



2022 AML Trends Report



The ever-changing business landscape is forcing anti-money laundering (AML) compliance teams to continuously find ways to adapt while still managing increasing risks and costs. This is especially challenging when technology, products and payment rails are changing faster than regulations.

So how does a compliance team in 2022 keep up with these changes? The Alessa team at Tier1 Financial Solutions polled hundreds of respondents across the globe and interviewed several compliance leaders to get their perspective on the challenges they are facing, how they plan to invest compliance budgets and where they would like to see the industry go.

This report includes a summary of the survey results, as well as a carefully curated collection of insights from our compliance experts.

Our panel of compliance experts



Shane Bauer, First Vice President - Compliance, BSA and Security Officer, Bankers' Bank

Shane's responsibilities at Bankers' Bank include ensuring compliance to the Bank Secrecy Act, contributing to the Payments Strategy Group and a variety of other risk management functions. Bankers' Bank provides correspondent banking services to community banks throughout the upper Midwest, including asset liability management, bank cards, cash letters, commercial and international, investments, leasing, mortgages, and wealth management.

Shane is a graduate of the University of Wisconsin – Madison for both his bachelor's degree and his MBA. He also completed the Graduate School of Banking in Madison, is the recipient of the AIB Bank Operations Diploma, a graduate of the ABA School of Bank Card Management and holds corresponding certifications from the ICBA.



Carolyn A. DaCosta, Group Chief Compliance Officer & Corporate Secretary, JMMB Group Limited

Carolyn specializes in corporate governance, financial operations, law, regulatory and international compliance and is responsible for legal and regulatory matters for the JMMB Group of Companies. In keeping with the Group's commitment to effective corporate governance, she ensures compliance with all relevant statutory and regulatory requirements, monitors changes in relevant legislation and ensures appropriate action is taken when required.

She holds certification in Corporate Governance from Harvard Business School, an MBA in Finance, a Diploma in International Compliance from the Manchester Business School in the UK, a Bachelor of Laws degree from the University of London and a Bachelor of Arts degree from the University of the West Indies.



Neil Kumar, Vice President, Compliance, Alloya Corporate FCU

Neil specializes in the USA PATRIOT Act, Bank Secrecy Act (BSA), AML Act of 2020, KYC/CIP, business continuity management, risk management, financial crimes management, OFAC sanctions and quality assurance for the retail and wholesale financial services industry. In addition to overseeing the anti-financial crime activities at Alloya, he is a contributing member to the Faster Payments Council (FPC) Fraud Information Sharing Work Group.

His 17 years of BSA Officer experience is supported by his Anti-Money Laundering and Global Sanctions specialist certifications from the Association of Certified Anti-Money Laundering Specialists (ACAMS) and his membership to the Association of Certified Fraud Examiners (ACFE).

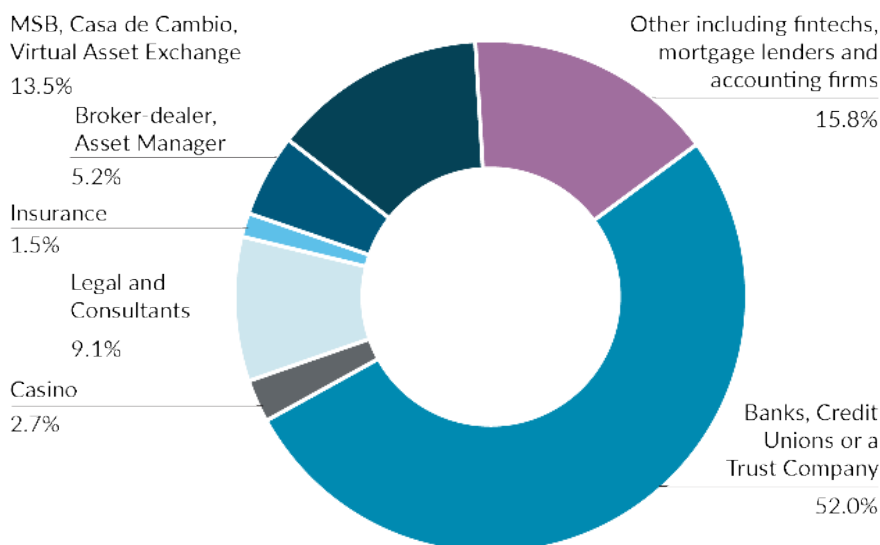


The Respondents

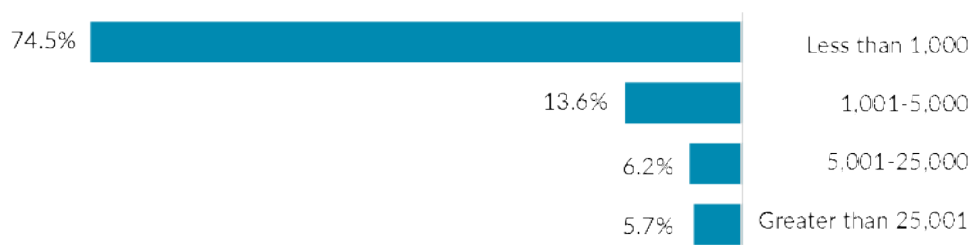
The respondents for our first annual AML Trends Report were mainly located in the United States., Canada and the Caribbean. The majority were part of compliance teams at banks and credit unions. We also saw participation from many MSBs, casa de cambios, virtual asset exchange providers and fintechs.

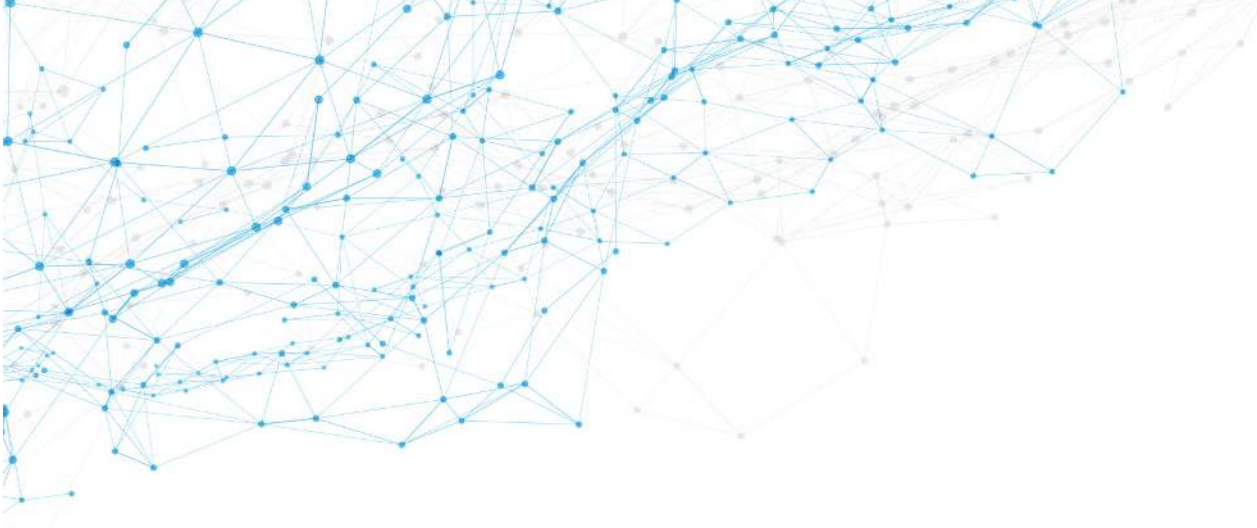
In terms of experience, we received responses from a variety of job functions within the compliance team, including C-suite and compliance officers, analysts and investigators. This provided both a view from the top, as well as a perspective from those responsible for the detailed execution of compliance. An overwhelming amount of our respondents came from compliance teams with less than 50 people and organizations with less than 1,000 employees.

For whom do the respondents work for?

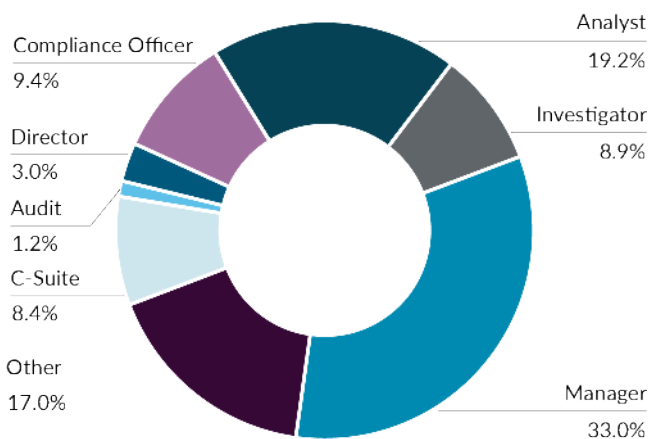


How many employees work at the companies of the respondents?

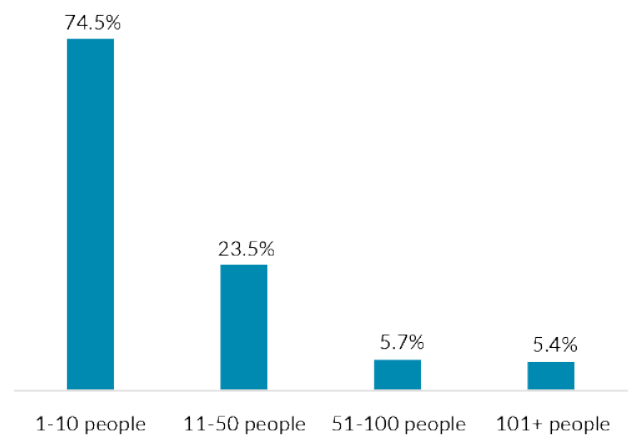




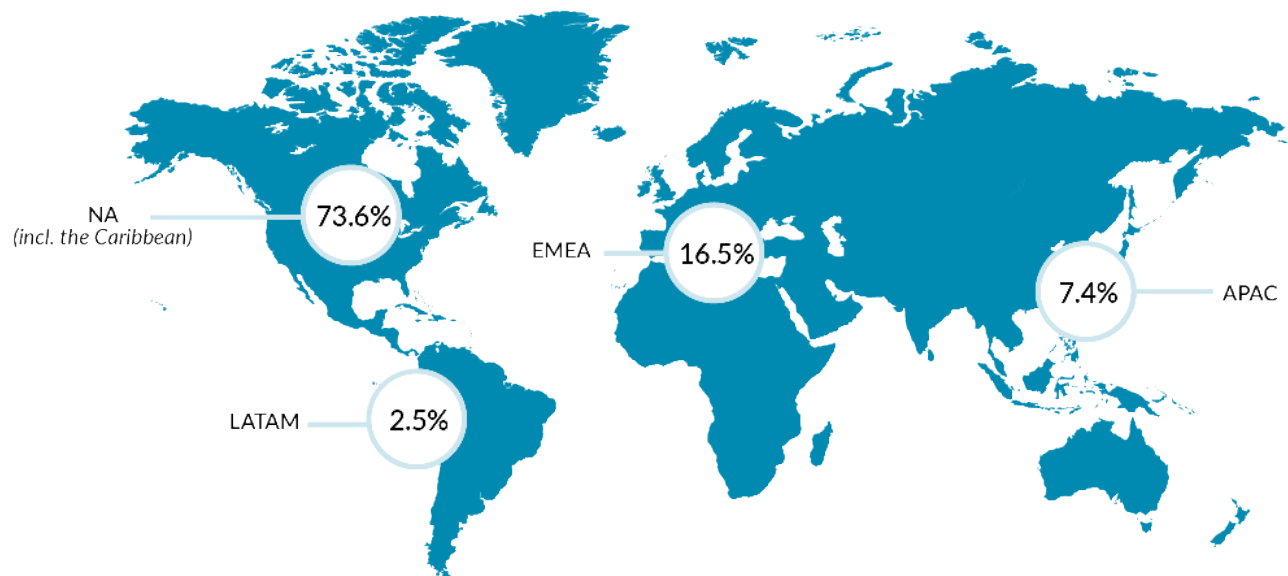
What positions are held by our respondents?



How many people are in the respondent's AML compliance team?



Where are the respondents located?



Money Laundering Risk

According to the FFIEC, “a well-developed BSA/AML risk assessment assists the bank in identifying ML/TF and other illicit financial activity risks and in developing appropriate internal controls (i.e., policies, procedures, and processes)”.

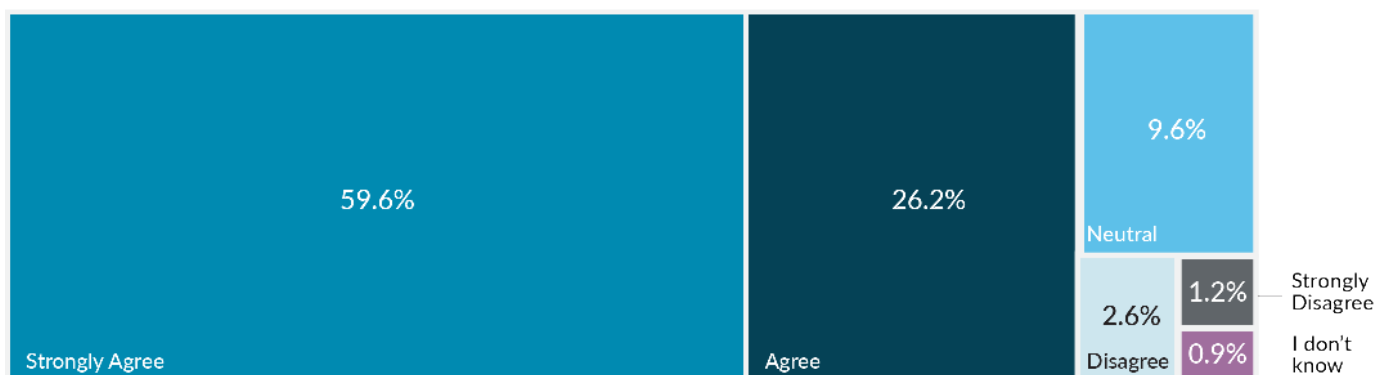
When a regulated entity understands its risk profile, it can better apply appropriate risk management processes to mitigate and manage risks to comply with regulatory requirements. It also allows entities to identify and mitigate any gaps in controls.

When looking at risk categories, regulated entities should consider their products, services, customers, and geographic locations. Risk assessments should be updated when there are changes to these areas to ensure an accurate reflection of the organization’s risks.

"Payment transparency is key to combatting illicit financial crime and regulations should be tailored to achieve greater payment transparency. More details surrounding payments provide additional opportunities to identify red flags associated with anti-financial crime efforts."

Neil Kumar, Vice President,
Compliance, Alloya Corporate FCU

Is money laundering considered a high-risk area within your organization’s business risk assessment?



When asked about whether money laundering is considered a high-risk area, nearly 86 percent of respondents strongly agreed or agreed with this statement.

"In the United States, AML rules are written such that they are rail-agnostic. They don't care how you find out who you're doing business with, they just want you to know that you do."

Shane Bauer, First Vice President - Compliance,
BSA and Security Officer, Bankers' Bank

"The increased adoption of virtual assets, crypto and digital currencies by clients is an emerging risk that needs to be better addressed by the financial industry. Regulators need to apply more focus on the KYC requirements for these as our regulations and supervisory authorities are still largely built around in person transacting and protections. We also feel that cyber and fraud risk continue to be growing risks in our industry."

Carolyn A DaCosta, Group Chief Compliance
Officer & Corporate Secretary,
JMMB Group Limited



Greatest AML Challenges Today

Heightened and evolving regulatory expectations was a challenge that was mentioned by nearly half of the respondents. The next biggest challenge was budget constraints.

With regards to know your customer (KYC) and customer due diligence (CDD), a little over one in four selected poor quality data on customer (27 percent). Respondents also struggled with getting a single view of customer data (20.6 percent) and sanctions compliance (17.4 percent).

When it comes to day-to-day processes, lack of automation, volume of manual processes (39 percent), amount of alerts (18 percent), quantity of false positives (27 percent), increases in transaction volume (29.4 percent) and detection of suspicious transactions (26.7 percent) were cited by the respondents. Finding trained staff was a challenge for nearly one in three respondents.

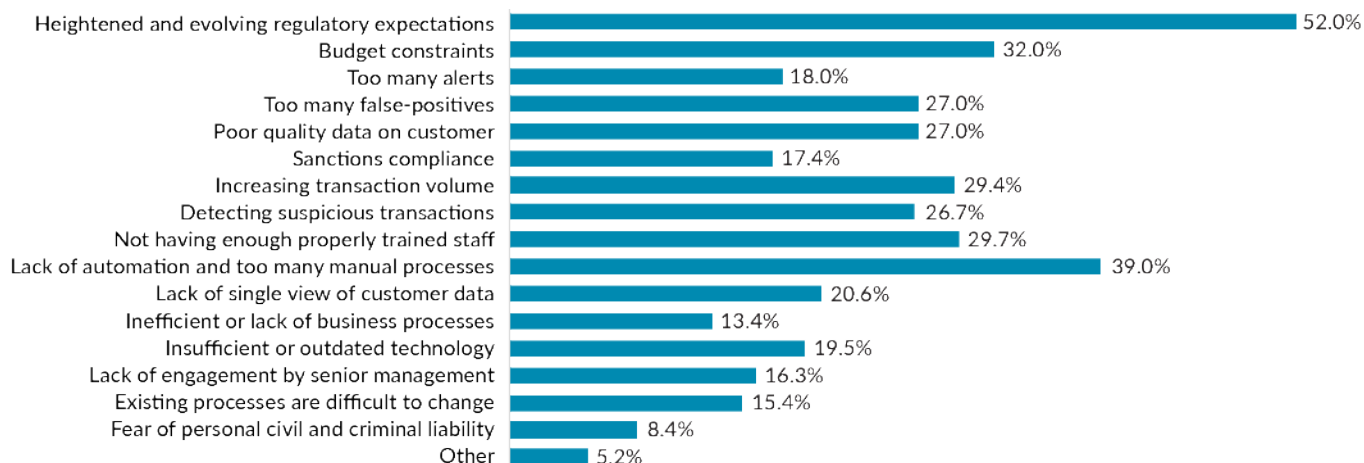
Fortunately, only a relatively small percentage of respondents cited lack of engagement by senior management (16.3 percent), inefficient or lack of business processes (13.4 percent), and/or difficulty in changing existing processes (15.4 percent) as an AML challenge.

The top three answers for respondents in the U.S were heightened and evolving regulatory expectations, budget constraints and not having enough properly trained staff.

Other AML challenges cited by respondents included:

1. Developing risk matrixes and risk models
2. Difficulty tracking source of funds for private equity firms and family businesses
3. Availability of beneficial ownership information

What are your organization's greatest AML challenges?



In this portion of the survey, respondents could select as many of the AML challenges as they encounter in their organization.

"The speed and the new innovations in payments are really going to be a challenge for BSA rules. The AML Act of 2020 has created a framework for looking at thresholds, how the rules work, and how things happen. But not much has been decided yet."

Shane Bauer, First Vice President - Compliance,
BSA and Security Officer, Bankers' Bank

"Commensurate with requirements for a risk-based approach, regulators should provide guidance with respect to how they evaluate the FI's AML/CFT programme against new expectations."

Carolyn A DaCosta, Group Chief Compliance
Officer & Corporate Secretary,
JMMB Group Limited

"Regulators and legislators should consider mandating that a purpose classification code be included with every electronic payment so that financial institutions have a record of the reason for the payment. I also think that all fraud should be required to be reported to a central repository, regardless of dollar amount."

This would allow financial institutions, payment processing companies, FinTechs and law enforcement to improve their fraud prevention capabilities."

Neil Kumar, Vice President, Compliance, Alloya Corporate FCU



Emerging Risks

Unsurprisingly, crypto and digital currencies were a concern for nearly half of the respondents. Cybercrime and data collections, storing and privacy were the next emerging risks that the respondents felt needed to be addressed.

Finally new ultimate beneficial rules, fraud, cannabis-related businesses and use of unregulated financial sector were a concern for about one in four respondents.

Fortunately for compliance teams, more third-party tools are becoming available to reduce the risk associated with these specific areas including crypto and cannabis intelligence data providers.

For beneficial ownership, more jurisdictions are in the process of establishing, or already have, beneficial ownership information databases. There are also a number of third-party data providers who offer the ability to ease the burden of determining ultimate beneficial owners.

The top 5 emerging risks from respondents in the U.S. were

1. Crypto and digital currencies
2. Cybercrime
3. Cannabis-related businesses
4. Data collection, storing and privacy laws
5. Fraud due to exploitation of economic stimulus and emergency measures

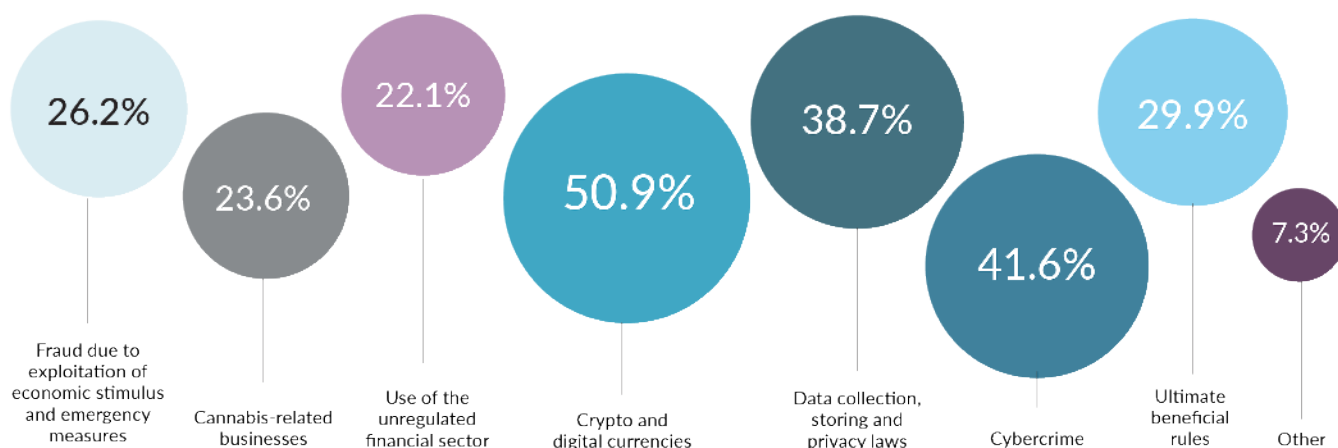
Other emerging risks cited by respondents include

1. The use of legacy systems
2. Online marketplaces and third-party payment processors
3. Limited political will relative to legal framework
4. Money flowing from bad, sanctioned actors into unregulated, unscrupulous investment vehicles
5. Inability to consolidate customer and transaction information from different databases

"In addition to more KYC requirements for virtual, crypto and digital currencies, there needs to be a revamp and upgrade of the records FIs can access online, including photo identification, complete and current companies registry documents, and land registry documents. This will facilitate digital onboarding, increase ease of doing business, and strengthen the financial system."

Carolyn A DaCosta, Group Chief Compliance Officer & Corporate Secretary, JMMB Group Limited

What are some emerging risks that you feel need to be better addressed by your organization?



In this portion of the survey, respondents could select the emerging risks that they felt needed to be addressed by their organization.

"We have fully implemented an ERM program here at Bankers' Bank and have gone through a couple of revisions of it already. But for banks that haven't done that yet, how do you really fine-tune your AML program if you don't have good measurements of risk across the organization? Every payment rail has its own fraud definitions. Every area of the bank might have different processes and procedures for how they handle their relationships with downstream banks or upstream vendors or whomever they are.

Without a good, solid risk assessment that actually has the same measuring system across the organization, you maybe have inaccurately measured risks. And if you have inaccurately measured risks, then you can't really do a risk-based AML program."

Shane Bauer, First Vice President - Compliance, BSA and Security Officer, Bankers' Bank



"We're seeing a lot more fraud due to business email compromises. This is primarily due to lack of security control best practices, especially at smaller businesses with limited resources.. All business entities, including small financial institutions, need to ensure that proper protections are in place so that their email servers and accounts cannot be infiltrated and manipulated by criminals."

Synthetic identity fraud is also still an issue. The Social Security Administration (U.S.) did roll out a system to confirm social security numbers with other data elements, but it's not available to everybody yet. The industry and individual consumers would benefit from a broader roll out of that system."

Neil Kumar, Vice President, Compliance,
Alloya Corporate FCU




Evolving AML Compliance Programs for VASPs

Given the increased use of virtual assets, your financial institution might be considering banking virtual asset service providers (VASPs). As outlined in a recent webinar, if you do decide to include VAs and VASPs as part of your business, here are some things that need to be done to mitigate risks:

- When evaluating cryptocurrency risks, the cryptocurrency type must be analyzed and understood. While each cryptocurrency type presents a different form of risk, privacy coins pose the highest risk from an AML/KYC Perspective.
- You need to **risk profile** all cryptocurrencies used by your clients. If a client is bringing money in from an exchange, you need to know the currency that they transacted with, work with the exchange to understand if there were other currencies involved and be informed of the types of transactions being performed by that user.
- You need to complete **enhanced due diligence** on any VASPs that you're going to do business with and understand the nature of the business, value and purpose and make sure the business is running legally and securely.
- Like with fiat currency, you need to conduct **transaction monitoring**. This is where blockchain forensics is incredibly important and can be used for when money comes in and for investigations after the fact.
- Finally, keep doing what you are doing. Everything you do with traditional fiat currency applies for cryptocurrencies including **sanctions screening, PEP screening, adverse media, etc.**
- New coins and new types of cryptocurrencies will continue to emerge as coins split (hard fork), new coins are developed, and new problems are solved through cryptocurrency. It is important to stay informed and assess the risk with each.

"There is a need for changes in legislation to facilitate a framework for the sharing of information across FIs. Information with respect to KYC, results of sanctions screening, adverse media screening etc. will augur well in the fight against financial crimes."

Carolyn A DaCosta, Group Chief Compliance Officer & Corporate Secretary, JMMB Group Limited

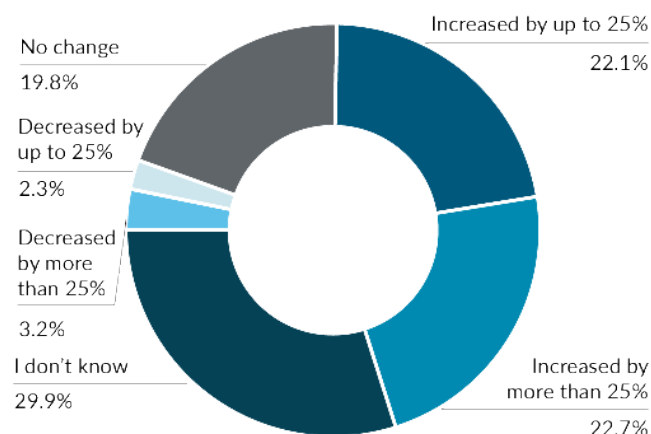


"As a result of the pandemic, smaller institutions — which weren't necessarily willing, ready, and able to be in the mobile-first environment - have now found themselves having to be there. Banks have been forced to accelerate the timeline on some of these hands-off processes. It will soon be time to take a close look at those processes and figure out are they effective? Are they efficient? Are you actually managing your risk? Do you really know these people you're doing business with? Do your tools work the way you think they do? That's all really important because if they don't, if they fail in any of that regard, the regulators will be viewing these as deficiencies. You don't get a pass because you didn't know what you're doing."

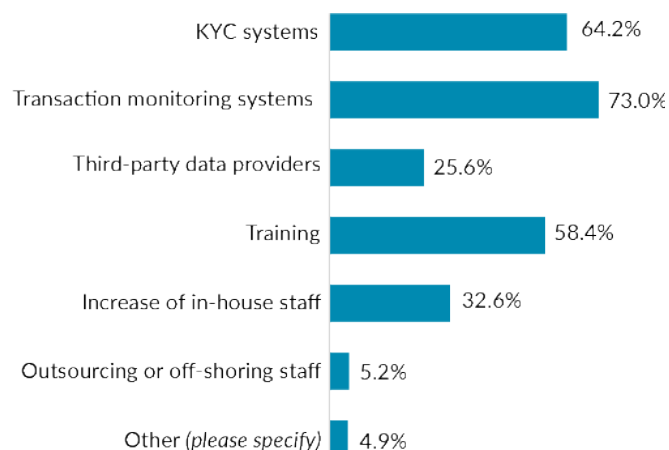
Shane Bauer, First Vice President - Compliance, BSA and Security Officer, Bankers' Bank

AML Compliance Budgets

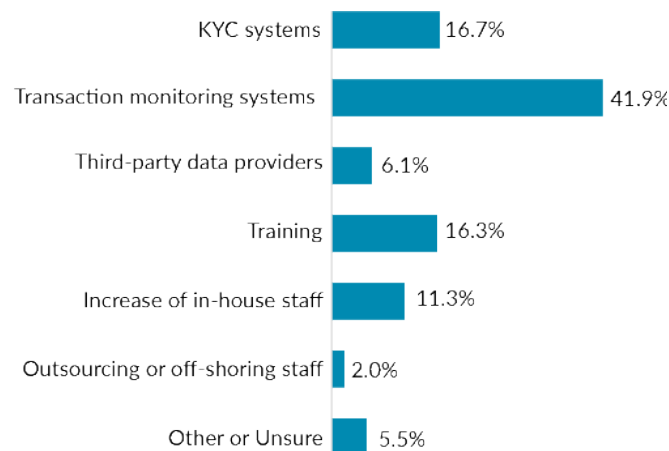
How much has total investment in AML activity changed compared to three years ago?



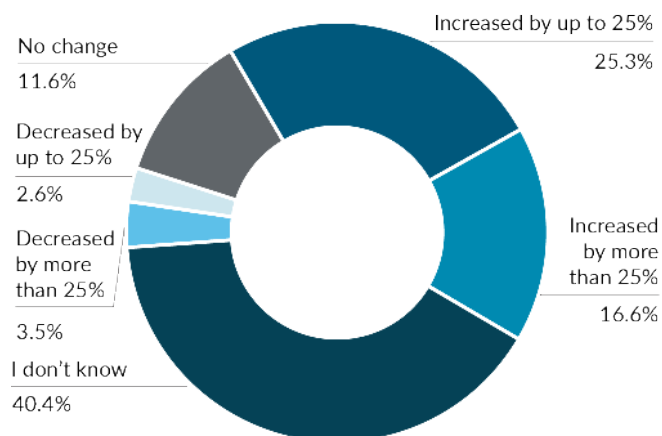
What are the top 3 areas for AML investment?




What is your greatest area of spend for your AML investments?



What is the anticipated change in AML investment in the next three years?





"Any tool that automates KYC requirements and effectively performs the risk assessment using core or client depository system as source is a game changer for the industry. Technology that is supported by artificial intelligence and behavior-based analytics to generate insights on alerts, identifying potential suspicious transactions more accurately and efficiently by reducing the number of false positives is another game changer.

Carolyn A DaCosta, Group Chief Compliance Officer & Corporate Secretary, JMMB Group Limited

"I'm not going to say machine learning has no role to play in AML compliance but there's not going to be full automation that comes out of it. I'm a technology guy and I get excited by the idea that machines can make decisions based on their own understanding of the world. But in the end if you can't explain why a machine made the decision it made, that isn't going to work for AML compliance or regulators.

Shane Bauer, First Vice President - Compliance, BSA and Security Officer, Bankers' Bank

In terms of investment, it was not surprising to see that nearly 45 percent of respondents said that investment in compliance increased in the past three years.

Twenty-five percent of respondents said their organization's investment in compliance was expected to increase by up to 25 percent in the next three years, while nearly 17 percent thought that it would increase by more than 25 percent.

Areas of greatest spend were KYC systems, transaction monitoring systems and training. Increase of in-house staff or outsourcing and offshoring was a top spend for nearly 38 percent of respondents.

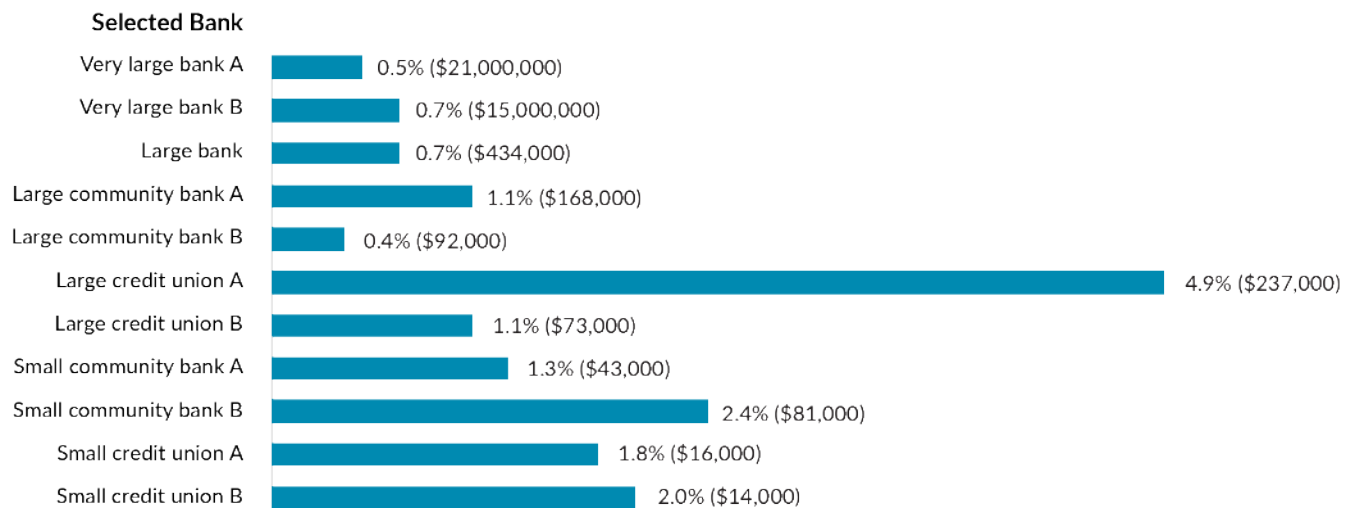
Other areas of spend mentioned by respondents included case management systems, digital onboarding systems, anti-fraud technology and sanctions screening systems.

In terms of top area of spend, nearly 42 percent answered with transaction monitoring systems. KYC systems was the next area of spend, followed by training. KYC systems was the next area of spend, followed by training.

"Risk is evolving rapidly and most times FIs are usually trying to catch up with the changes. Challenges include rapid changes in the industry, slow pace of regulatory changes and client reluctance to provide detailed and accurate information, particularly in areas such as beneficial ownership."

Carolyn A DaCosta, Group Chief Compliance Officer & Corporate Secretary, JMMB Group Limited

Estimated Total Direct Costs for Complying with the Bank Secrecy Act as a Percentage of Operating Expenses and Estimated Total Direct Compliance Costs for Selected Banks in 2018



Source: GAO analysis of data from selected banks, Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, and National Credit Union Administration. | GAO-20-574

In 2020 the U.S. Government Accountability Office (GAO) released a report called “Anti-Money Laundering: Opportunities Exist to Increase Law Enforcement Use of Bank Secrecy Act Reports, and Banks’ Costs to Comply with the Act Varied”.

In it, the government watchdog reviewed a sample of 11 banks that varied in terms of their total assets (and other factors) and estimated that their total direct costs for complying with the Bank Secrecy Act ranged from about \$14,000 to about \$21 million in 2018.

The group also found that BSA compliance costs generally tended to be proportionally greater for smaller banks than for larger banks and that costs can differ between similarly sized banks due to differences in compliance processes, customer bases, and other factors.



Onboarding and Customer Due Diligence Checks

When it comes to onboarding and customer due diligence, 83 percent of respondents said they leverage identity verification checks. 62 percent used business formation documents, annual reports and financial statements while 61 percent used beneficial ownership tools

For screening, 68 percent used PEP screening tools, 60.2 percent used negative news checks and nearly 50 percent used enhanced watchlist checks. Only a little under 23 percent used third-party enhanced due diligence (EDD) reports.

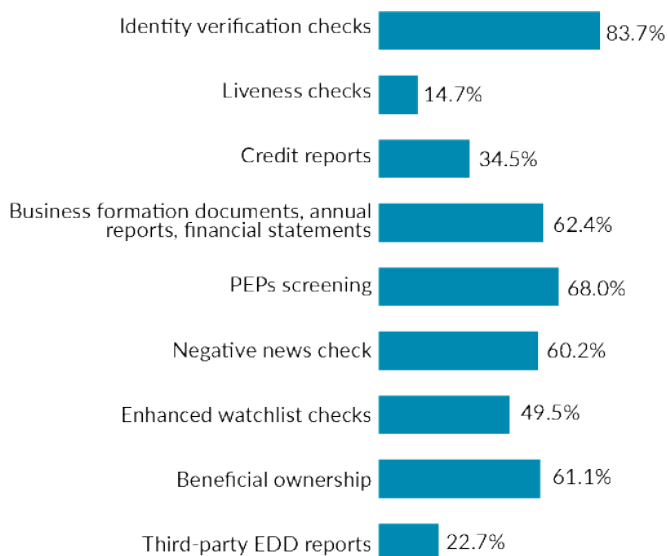
Liveness checks is a relatively new technology for respondents with only 14.7 percent saying that

they used this tool as part of their customer identification program.

Other technology trends for financial institutions to consider for KYC include

- Automation tools to reduce repetitive tasks
- Analytics, machine learning and artificial intelligence to improve detection of anomalies
- Data cleansing and data enhancing tools to reduce the effort to collect information, enter missing information and reduce duplication

What tools do you leverage during onboarding and for customer due diligence checks? *(Check all that apply)*



"FIs have to be mindful of the length of time to on-board a new customer yet in order to determine the risk associated with a customer you have to know the customer. The more documentation that is required, the longer the service delivery time which affects customer satisfaction. Adding to the challenges is a lack of public registry on some critical KYC matters, such as national registry of local PEPs."

Carolyn A DaCosta, Group Chief Compliance Officer & Corporate Secretary, JMMB Group Limited

"One challenge with the beneficial ownership requirement is, unlike every other BSA rule, it is by account instead of by customer. Customers get really upset when they keep getting asked, over and over and over again, for their beneficial ownership information. We have leasing customers that open 30 or 40 leases a year with us and for every one of them we need a-nothing-has-changed form. They don't like it, and I don't blame them. They keep asking "Why do you have to keep doing this?" and all we can say is that's the way the law is written and we can't help it."

Shane Bauer, First Vice President - Compliance,
BSA and Security Officer, Bankers' Bank

"Since the pandemic (COVID), institutions are looking into alternate methods of servicing their members. They're looking at ITMs (interactive teller machines) and online banking requests. Those considering this need to have the right security features and controls in place to actually identify and confirm legitimate requests. With the dark web, a lot of the personal information is available for most consumers. So the challenge becomes, how are you making sure that your MFA (multi-factor authentication) questions are not related to information that is publicly available?"

Neil Kumar, Vice President, Compliance,
Alloya Corporate FCU



Customer Risk Profile

High quality data is a key requirement for assessing risk. When determining the risk associated with a customer, 52.4 percent said that getting access to current and historical customer profiles was one of their greatest challenges.

Getting a view of connection with other potentially high-risk or sanctioned entities and having a complete view of all transactions were the next biggest challenges when looking at customer profiles.

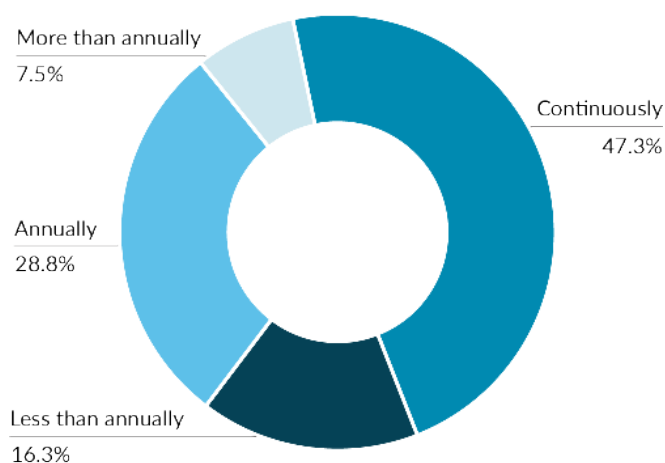
In terms of identifying the risk levels of customers, 34.5 percent said that testing, validating and documenting risk models were a challenge, while 32.9 percent said that it was being able to apply

different risk calculation models depending on segmentation.

Other challenges mentioned by the respondents include:

- Determining beneficial owners and percent of ownership
- Having properly trained frontline staff that ask the right customer due diligence and enhanced due diligence questions
- Unscrupulous actors/firms who lie about their activities and are able to conceal illicitly acquired funds.

How often does your organization review the risk profile of customers?

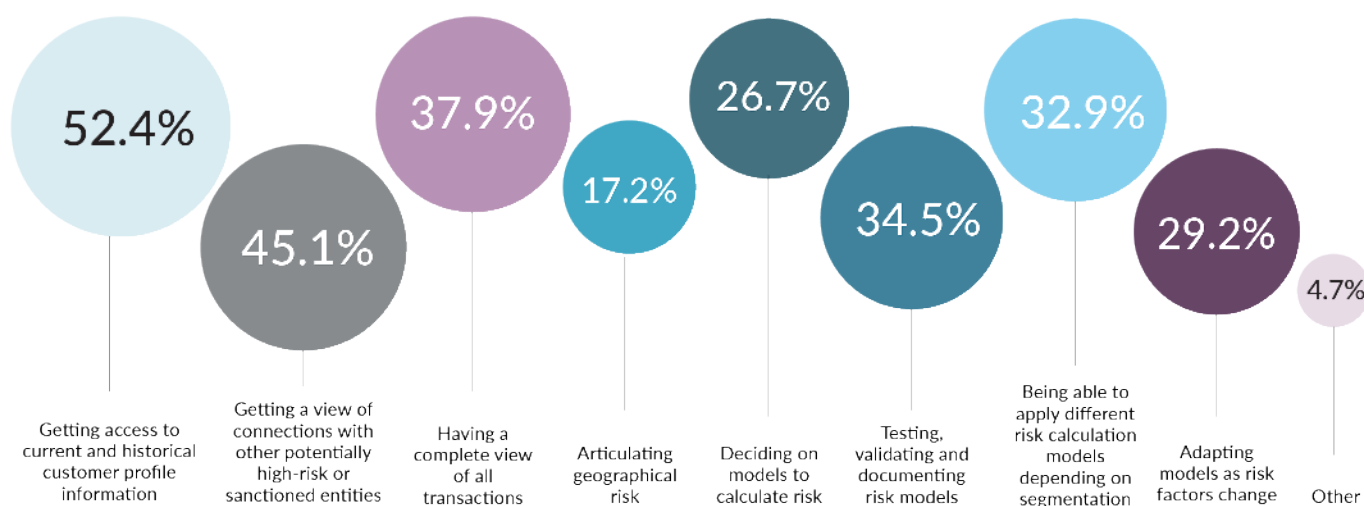


"Model risk governance is one of the challenges in implementing a risk-based AML program. Financial institutions need to have the discipline and practice to periodically retune and test the risk model, the analytic parameters, and the screening parameters. They also need a very simplified user-friendly automated monitoring solution."

Neil Kumar, Vice President,
Compliance, Alloya Corporate FCU



What are some of the greatest challenges when trying to determine the risk associated with a customer? (check all that apply)



"Adopting a risk-based approach to AML can be challenging in a group or enterprise wide institution but it is particularly challenging when (1) regulators are very prescriptive, (2) National Risk Assessment and other documents which contain national priorities are not published in a timely manner, (3) internal and external auditors don't change their focus of review to address the new focus of a risk-based AML/CFT programme, and (4) inappropriate resources are invested for the development and maintenance of a risk-based approach."

Carolyn A DaCosta, Group Chief Compliance Officer & Corporate Secretary,
JMMB Group Limited



Determining Geographical Risk

Geographic risk alone does not necessarily determine a customer's or a transaction's risk level. Unfortunately, there is no standardized measurement of a country's money laundering risk. As a result, financial institutions need to develop their own models to determine risks associated with a jurisdiction.

Risk indicators can be separated into four high level categories:

- Quality of the AML/CFT regulatory framework
- Financial transparency and regulations
- Bribery and corruption levels
- Involvement/support of sanctioned activities

To help calculate the risk associated with geography, here are some tools to consider:

- Basel Index – a country ranking and review of money laundering and terrorist financing risks around the world

- FATF data – use whether country is a member of FATF, a FATF-style regional body member, a country or a black list country
- Tax justice network – indicates country rankings for corporate tax haven and financial secrecy
- Transparency International Perceptions Index – indicates perceived levels of public sector corruption
- TRACE Bribery Risk Matrix – Measures business bribery risk in 200 countries

To learn about how to use this data to calculate geographic risk, watch our presentation on Elements of Customer Risk: Assessing AML Geographic Risk.

"One of the greatest challenges when determining risk is the lack of data at the front line. We need to be able to promptly identify that there's been a change in historical payment patterns when the person is right in front of you. To do this, your automated monitoring solution (AMS) should be tied with your core system to then send an alert when there is an unusual transaction."

Neil Kumar, Vice President, Compliance, Alloya Corporate FCU



"As clients move further from the physical branch, the risk of fraud and money laundering increases – so I anticipate major investments in new technology (i.e, facial recognition). Upgrades of monitoring systems to better manage the risk of virtual transacting, as well as, investment in existing team members who have to manage these systems to ensure the control structures are in place to deal with emerging technologies will also be an investment area."

Carolyn A DaCosta, Group Chief
Compliance Officer & Corporate Secretary,
JMMB Group Limited

"As a bank for banks, if there are specific products that create more BSA or AML risk for us, we'll do some additional due diligence, and we'll take a close look at certain aspects of their programs, depending on what we have concerns about. What we do rely on the fact that they're banks, and they're banks that are still in operation, and they've gotten the stamp of approval from the regulators. And so, that means that they must be doing something right."

Shane Bauer, First Vice President -
Compliance, BSA and Security Officer,
Bankers' Bank

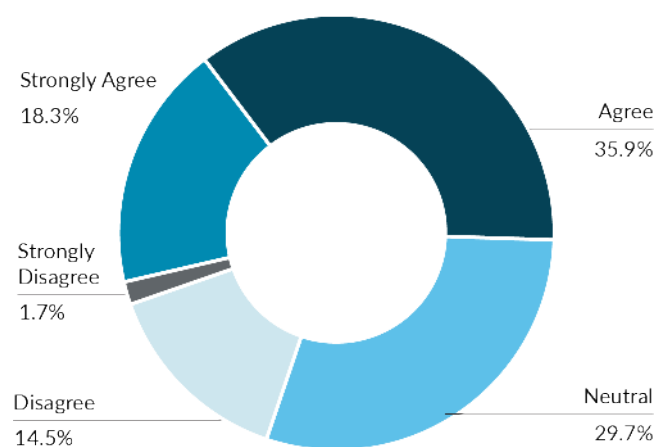
Transaction Monitoring

When it comes to transaction monitoring, the survey focused on understanding how our respondents felt about their current systems and whether it was flexible enough to meet some of their most basic needs.

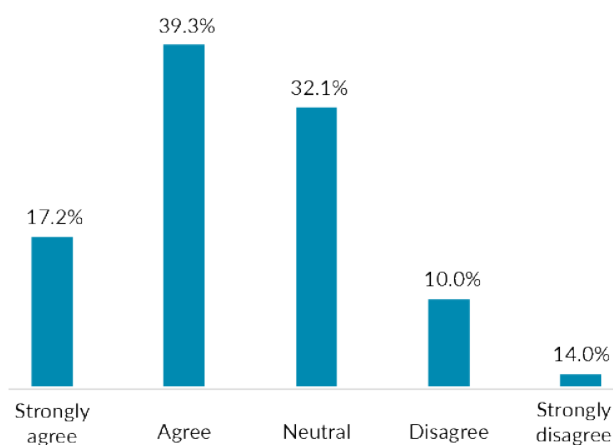
In terms of satisfaction with their existing systems, 54.2 percent agreed or strongly agreed that they were satisfied with their existing solution. Fifty-six and half (56.5) percent agreed or strongly agreed that it was effective at detecting suspicious activities while, 45.2 percent agreed, or strongly agreed that their transaction monitoring system can be easily updated with new threat scenarios.

We saw similar ratios when looking at whether the systems could be tuned to reduce false positives and monitor transactions across multiple business units and multiple jurisdictions.

I am satisfied with the performance of my transaction monitoring system.

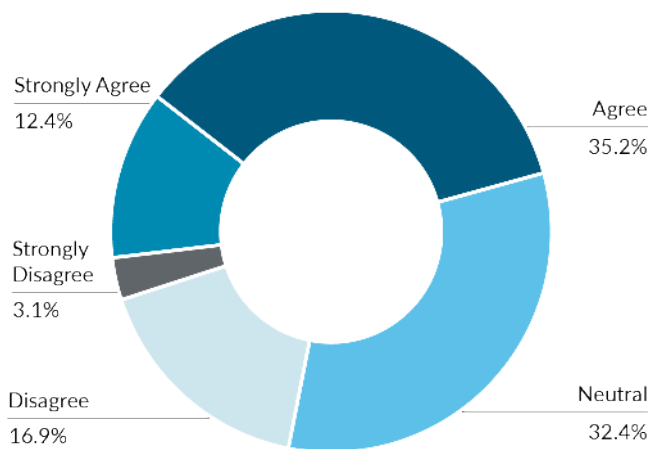


My organization's transaction monitoring system effectively identifies suspicious transactions.

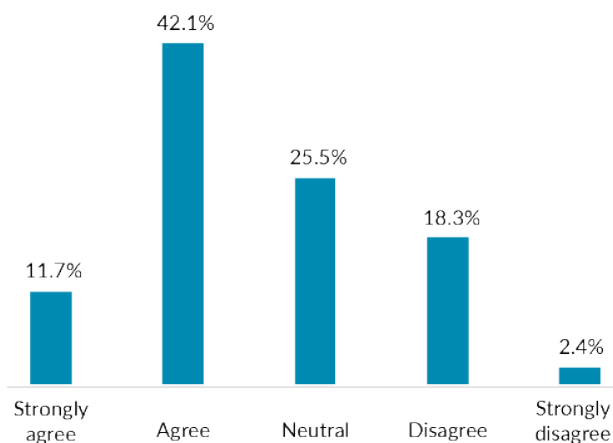




My organization's transaction monitoring system is effectively tuned to reduce the number of false positives.



My organization's transaction monitoring system provides all the information my investigators need to review the suspicious transactions.



"The speed of transactions is increasing. We've got instant payments of different types coming online, and the compliance regimes around those are unclear. Cryptocurrency is in its infancy, and its impact on financial services right now, especially for smaller institutions, is minimal, but that will change. It's just too good of a rail and too suited to certain uses, not all of which involve crime."

Shane Bauer, First Vice President - Compliance, BSA and Security Officer, Bankers' Bank

Transaction Monitoring Analytics

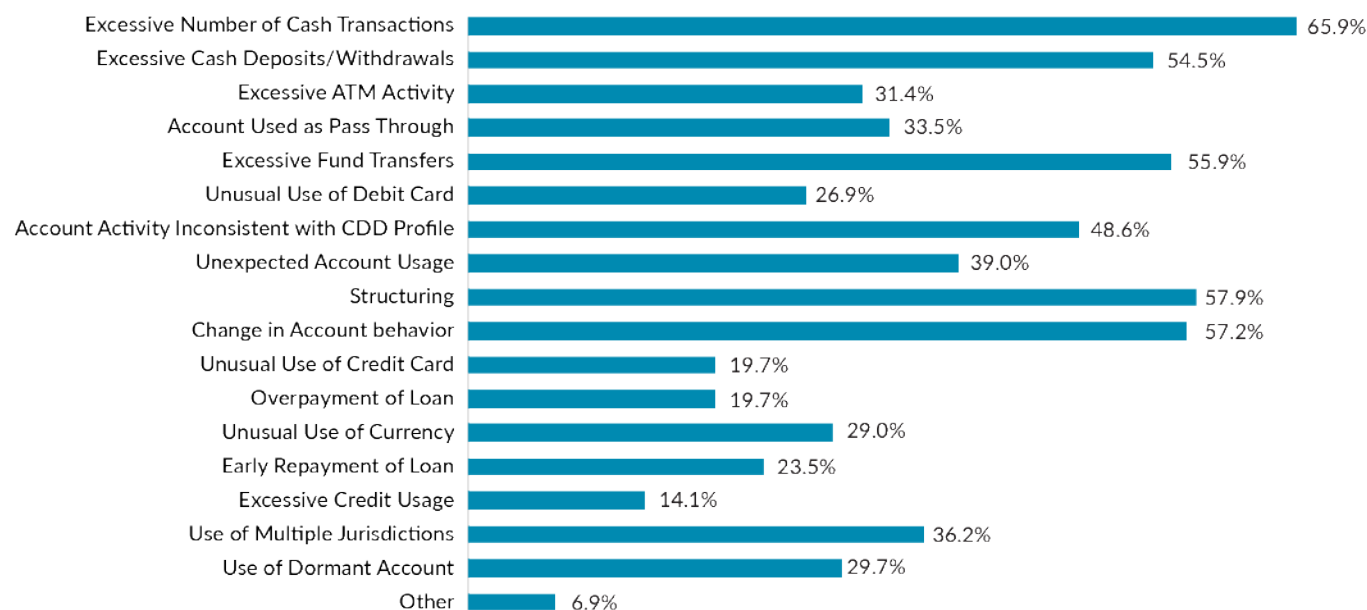
Analytics are a pillar of transaction monitoring systems. We asked our respondents for the scenarios that they use in their transaction monitoring systems.

Unsurprisingly, excessive number of cash transactions, cash deposits/withdrawals and funds transfers were the most popular analytics. Unusual credit card use was the least used analytic, likely due to the profile of the respondents.

Here are some of the other scenarios used by respondents' transaction monitoring platforms:

- Income commensuration with type of business
- Cash deposits to facilitate wire transfers
- Wire transfers followed by cash withdrawals
- Non face-to-face transactions
- Transactions exceeding threshold
- High-risk customers
- Staff accounts

Which of the following scenarios do you use in your transaction monitoring platform? *(check all that apply)*





What Compliance Want from their AML Solutions

ID Verification Be able to include mortgages to monitor mortgage payments and payoffs
Freely create and modify data sources **Workflows** Built in negative news check
Reduce the amount of false positives **End-to-end digital onboarding**
Dynamic risk rating Connected and easier filing to regulators
Display customer account activity for past year during alert review
Ability to detect foreign-sourced wire transfers going through a US correspondent bank
Block repeat customers transactions after not providing documents **Audit Trails**
Real-time KYC Beneficial owner information and identifiers
Daily OFAC and screening for customers, suppliers and directors
Intermediary wires functionality and rules Reduce the amount of false positives
Client Risk Management Birthdate on all Alerts
Ability to search businesses/people and address within it
Red flag alerts More rigorous screening algorithms
Risk assessment on account and transactions **PEPs and sanctions detections**
Customer Due Diligence Customer behavior deviation
CIP methods to detect inconsistencies in application
Connections and link analysis Transaction velocity
Standard, customizable scenarios with ability to create scenarios
Ability to monitor activity across business **Risk Scoring listed on Main Page**
Monitor Virtual currency transactions Machine learning to prefill SARs
Case management system **Built in analytics and reporting tools**
Improved AML/BSA Alert Scenarios **Cloud**
Real-time transaction monitoring and notification

AML Compliance with Alessa

Alessa provides all the anti-money laundering (AML) capabilities that banks, money services businesses (MSBs), fintechs, casinos and other regulated industries need – all within one platform. Capabilities of the product include:

Due Diligence: To support KYC, CDD, and EDD processes, Alessa combines data from onboarding systems with identity verification and risk intelligence data to provide a risk score based on profile, activities and relationships.

Sanctions Screening: Alessa screens individuals and businesses against multiple lists including PEPs, negative news, OFAC, and other sanctions lists. Screening can be done in native characters and in real time, periodically or on demand.

Transaction Monitoring: Alessa analyzes every transaction in real-time and using advanced analytics, generates alerts for suspicious activities. These are directed to the appropriate personnel for investigation and/or reporting.

Regulatory Reporting: All suspicious activity alerts include data needed for regulatory reports. Once it is determined that a Suspicious Transaction Report or a Suspicious Activity Report needs to be filed, Alessa can auto-populate (and electronically file) as many as 70% of these reports. Alessa can also automate as much as 100% of CTRs.

Risk Scoring: Alessa uses data from various sources, including sanctions lists, to provide an assessment of the risks of doing business with an individual or business. The solution also periodically reviews an

organization's customer base and updates their risk level based on their activity and third-party data.

Configurable: With Alessa, organizations can select the functionality they need or the complete solution. Permission-based functionality allows different users to access only the information they need to perform their responsibilities, and data can be maintained in the cloud or on-premise, ensuring compliance with regulations.

Data Management: Alessa accesses data from any platform, including ERPs, bespoke applications, and core business systems. The data is then cleansed and aggregated to increase its accuracy, and cross-referenced to reveal big-picture insights. Better data means better insights.

Investigation Tools: Alessa offers dynamic workflows to guide processes and investigations. Enterprise search capabilities allow for easy searching of data within internal and external sources, while case management offers a collaborative approach to investigations, compliance, and decision making.

Metrics & Insights: Alessa offers configurable dashboards that track key metrics and allow compliance staff to drill down into the alerts. Advanced analytics allow for sound decision-making and actions to be taken based on comprehensive information and insights.

To learn more about how Alessa can help with your AML compliance activities, visit www.tier1fin.com/alessa/

About Alessa

Alessa, by Tier1 Financial Solutions, is a compliance, controls monitoring and fraud prevention solution for banking, insurance, fintech, gaming, manufacturing, retail and more. With deployments around the world, Alessa allows organizations to quickly detect suspicious transactions, identify high-risk customers and vendors and decrease fraud risks that reduces profitability and increases costs. To learn more about how Alessa can help your organization ensure compliance to regulations, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at <https://www.alessa.com/>.



150 Isabella Street, Suite 800,
Ottawa, ON K1S 1V7, Canada



1-844-265-2508



alessa@tier1fn.com



www.alessa.com

