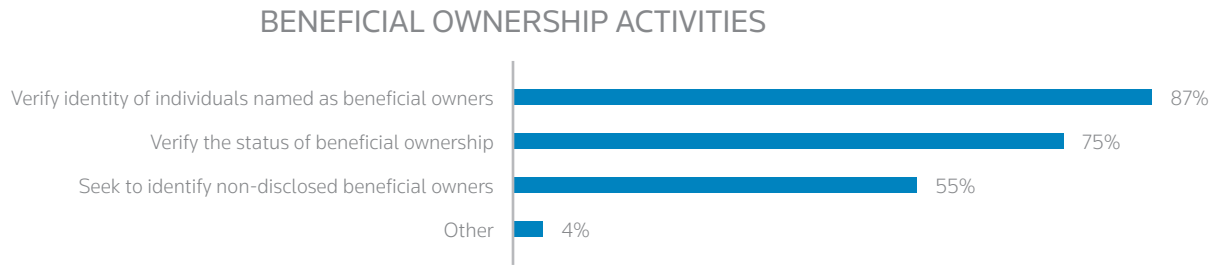
The four most common triggers for SARs were: suspicious transfer activity (57%); multiple deposits/structuring (53%); business activities that deviate from the norm (46%); and changes in transaction patterns (38%). Meanwhile, only 17 percent of respondents reported insufficient identity verification as a common SAR trigger. This disparity raises the question: Could better customer identity management and verification improve the accuracy of SAR reporting?

Additionally, organizations need to consider the standard fields that guide their SAR data collection and reporting. The survey revealed the top four SAR fields include: transaction details (86%); details on why the transaction was suspicious (84%); dates and time of activity (83%); and locations of activity (75%). Only 45 percent of respondents said they include additional identifiers not included in required fields. Going back to the DFS' and FinCEN's recent guidance, FIs need to start migrating to new data inputs that more intimately reflect their proprietary risk exposures.



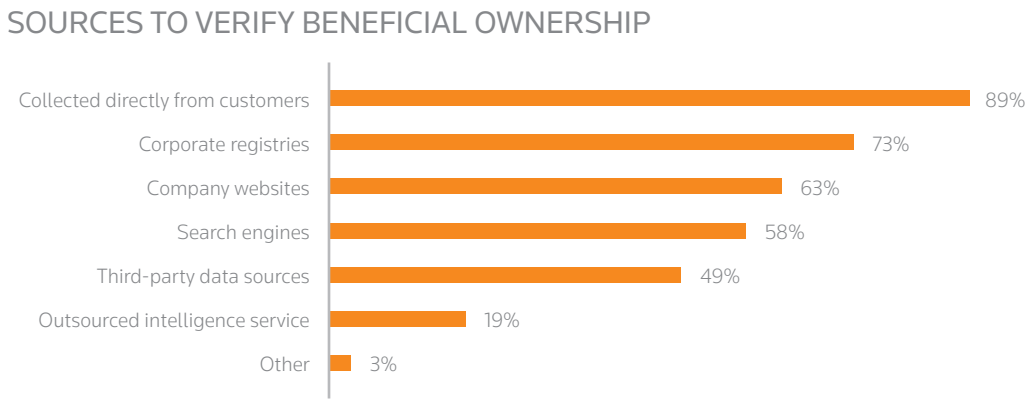
BENEFICIAL OWNERSHIP

With the May 11, 2018 deadline for the implementation of FinCEN's UBO rules fast approaching, it's no wonder beneficial ownership ranked second in terms of driving increased workload for compliance personnel. According to the survey, organizations most frequently engage in the following UBO activities:



To gather beneficial ownership data, 89 percent of respondents said they collect this information directly from customers. Other frequently cited sources for UBO data include: corporate registries (73%), company websites (63%), search engines (58%) and third-party data vendors (49%).

Given how essential the web has become to business positioning in the 21st century, company website information, search engine data and social media company pages will play an increasingly important role in the screening of legal entity accounts. Put more simply, digital identity needs to assume a higher priority for AML analysts as they review new business accounts. Business customers and other legal entities that lack a discoverable digital footprint pose a higher risk of being shell vehicles established for the sole purpose of sheltering and moving illicit funds.

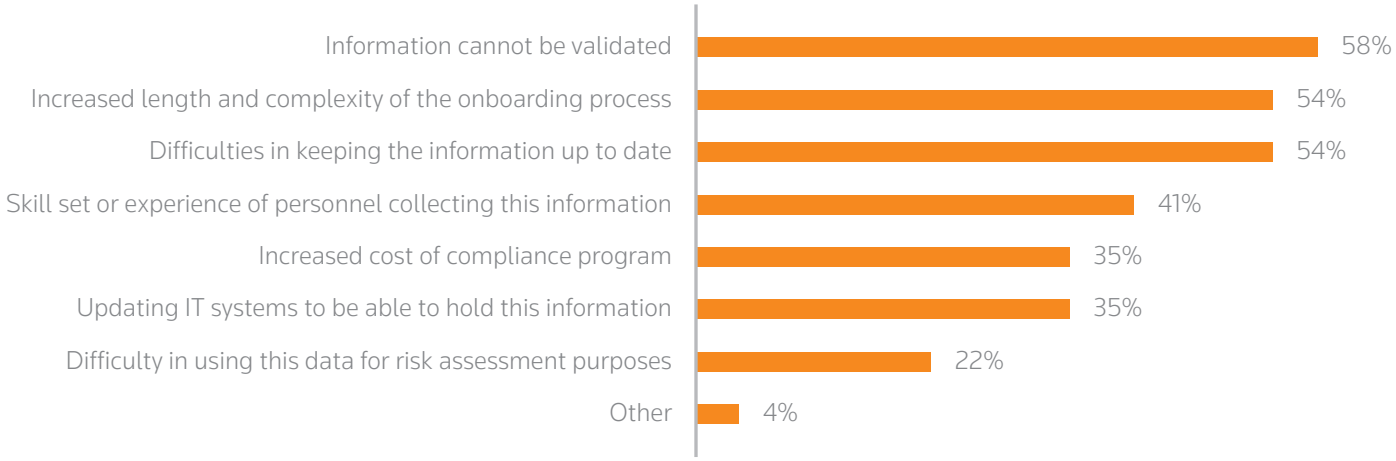


Not surprisingly, the greatest operational challenge related to beneficial ownership was the inability to validate UBO information, with 58 percent of respondents citing this as their chief obstacle. This is understandable because often times in sophisticated criminal conspiracies, money launderers will employ "dozens of nominees — people who appear to own or control businesses, but who are really proxies disguising the real owners," according to the Organized Crime and Corruption Reporting Project, an investigative journalism non-profit. [2]

For CDD analysts monitoring criminal shell companies, their task becomes even more complicated because the strawmen who pretend to be key stakeholders will frequently transfer company shares among themselves and conduct phony sales of corporate assets. This might explain why difficulties keeping information current (54%) was the second-most-cited UBO operating challenge by survey respondents.

Additionally, corporate directors of illegitimate enterprises, or those who would satisfy a control prong under UBO rules, will also frequently change, resigning and switching titles as if they were playing a game of musical chairs. Although verification remains a problem, the current UBO regime asks only that the data be collected, so this challenge is unlikely to create significant operational stress. Regardless, UBO risk screening should be fine-tuned to flag legal entities that frequently change ownership, that have virtually nonexistent activity preceding large transactions and that suffer from high managerial turnover. Risk analysts should be trained to identify these suspicious behaviors and assign risk accordingly.

GREATEST OPERATIONAL CHALLENGES RELATED TO BENEFICIAL OWNERSHIP

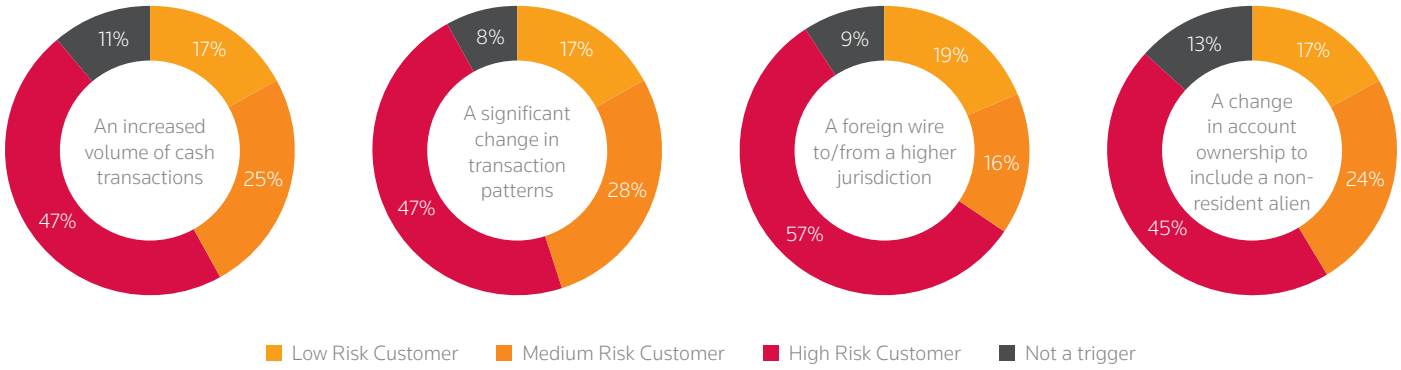


Further, nearly three-quarters of organizations said they either verify UBOs at the 25 percent to 49 percent threshold (37%), or the 1 percent-to-24-percent level (34%). This means that over one-third of survey respondents would be able to relax their UBO screening controls (and related budget), while still achieving full compliance with FinCEN regulations.

[2] https://www.occrp.org/en/investigations/6750-how-the-camorra-went-global

ENHANCED DUE DILIGENCE

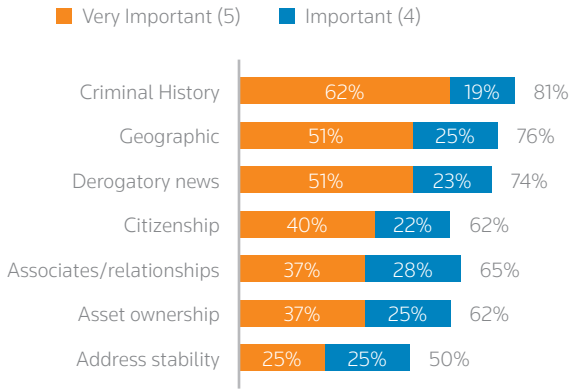
Overwhelmingly, respondents cited compliance (86%) as the division that oversees enhanced due diligence (EDD) processes. When evaluating four standard transaction-monitoring risk indicators, the survey revealed that high-risk customers accounted for nearly 50 percent of EDD screens on average. This makes sense, but organizations need to consider that risk is a dynamic entity, with criminals continually seeking ways to game the system and fly under the radar. For example, transaction laundering [3] has corrupted e-commerce, creating a quandary where business sectors previously classified as "low risk" are frequently being exploited by criminals, making yesterday's screening rules obsolete.



Survey participants also said KYC information was the most frequent trigger for EDD screens, with 66 percent saying it always triggered enhanced investigation. Another 29 percent said new KYC information sometimes led to further examination. Additionally, respondents cited criminal history (81%), geographic location (76%) and adverse media coverage (74%) as the most important EDD-screening data.

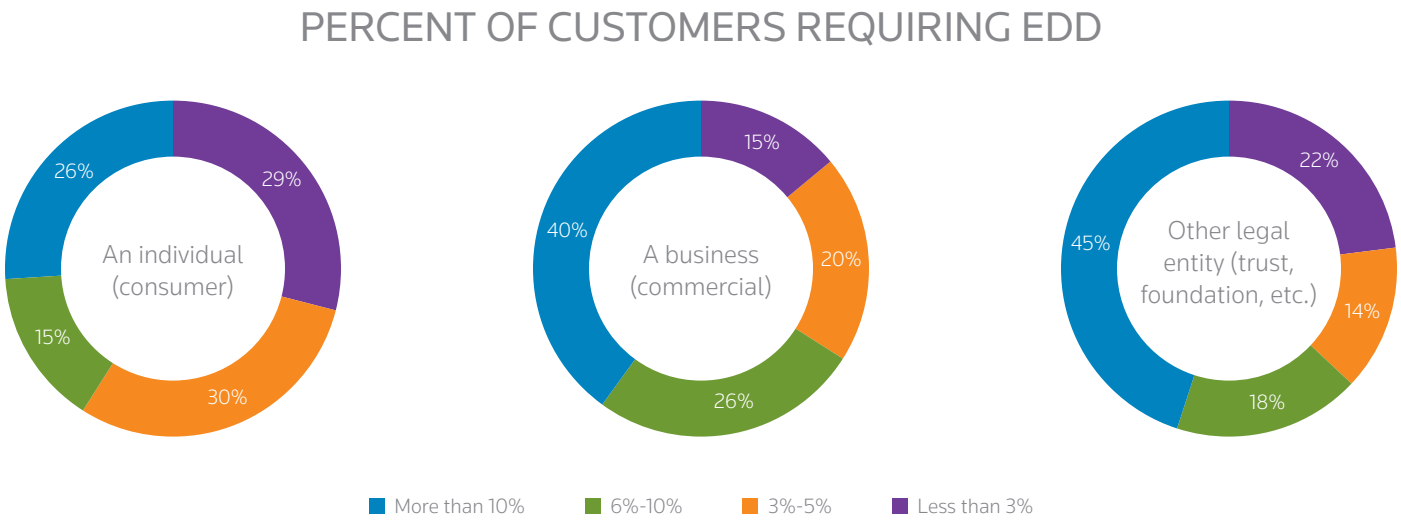
With regard to business customers and other legal entities, four in 10 respondents said more than 10 percent of these accounts required EDD screening. As stated in the previous section, frequent changes to corporate ownership and/or company management should assume a more significant role in legal entity EDD screening.

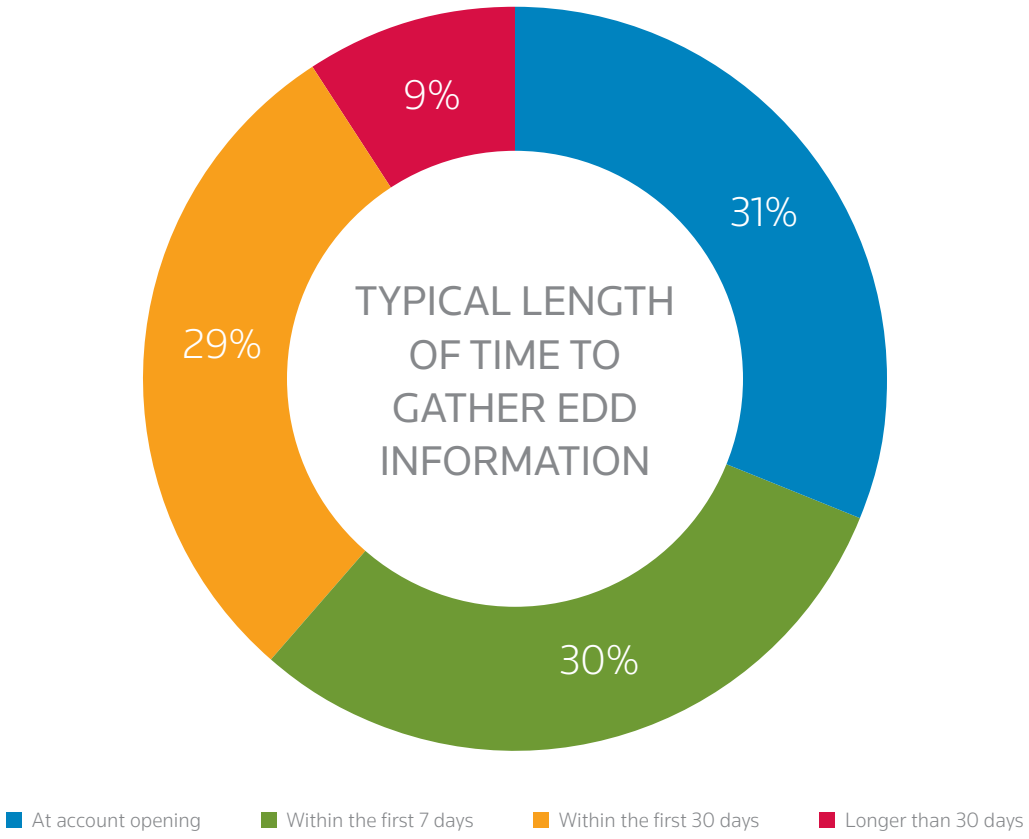
IMPORTANCE OF INFORMATION WHEN CONDUCTING EDD



[3] https://ftalphaville.ft.com/2017/03/17/2186157/why-transaction-laundering-is-turning-into-a-huge-financial-blindspot/

Diving deeper into the efficiency of EDD data collection, more than 60 percent of organizations said they collect EDD information at account opening (31%) or within the first seven days of account opening (30%). Another 29 percent of respondents said they collect EDD information within the first 30 days. For legal entity customers, it would make sense to track previous owners over a predetermined period of time and subject past stakeholders to similar EDD screening processes.

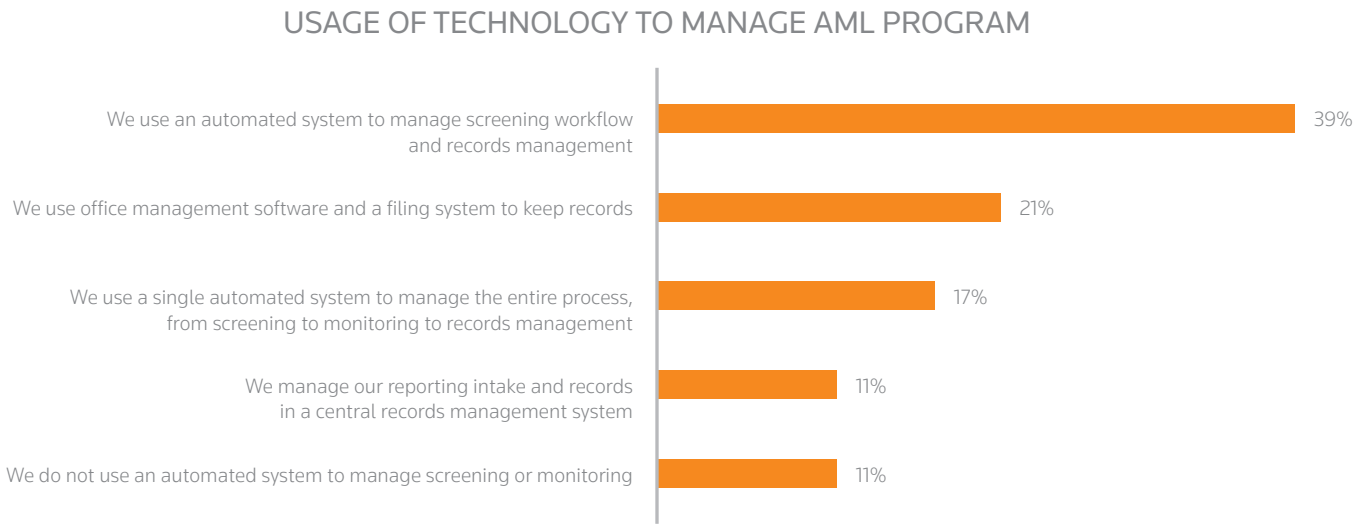




DATA SOLUTIONS AND DECISIONS

Fueled by innovation and intensifying regulatory demands, regtech has become the nucleus of financial services AML in the 21st century. [4] While legacy technologies are still searching for the proverbial million-dollar wire transfer from Miami to Bogota, the threat has evolved. Now adversaries like the Islamic State are exploiting online loan fraud [5] and e-commerce platforms to finance terrorism. [6]

Fortunately, modern-day regtech solutions are powered by artificial intelligence (AI), leveraging machine learning and pattern recognition to spot new indicators of suspicious activity. Still, roughly 40 percent of survey respondents said they used an automated regtech system to manage screening, workflow and records management. Additionally, 11 percent said they do not use an automated system to manage screening and monitoring.



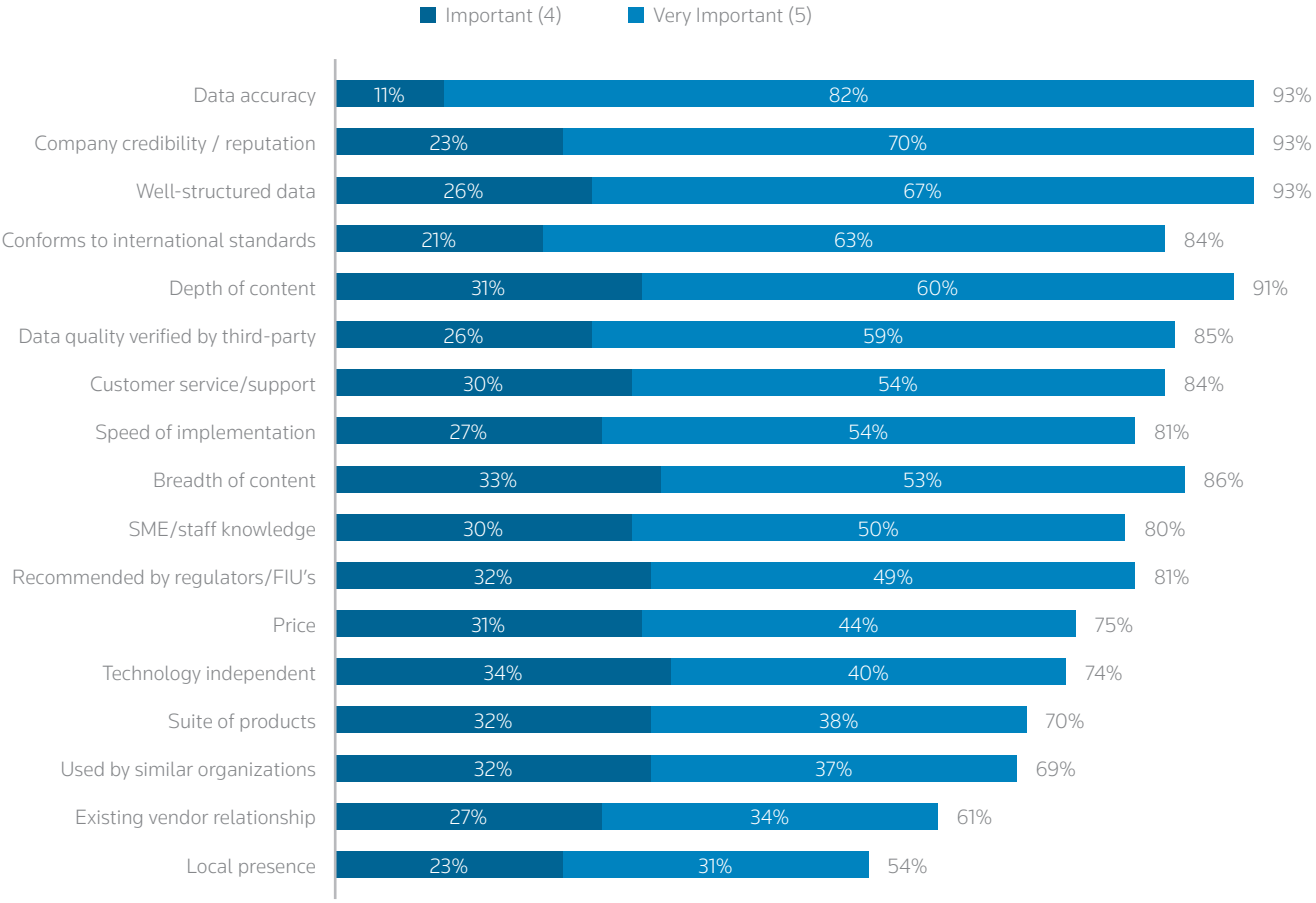
The use of third-party data vendors was split fairly evenly, with 51 percent of participants reporting the use of an outside provider and 49 percent saying they kept their processes in-house. When it comes to third-party vendor selection, respondents cited data accuracy (82%), vendor credibility/reputation (70%), well-structured data (67%), conformity to international standards (63%) and depth of content (60%) as "very important" when choosing a data provider.

[4] https://www.wired.com/story/quantaverse-ai-terrorist-funding/

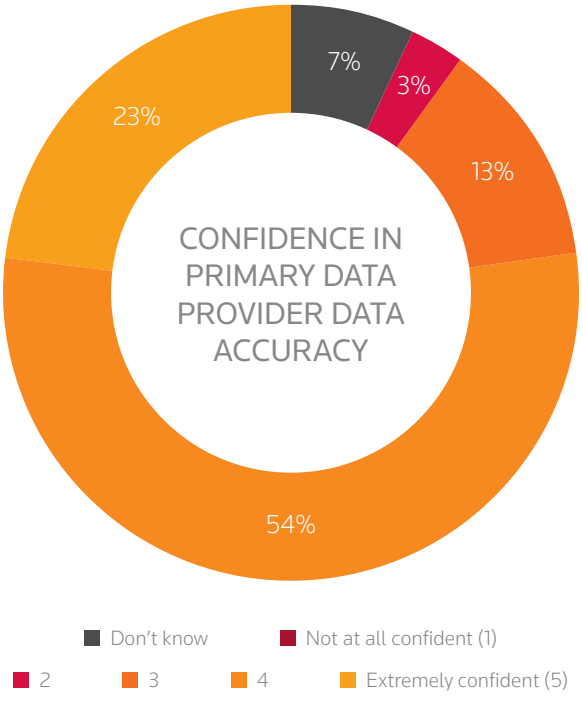
[5] http://fortune.com/2015/12/08/online-lender-says-it-gave-money-to-san-bernardino-shooter/

[6] https://www.wsj.com/articles/fbi-says-isis-used-ebay-to-send-terror-cash-to-u-s-1502410868

IMPORTANCE OF THIRD-PARTY DATA PROVIDER FACTORS



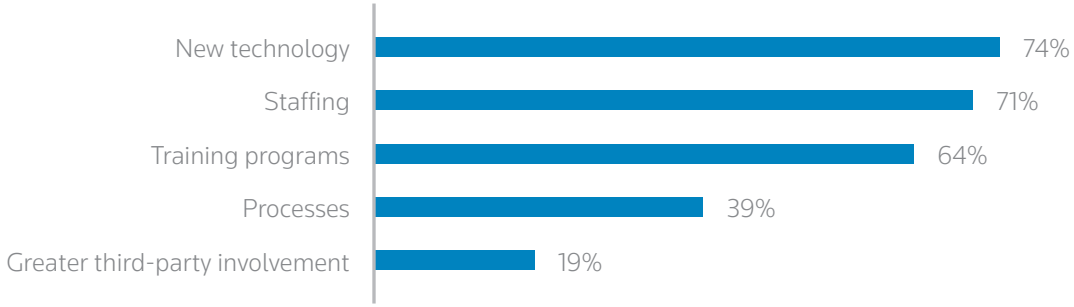
But only 23 percent of respondents said they were "extremely confident" in their primary data provider, while more than half (54%) said they were merely "confident" in their vendor. The biggest drivers for concern were gaps in geographic coverage, timeliness of data and data structure.



BUDGET AND STAFFING

According to a 2016 report by the Heritage Foundation, a conservative think tank, the U.S. AML regime costs an estimated $4.8 billion to $8 billion annually. [7] But remarkably, more than 70 percent of survey respondents said they did not know how much their organizations were spending on AML and CDD. Furthermore, 21 percent reported having no dedicated AML/CDD budget. On the bright side, this is an area ripe for resource optimization and improvement. The right third-party regtech provider can empower organizations with better analytics and budget transparency to illuminate this blind spot, driving revenue growth and improving balance sheet performance.

EXPECTED AREAS FOR BUDGET INCREASE



Analyzing year-over-year change in budget expectations, roughly two-thirds of respondents said their personal workload increased this year, but slightly less (63%) expect their obligations to increase in the next year. Additionally, 43 percent said that their compliance staff will grow and 40 percent said that their AML/CDD budget will rise in the next 12 months. Roughly 30 percent said they do not know how their budget will be impacted this year.

[7] http://www.heritage.org/markets-and-finance/report/financial-privacy-free-society

On the heels of more aggressive local regulations by the state of New York and FinCEN's sharpening focus on capturing cyber-enabled financial crime, it should come as no surprise that respondents cited new technology (74%) as the focal point of anticipated compliance spend. Beyond technology, staffing (71%) and employee training programs (64%) were cited as key areas for budget rebalancing. The connection between employee training and technology investment is obvious: Organizations will need to train their staff to operate the regtech assets of the future.

EXPECTED AND ANTICIPATED CHANGES

CONCLUSION

Despite the aggressive financial surveillance and AML regimes enacted in the wake of 9/11, less than 1 percent of global illicit financial flows are seized or frozen, according to the United Nations Office on Drugs and Crime. [8] And with the Tax Justice Network, an anti-tax evasion advocacy group, designating the U.S. as one of the top three financial secrecy jurisdictions in 2015, trailing only Switzerland and Hong Kong, [9] American financial institutions stand squarely in the eye of the AML storm.

While illicit financial flows cascade around the world through increasingly byzantine shell structures and digital payment channels, legacy transaction monitoring systems, programmed to flag the suspicious activity of the past, are ill equipped to spot present-day threats. Beyond the rise of transaction laundering, cryptocurrencies, which use encryption to enable transactional anonymity, present additional challenges to the financial services establishment. With more than $4 billion in bitcoin allegedly laundered by BTC-e [10] – just a single virtual currency exchange – how ready are banks to combat digital money laundering?

But more concerning, of the 4 million-plus suspicious activities cited in 2015 SAR submissions, only 2,188 were terrorism-related, according to FinCEN data. [11] This paltry ratio may be explained by the legacy AML risk priorities designated by the 2001 Patriot Act, which pre-date the peer-to-peer (P2P) payment platforms, virtual currencies and online lending vehicles spawned by the fintech revolution.

These same mobile Internet payment systems are frequently being exploited by terrorist groups such as ISIS, [12] which require nothing more than an Internet connection, an impressionable audience and a P2P payment app to fund and coordinate attacks.

Although Patriot Act AML reforms were implemented with the best intentions, the astronomically high SAR false-positive rates uncovered by this survey reveal that many law-abiding customers are being erroneously flagged. So two key issues emerge: properly identifying suspicious activity and delivering a better customer experience to the vast majority of accountholders, who are doing nothing illegal. To this end, better-quality data is needed, along with the next-generation technologies that automate processes and identify criminality with greater accuracy. Ultimately, the right regtech solution can help organizations control compliance costs, allocate resources more efficiently and deliver the operational transparency needed to drive growth.

[8] https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html

[9] http://www.financialsecrecyindex.com/

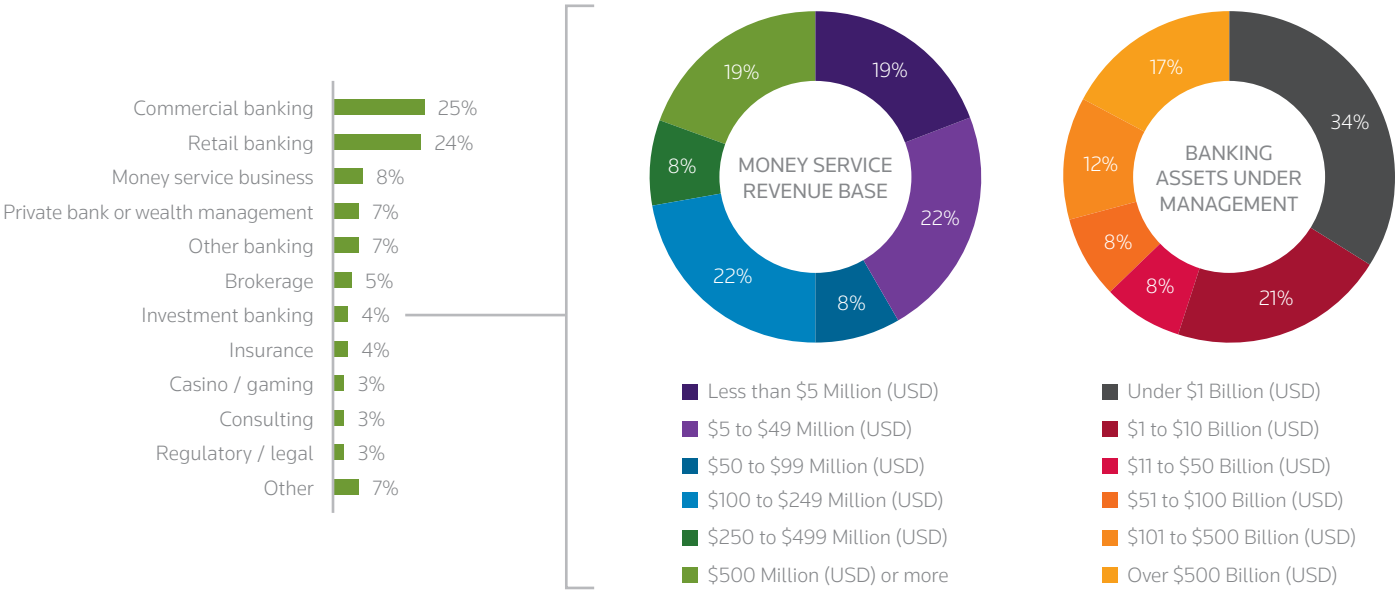
[10] https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged

[11] http://www.newsweek.com/do-money-laundering-laws-catch-criminals-509758

[12] http://www.acams.org/wp-content/uploads/2015/08/Combating-the-Proliferation-of-Mobile-and-Internet-Payment-Systems-as-ML-Vehicles-S-McCrossan.pdf

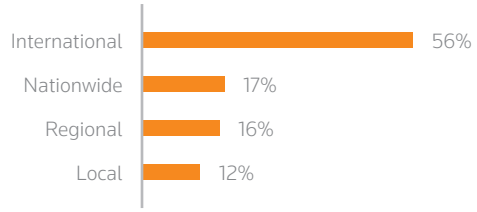
RESPONDENT PROFILE AND COMPANY DEMOGRAPHICS

Most survey respondents identified themselves as commercial (25%), retail (24%), MSB (8%) or private banking/wealth management (7%) entities. One-third of banking organizations reported less than $1 billion in assets under management (AUM), while 21 percent said they have between $1 billion and $10 billion AUM. Seventeen percent reported AUM in excess of $500 billion.



For MSB participants, organizational revenue most commonly ranged between $5 million to $49 million (22%), or between $100 million and $249 million. But 19 percent of MSBs reported revenues greater-than-or-equal-to $500 million. Similarly, another 19 percent said they have revenues below the $5 million threshold.

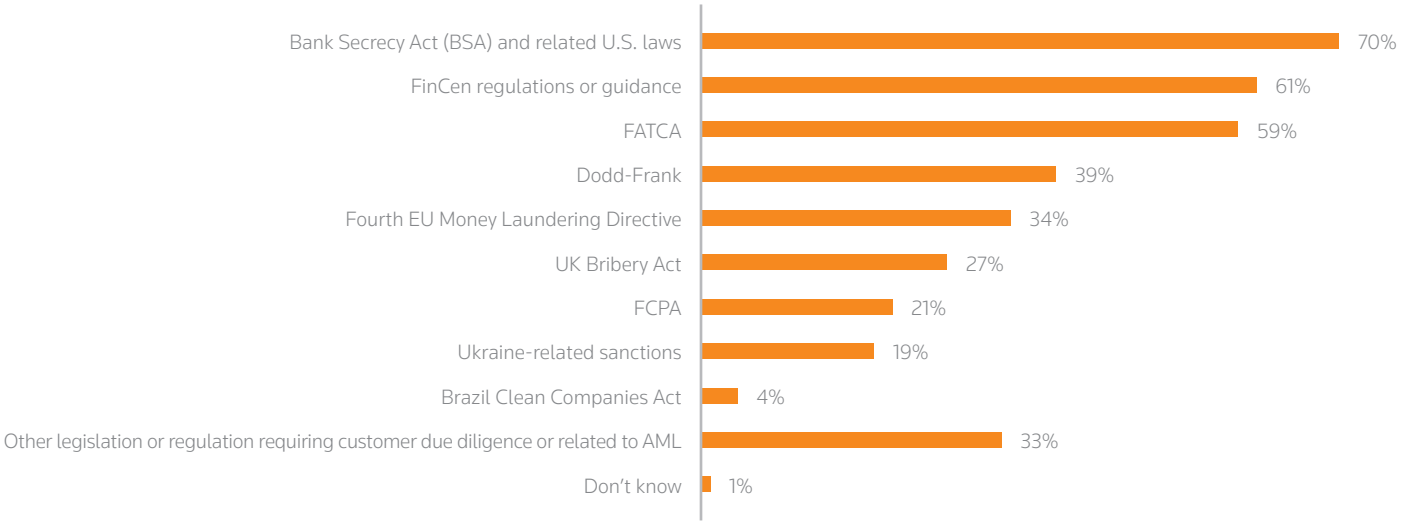
GEOGRAPHIC CUSTOMER BASE



Forty-one percent of participants are headquartered in the U.S., while 59 percent are based out of international locations.

The regulations that most impacted compliance and due diligence were the Bank Secrecy Act (70%), Financial Crimes Enforcement Network guidance and rules (61%) and the Foreign Account Tax Compliance Act (59%). Dodd-Frank, which could possibly be repealed, accounted for 39 percent of responses.

COMPLIANCE AND DUE DILIGENCE INFLUENCES



Forty-seven percent of respondents said their primary regulator is outside of the U.S. The other three most commonly cited regulators were FinCEN (34%), other (26%) and the Office of the Comptroller of the Currency (20%).

REGULATORY AGENCIES ADHERED TO