

# DOW JONES & SWIFT

---

GLOBAL ANTI-MONEY LAUNDERING  
SURVEY RESULTS 2017



DOW JONES



# Contents

- 2** Contents & Infographic
- 5** Executive Summary
- 6** Survey Highlights
- 8** AML Challenges & Workloads
- 14** AML Data Providers
- 16** Client Screening
- 24** Data Cleansing, Fraud & Sanctioned Lists
- 29** Payments Transparency/Traceability
- 31** Peer Assessments
- 33** Human Trafficking
- 34** Trade Compliance
- 36** Regulatory Technology

## REGULATION TECHNOLOGY [PAGE 36]



Nearly **60%** agree RegTech has improved their ability to handle AML, KYC and sanctions requirements



**More than half** are likely to increase RegTech investments in the next 3-5 years

## PAYMENT PROCESSES [PAGE 29]



**NEARLY  
65%**

report their organizations have systems in place to check their own payments transparency data quality and monitor the data provided by other banks.

## MOST COMMON SCREENING SOURCES [PAGE 34]



**MORE THAN  
50%**

report their organizations screen transactions against controlled goods lists, most often the U.S. Commerce Control List and EU Dual Use Goods List.

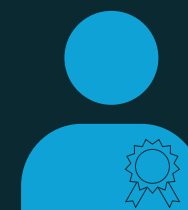
## LIST UPDATES [PAGE 27]



**Nearly 90%** expect internal lists to be updated within 24 hours of changes to sanctioned/official lists.

## ORGANIZATIONAL CHALLENGES [PAGE 10]

Main organizational challenges facing companies:



Having enough trained staff



Relying on outdated technology



Too many false-positive alerts

## Executive Summary

As a maturing market, there is a growing need to understand how companies are dealing with the current regulatory environment and to assess how new regulations are impacting the way companies work.

The 2017 global anti-money laundering survey, sponsored by Dow Jones Risk and Compliance and SWIFT, surveyed over 500 risk executives around the world to:

- Assess the current regulatory environment and impact on organizations
- Deepen understanding of client-screening processes, content and systems
- Explore emerging issues related to regulatory expectations, data cleansing, fraud detection, sanctioned lists, payments transparency/traceability, peer assessments, human trafficking, trade compliance and regulatory technology
- Trend key measures from previous AML surveys

To see how Dow Jones is using these and other insights to build industry-leading third party risk management and regulatory compliance solutions, visit [www.dowjones.com/products/risk-compliance](http://www.dowjones.com/products/risk-compliance).

SWIFT provides a growing portfolio of sanctions, know your customer (KYC), anti-money laundering (AML) and anti-fraud offerings that help financial institutions combat financial crime effectively and efficiently while fostering regulatory compliance and a more secure, dependable and entrusted payments ecosystem. For more information, visit [www.swift.com/complianceservices](http://www.swift.com/complianceservices).

**DOW JONES RISK & COMPLIANCE TEAM**  
**SWIFT FINANCIAL CRIME COMPLIANCE TEAM**

# Survey Highlights

## REGULATORY CHALLENGES AND WORKLOADS

Increased regulatory expectations continue to represent the greatest compliance challenge, followed by concerns about increased enforcement of current regulations.

## ORGANIZATIONAL CHALLENGES

Concerns about having enough trained staff, relying on outdated technology and getting too many false-positive alerts are the main organizational challenges facing companies.

## ADDED WORKLOADS

OFAC and EU 50% Rule sanctions and the FINCEN CDD Rule (both new in 2017 survey) are cited by over 70% of respondents as contributing to increased workloads. FATCA, the Fourth EU Money Laundering Directive and other tax evasion legislation are the other regulations mentioned by more than half of respondents as adding to workloads.

## DATA ACCURACY REMAINS MOST IMPORTANT

Data accuracy remains the single “most important” factor in choosing AML data providers. Almost 65% of respondents report their organizations are using multiple AML data providers.

## FIGHTING FRAUD

Over 65% work in companies in which the AML department handles fraud detection and prevention, an increase from 2016.

## VERIFICATION ON THE RISE

Nearly half of respondents report their companies adhere to the standard of 25% beneficial ownership verification. The proportion requiring 10% verification increased in 2017 to more than 30%.

## LIST UPDATES

Nearly 90% expect internal lists to be updated within 24 hours of changes to sanctioned/official lists.

## PAYMENT PROCESSES

Nearly 65% report their organizations have systems in place to check their own payments transparency data quality and monitor the data provided by other banks. Among these companies, over 90% have a view of all the payments systems in place across groups.

## REPORT ORDERING

Over 75% represent organizations that get benchmark and/or peer comparison reports, with regulators and consultancy/advisory companies mentioned as the most frequent sources of the reports.

## THIRD-PARTY TESTING

Overall, 70% report their companies do some type of systematic third-party testing. 70% report their organizations have modified AML training and/or transaction monitoring to incorporate human trafficking and smuggling red flags and typologies, a decrease from 2016.

## MOST COMMON SCREENING SOURCES

More than half report their organizations screen transactions against controlled goods lists, most often the U.S. Commerce Control List and EU Dual Use Goods List. Most of these companies use risk based on origin/destination, industry-standard red flags and trade profile deviations as controls to detect trade-based money laundering.

## REGULATION TECHNOLOGY

Nearly 60% agree RegTech has improved their ability to handle AML, KYC and sanctions requirements. More than half are likely to increase RegTech investments in the next 3-5 years.

2017 total results are compared to 2015 and 2016 to measure trends; statistically significant differences between 2016 and 2017 are noted with arrows.

# AML Challenges & Workloads

## CURRENT REGULATORY CHALLENGES

Increased regulatory expectations continue to represent the greatest compliance challenge, cited by nearly 70% of respondents, followed by concerns about increased enforcement of current regulations. (Nearly all issues are mentioned more often in 2017 compared with 2016, but survey changes likely contributed to these increases).

	2015	2016	2017	MAIN CHALLENGE
Increased regulatory expectations*	62%	60%	69% ↑	42%
Increased enforcement of current regulations*			50%	18%
Understanding regulations outside home country	23%	25%	42% ↑	16%
Additional regulations	26%	26%	37% ↑	11%
Understanding regulations in home country	9%	9%	22% ↑	5%
Formal regulatory criticism	15%	19%	18%	6%

## AML COMPLIANCE CHALLENGES IN NEXT 12 MONTHS

Increased regulatory expectations and enforcement of current rules continue to be the key future challenges for AML professionals. In addition, concerns about future additional regulations are mentioned by nearly 50% in 2017. (Nearly all issues are mentioned more often in 2017 compared with 2016, but survey changes likely contributed to these increases).

	2015	2016	2017
Increased regulatory expectations*	58%	57%	64% ↑
Increased enforcement of current regulations*			49%
Additional regulations	37%	40%	47% ↑
Understanding regulations outside home country	16%	18%	29% ↑
Understanding regulations in home country	8%	7%	20% ↑
Formal regulatory criticism	13%	16%	17%

Response list was reduced in 2017; interpret YOY changes with caution

\* Was single combined item 2015 & 2016

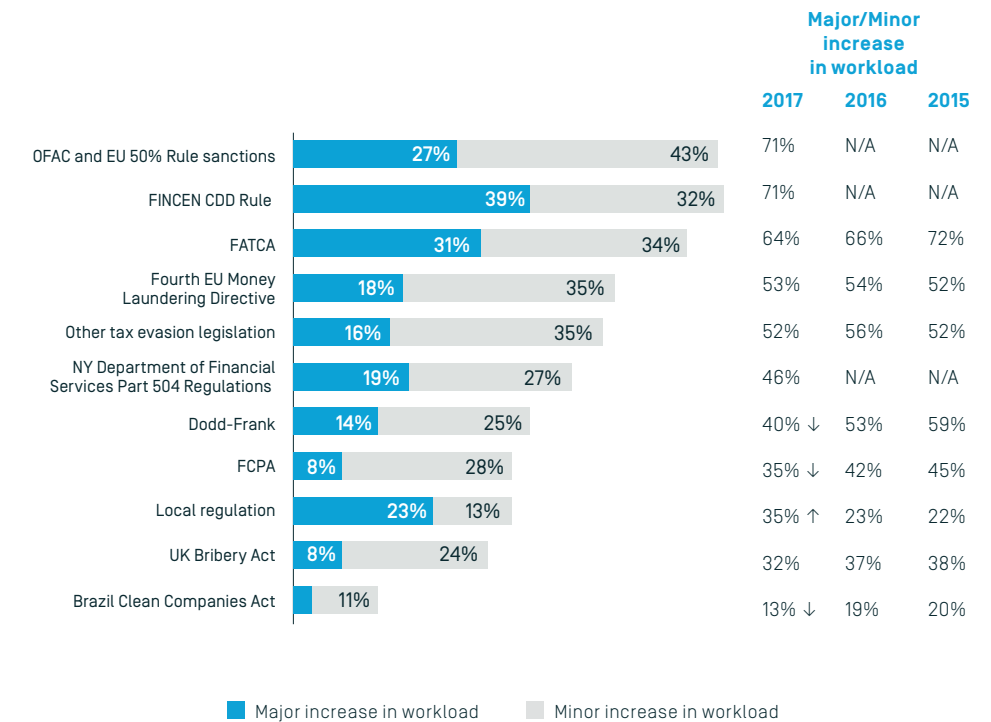
## CURRENT ORGANIZATIONAL CHALLENGES

Concerns about having enough trained staff, relying on outdated technology and getting too many false-positive alerts are the main AML-related organizational challenges facing companies. Budgetary constraints/scrutiny are also mentioned by more than one-third of respondents.

	2017	MAIN CHALLENGE
Having enough properly trained AML staff	57%	26%
Insufficient, inadequate or outdated technology	48%	24%
Too many false positive screening results	46%	16%
Budgetary constraints and increased scrutiny related to independent third party reviews	35%	11%
Avoiding sanctions enforcement actions	20%	5%
Fear of personal civil & criminal liability	17%	5%
Lack of senior management / Board of Directors engagement	17%	6%
A regulatory fine	15%	3%

## IMPACT OF REGULATIONS ON ORGANIZATION WORKLOAD

OFAC and EU 50% Rule sanctions and the FINCEN CDD Rule (both new in 2017 survey) are cited by over 70% of respondents as contributing to increased workloads. FATCA, the Fourth EU Money Laundering Directive and other tax evasion legislation are the other regulations mentioned by more than half of respondents as adding to workloads. The proportion mentioning local regulations increases in 2017, while the proportions citing Dodd-Frank, FCPA and the Brazil Clean Companies Act decrease.



## REGULATION WITH MOST IMPACT ON ORGANIZATION WORKLOAD

The FINCEN CDD Rule (new in 2017 survey) is cited by nearly 20% of respondents as the regulation most responsible for increased workloads, followed by local regulations and FATCA. The relative impact of Dodd-Frank continues to decrease. The proportion of respondents who claim none of these specific regulations have a major impact on workloads decreases from 2016 to 2017.

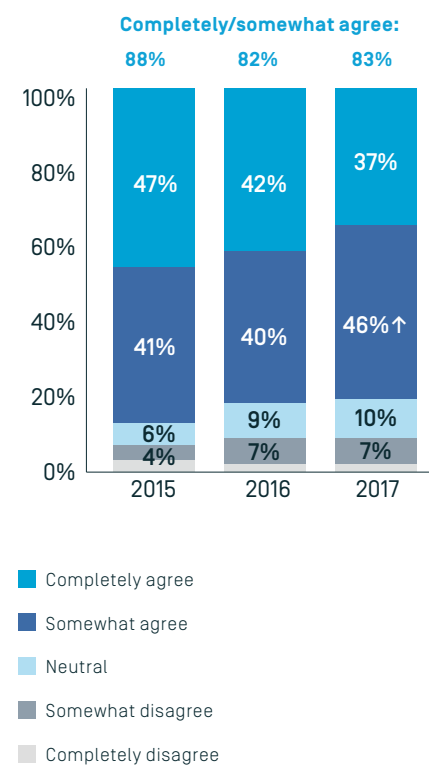
	2015	2016	2017
FINCEN CDD Rule			19%
Local regulation	8%	9%	13%
FATCA	17%	11%	11%
OFAC and EU 50% Rule sanctions			8%
Fourth EU Money Laundering Directive	5%	5%	5%
NY Department of Financial Services Part 504 Regulations			5%
Dodd-Frank	16%	8%	4% ↓
Other tax evasion legislation	2%	2%	3%
None will cause major increase	39%	35%	29% ↓

Mentions less than 3% in all years omitted

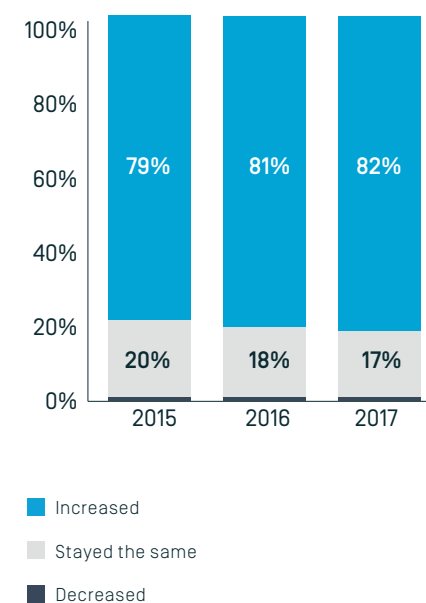
## COMPANY RISK POLICIES & OPERATIONAL EFFECTIVENESS

More than 80% of respondents continue to believe their companies' risk policies and/or operations reflect a convergence of global compliance disciplines, although the proportion who "completely agree" is decreasing. As in previous years, about 80% report increased regulatory expectations for operational effectiveness in the past 12 months.

### POLICIES/OPERATIONS REFLECT CONVERGENCE OF COMPLIANCE DISCIPLINES



### CHANGE IN REGULATORY EXPECTATIONS FOR OPERATIONAL EFFECTIVENESS IN PAST 12 MONTHS



# AML Data Providers

## KEY FACTORS IN CHOOSING AML DATA PROVIDER

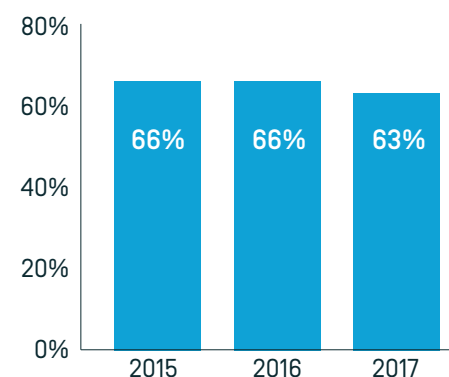
Compliance professionals continue to cite data accuracy as the single “most important” factor in choosing AML data providers. Well-structured data, depth of content, customer service, conforming to international standards and company reputation are also “very important” for 60% or more of respondents. The importance of implementation speed increases in 2017.

	2015	2016	2017
Data accuracy	89%	89%	88%
Well-structured data	74%	75%	76%
Depth of content	64%	65%	67%
Customer Service/support	63%	63%	66%
Conforms to international standards	57%	63%	65%
Company reputation		60%	63%
Speed of implementation	51%	48%	57% ↑
Breadth of content	56%	57%	57%
Data quality verified by 3rd party	48%	49%	52%
SME/staff knowledge	51%	51%	51%
Price	47%	51%	50%
Recommended by regulators/FIU's	42%	43%	48%
Technology independent	42%	43%	47%
Suite of products	42%	42%	44%
Used by similar organizations	29%	32%	34%
Local presence	23%	24%	29%
Existing vendor relationship	21%	19%	25%

## NUMBER OF AML DATA PROVIDERS USED

Similar to previous years, almost 65% of respondents report their organizations are using multiple AML data providers. Comprehensiveness remains the most-mentioned reason for using multiple providers, although coverage of specialized risk categories and decentralized AML regional requirements both increase in 2017.

### USE MULTIPLE SANCTIONS, PEP AND/OR ADVERSE MEDIA DATA PROVIDERS



### REASONS FOR USING MULTIPLE DATA PROVIDERS (AMONG THOSE USING MULTIPLE DATA PROVIDERS)

	2015	2016	2017
Comprehensiveness	55%	57%	55%
Specialized risk categories	40%	42%	51% ↑
Decentralized AML structure regional requirements	23%	19%	34% ↑
Result of legacy systems/contracts	27%	31%	32%
Risk of data provider outage	13%	16%	23%
Result of company acquisitions	12%	10%	14%

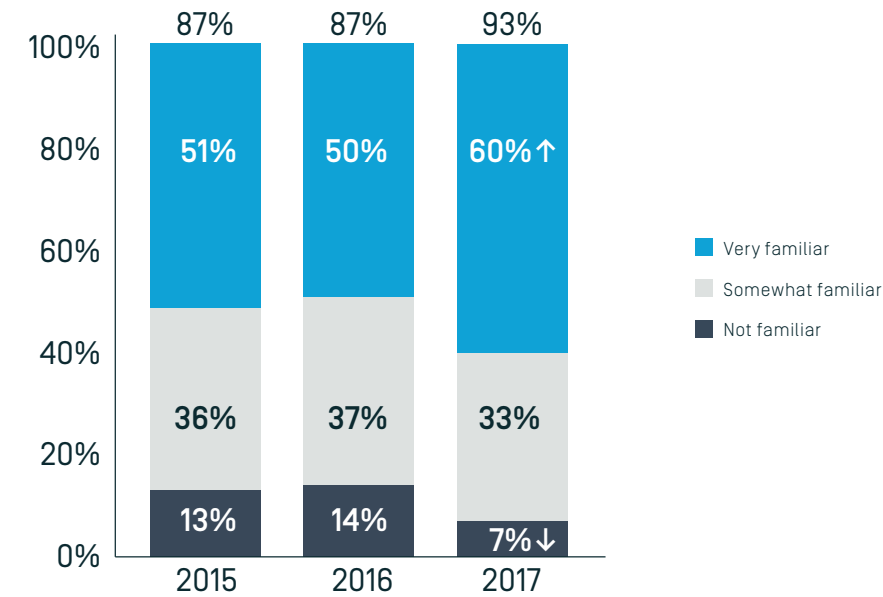


# Client Screening

## FAMILIARITY WITH CLIENT-SCREENING PROCESS IN ORGANIZATION

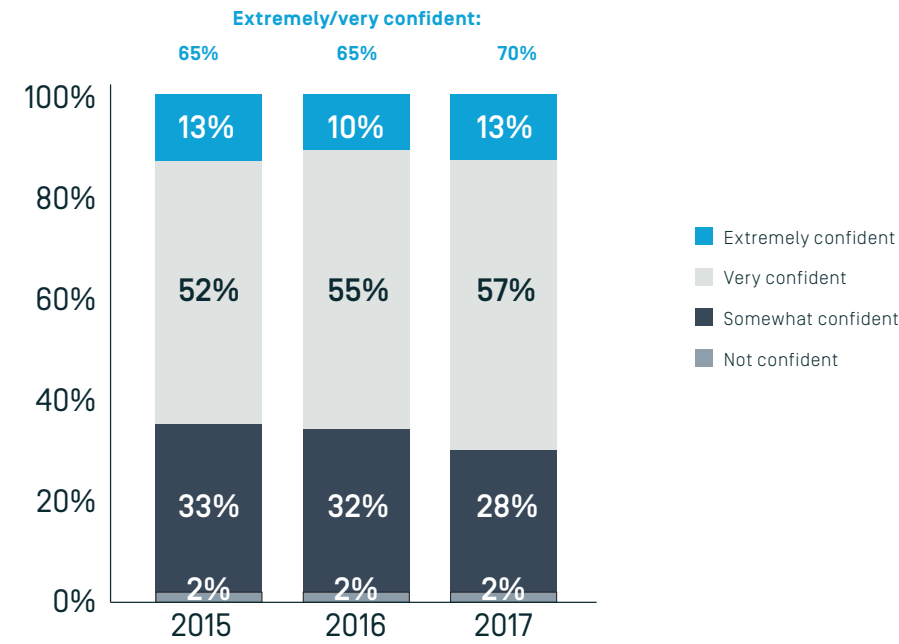
The majority of respondents are “very familiar” with the client-screening processes in their organizations, an increase from 2016. The remainder are mostly “somewhat familiar” with the processes.

AMONG THOSE WITH CLIENT SCREENING AS A MAIN FUNCTION



## CONFIDENCE IN CLIENT-SCREENING PROVIDER DATA ACCURACY

More than two-thirds of respondents remain “extremely” or “very confident” in the data accuracy of their primary data provider. Confidence levels have been steady in recent years.



## REASONS FOR LACK OF FULL CONFIDENCE IN CLIENT-SCREENING DATA ACCURACY

Excessive false-positive alerts remains the key factor hurting confidence in client-screening data providers, followed by concerns about data comprehensiveness. Coverage gaps, insufficient breadth of coverage and timeliness increased in importance in 2017.

### AMONG THOSE FAMILIAR WITH CLIENT SCREENING AND NOT "EXTREMELY" OR "VERY" CONFIDENT IN DATA ACCURACY

	2015	2016	2017
Too many false-positive alerts	44%	47%	51%
Comprehensiveness of the data	32%	42%	46%
Gaps in coverage / in certain regions	27%	27%	36% ↑
Insufficient breadth of coverage	24%	19%	34% ↑
Name variations / transliterations	41%	38%	33%
Data structure	24%	24%	26%
Timeliness	17%	14%	25% ↑
Too many false-negative alerts	23%	22%	24%
Lack of data coverage definition	13%	22%	21%
Not enough crime types covered	13%	12%	16%
Integration	18%	20%	15%

## TESTING CLIENT-SCREENING DATA QUALITY

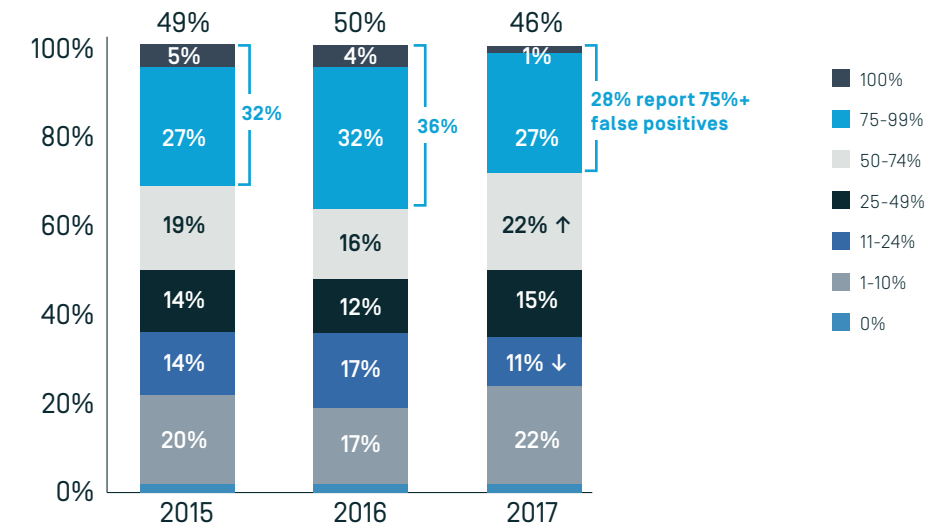
Consistent with recent years, 90% of respondents report that their companies test the quality of data from their client-screening data providers, including half who conduct quality checks monthly or more often.

### AMONG THOSE FAMILIAR WITH CLIENT SCREENING

	2015	2016	2017	
Daily	19%	22%	24%	Test monthly or more often 2015: 46% 2016: 48% 2017: 50%
Weekly	11%	12%	10%	
Monthly	16%	14%	16%	
Quarterly	12%	12%	13%	
Annually	14%	14%	12%	
Every few years	2%	1%	2%	
Only when issue suspected	16%	17%	14%	
Have never run quality checks	11%	9%	10%	2017: 90% run quality checks

## FALSE POSITIVE ALERTS IN CLIENT SCREENING

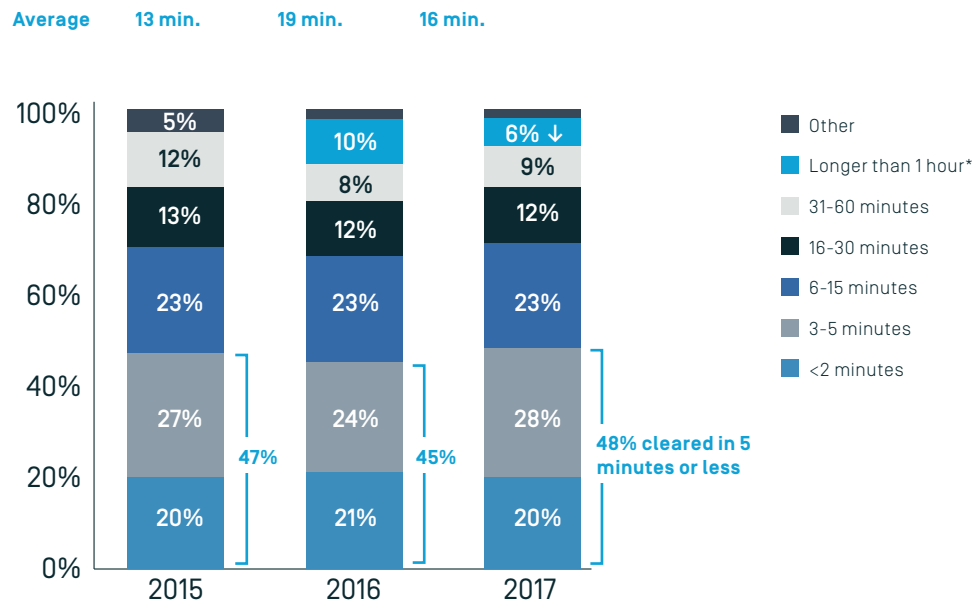
As in previous years, nearly half of the alerts generated in client screening are false positives. In 2017, almost 30% of respondents report 75% or more of their alerts are false positives.



## AVERAGE TIME TO CLEAR GENERATED ALERT

As in previous years, nearly half of respondents claim their companies typically clear a generated alert within 5 minutes or less. The average across all respondents decreases slightly due to a drop in the proportion reporting it takes “longer than 1 hour” to clear an alert.

### AMONG THOSE FAMILIAR WITH CLIENT SCREENING % OF ALERTS THAT ARE FALSE POSITIVES



\*New response option in 2016

## SECONDARY IDENTIFIERS USED IN CLIENT SCREENING

As in previous years, nearly all respondents report their organizations use secondary identifiers in the client-screening process. Date of birth, personal identification data and country of birth continue to be the most widely used secondary identifiers. The proportion using birth location information, name in original script and corporate identification data increased in 2017.

### AMONG THOSE FAMILIAR WITH CLIENT SCREENING

	2015	2016	2017
Date of birth	78%	81%	80%
Personal identification data (passport, ID card)	62%	62%	66%
Country of birth	53%	52%	59% ↑
City/state/province of birth	47%	44%	53% ↑
Entity type	49%	52%	50%
Gender	40%	44%	48%
Known location	43%	44%	44%
Name in original script	28%	33%	42% ↑
Corporate identification data	23%	26%	35% ↑
None	7%	4%	4%

2017: 96% use secondary identifiers

## REASONS TO REVIEW/CHANGE CLIENT-SCREENING TECHNOLOGY

Among respondents from companies with client-screening technology solutions in place, cost issues and excessive false alerts—positive and/or negative—remain the reasons most likely to prompt companies to review their solutions.

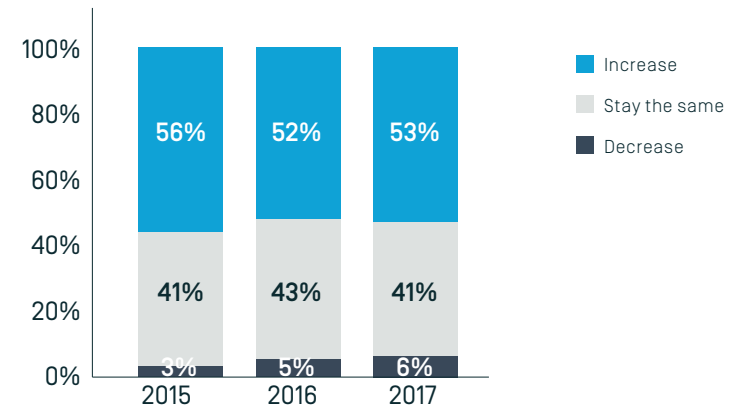
### AMONG THOSE FAMILIAR WITH CLIENT SCREENING AND HAVE SOLUTION IN PLACE

	2015	2016	2017
Cost issues	40%	46%	49%
Too many false-positive alerts	47%	45%	49%
Too many false-negative alerts	40%	43%	42%
Consolidation of software across risk areas	38%	35%	38%
Poor customer service / roadmap	33%	36%	36%
Enterprise technology consolidation	34%	35%	33%
Inability to handle non-Latin script	12%	11%	15%
Willingness to outsource			10%

## CHANGES IN COMPLIANCE OPERATIONS STAFF

Over half of respondents continue to anticipate increases in the number of operational compliance users over the next 12 months.

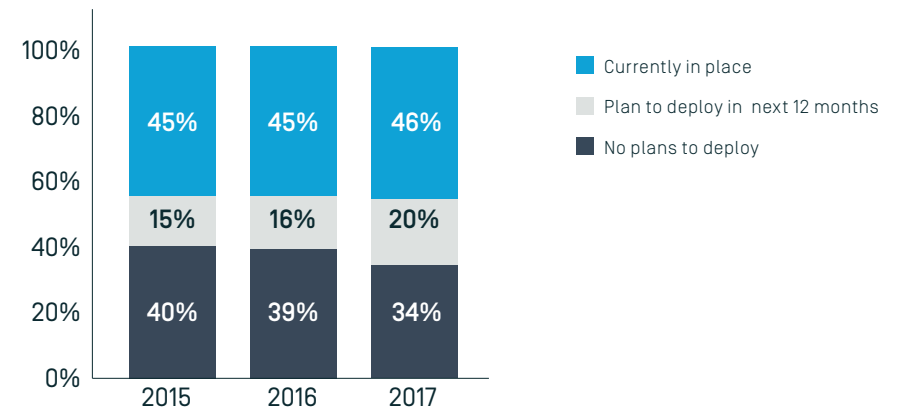
### CHANGE IN OPERATIONAL COMPLIANCE USERS IN NEXT 12 MONTHS [AMONG THOSE FAMILIAR WITH CLIENT SCREENING]



## GOVERNMENT RISK & COMPLIANCE PLATFORM DEPLOYMENT

The proportion of respondents reporting their companies have Government Risk & Compliance platforms in place is steady at about 45%. The proportion claiming their companies have no plans to deploy GRC systems is slowly decreasing.

### CHANGE IN OPERATIONAL COMPLIANCE USERS IN NEXT 12 MONTHS [AMONG THOSE FAMILIAR WITH CLIENT SCREENING]

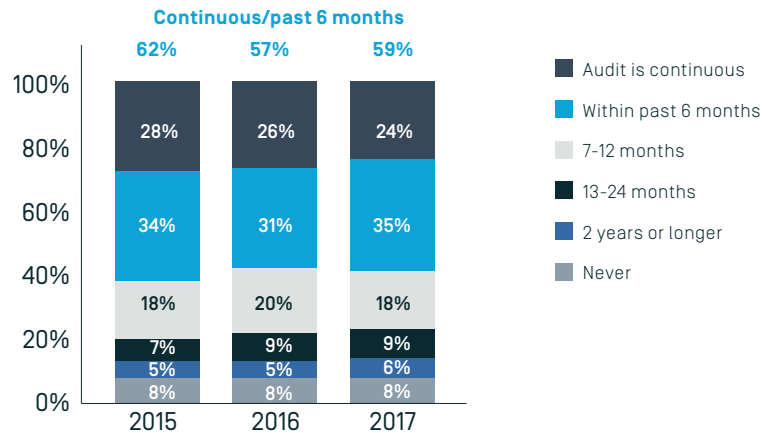


# Data Cleansing, Fraud & Sanctioned Lists

## CUSTOMER DATA AUDITS/CLEANSING

Nearly 60% of respondents report their companies have “cleansed” customer data in the past six months, including nearly one-fourth that conduct continuous audits. Results are consistent with recent years.

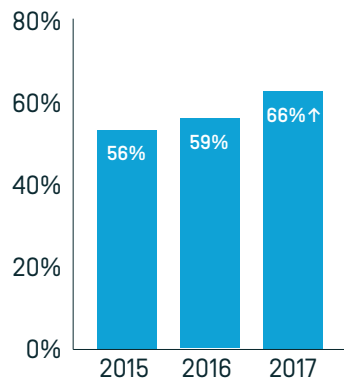
### TIME SINCE AUDITED/CLEANSED CUSTOMER DATA



## FRAUD DETECTION & PREVENTION

Over 65% of respondents work in companies in which the AML department handles fraud detection and prevention, an increase from 2016. Risk data remains the most relevant information for managing fraud, followed by crime typologies and news.

### AML DEPARTMENT HANDLES FRAUD DETECTION/PREVENTION



### TYPES OF DATA RELEVANT FOR MANAGING FRAUD

	2015	2016	2017
Risk data	83%	88%	90%
Crime typologies	77%	74%	75%
News	74%	71%	70%

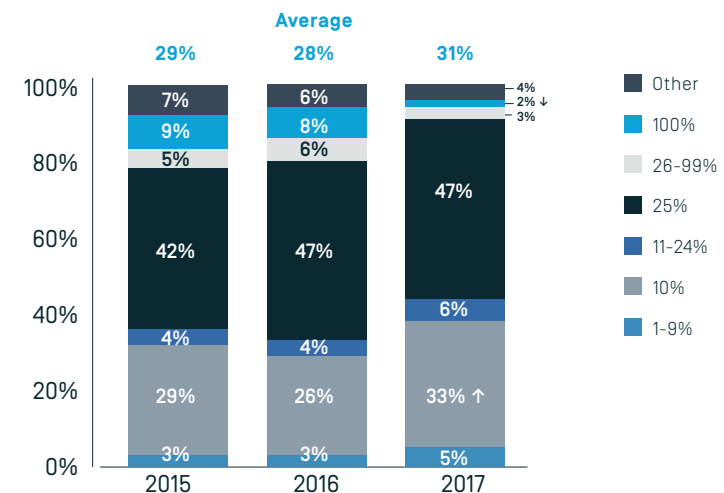
## HOW COMPANIES VERIFY BENEFICIAL OWNERSHIP

Beneficial ownership continues to be verified mainly as part of the KYC process or through internal due diligence. The proportion of respondents in companies using Country Company Registry as a verification source increases in 2017.

	2015	2016	2017
Part of KYC process	82%	83%	85%
Due diligence (internal)	69%	70%	72%
Country Company Registry	29%	31%	39% ↑
Outsourced due diligence	18%	21%	21%

## BENEFICIAL OWNERSHIP VERIFICATION REQUIRED

As in recent years, nearly half of respondents report their companies adhere to the standard of 25% beneficial ownership verification. The proportion requiring 10% verification increases in 2017 while the proportion requiring 100% verification decreases.



## CHOOSING LISTS FOR CLIENT SCREENING & PAYMENTS FILTERING

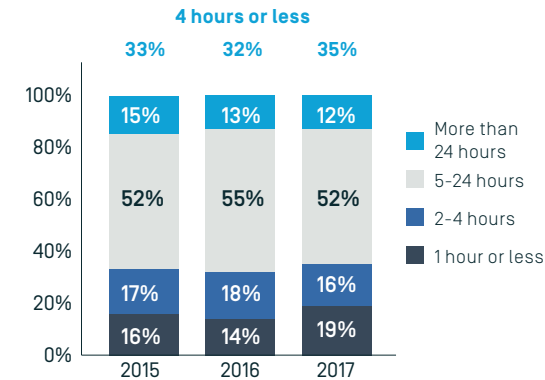
Risk-based decisions and guidance from local AML regulations continue to be the most widely used methods in choosing which sanctioned/official lists to use in client screening. These two methods both increased in 2017 while the impact of system capabilities decreased.

	2015	2016	2017
Risk-based decision by OFAC or AML officer/staff*	62%	57%	66% ↑
Guided by local AML regulation	47%	54%	63% ↑
Understanding of best practices	39%	41%	46%
System capabilities	26%	32%	25% ↓
Centralized decision	28%	30%	30%
Origin of list	23%	28%	28%
Risk of penalty	13%	17%	19%
Currency of payment	9%	12%	16%

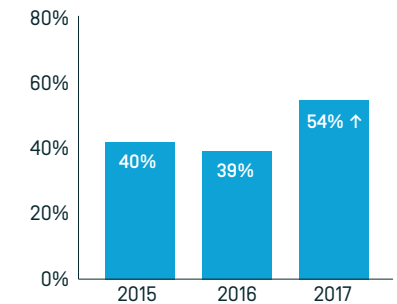
## INTERNAL UPDATES TO SANCTIONED/OFFICIAL LISTS

Nearly 90% of respondents expect internal lists to be updated within 24 hours of changes to sanctioned/official lists, including over one-third that expect updates within four hours. Nearly 55% of respondents report their companies are basing their expectations on regulator guidance in 2017, a sharp increase from 2016.

### ACCEPTABLE DELAY IN GETTING INTERNAL LISTS UPDATED



### INTERNAL EXPECTATIONS REGARDING SPEED OF LIST UPDATES ARE BASED ON REGULATOR GUIDANCE



## PREFERENCE FOR SPEED VS. ACCURACY IN LIST UPDATES

About half of respondents prefer accurate/complete list information over quicker updates. Another 30% claim that preference for quicker updates would depend on the effort required to correct any erroneous list information.

	2016	2017
More accurate and complete list information	53%	49%
Depends on the impact of additional research efforts to correct and enhance list information on the availability of list	30%	30%
Quicker updates of lists	16%	21%

## ADDITIONAL INFORMATION USED IN SANCTIONED/OFFICIAL LISTS

Additional names of people/companies/organizations, entities controlled or owned by other sanctioned entities and entities linked to sanctioned jurisdictions continue to be the most frequently used types of additional information.

The proportion of respondents reporting their companies include additional names of people/companies/organizations decreases in 2017 while the proportion adding BIC Codes and Debt and Equity Securities increases.

	2015	2016	2017
Additional names of people, companies, orgs.	77%	78%	71% ↓
Entities controlled/owned by other sanctioned entities	66%	66%	67%
Entities linked to sanctioned jurisdictions	68%	64%	66%
Vessels	44%	43%	42%
Cities & ports	33%	38%	42%
BIC codes	24%	27%	35% ↑
Debt and Equity Securities	13%	15%	23% ↑
Chinese commercial/telegraph codes	10%	14%	19%

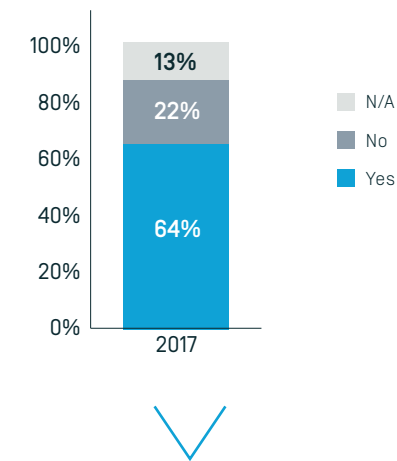
[2017 results exclude 13% that do not add any additional data to lists]

## Payments Transparency/Traceability

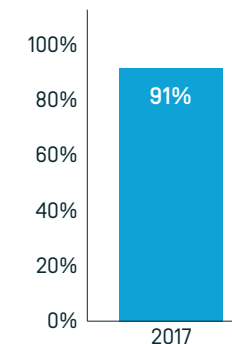
### PAYMENTS TRANSPARENCY SYSTEMS IN PLACE

Nearly 65% report their organizations have systems in place to check their own payments transparency data quality and monitor the data provided by other banks. Among those with systems in place, over 90% have a view of all the payments systems in place across groups. Automated real-time monitoring is the most used method.

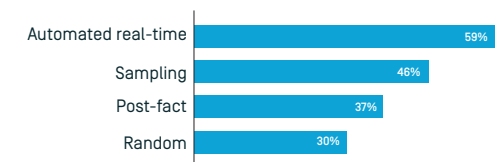
### HAVE SYSTEMS IN PLACE TO CHECK DATA QUALITY AND MONITOR DATA FROM OTHER BANKS



### HAVE VIEW OF PAYMENTS SYSTEMS IN PLACE ACROSS GROUP [AMONG THOSE WITH SYSTEMS IN PLACE]



### TYPES OF MONITORING DONE TO CHECK DATA QUALITY



## WHAT WOULD MOTIVATE ORGANIZATION TO IMPROVE DATA QUALITY

Enforcement of regulations as well as the need to improve KYC, sanctions and AML controls are the main reasons that could motivate companies without payments transparency systems in place to take actions to improve data quality.

### [AMONG THOSE THAT DO NOT HAVE PAYMENTS TRANSPARENCY SYSTEMS IN PLACE]

	2017
The need to improve KYC, sanctions and AML controls	78%
Enforcement of regulation	66%
Better management information	33%
Detection of stripping	26%
Pressure from counterparties	23%

## Peer Assessments

### BENCHMARK AND/OR PEER ASSESSMENT REPORTS

Over three-fourths of respondents represent organizations that get benchmark and/or peer comparison reports, with regulators and consultancy/advisory companies mentioned as the most frequent sources of the reports. Among those getting reports, 60% or more claim reports are available for AML transaction monitoring, KYC reviews and sanctions screening.

### SOURCE OF BENCHMARKS / PEER COMPARISON REPORTS

	2017	
Regulators	21%	76% get reports
Consultancy/Advisory companies	19%	
National financial institution associations or groups	13%	
Local financial institution associations or groups	12%	
Vendors	7%	
Other	4%	
None/Don't get benchmarks and/or peer comparison reports	24%	



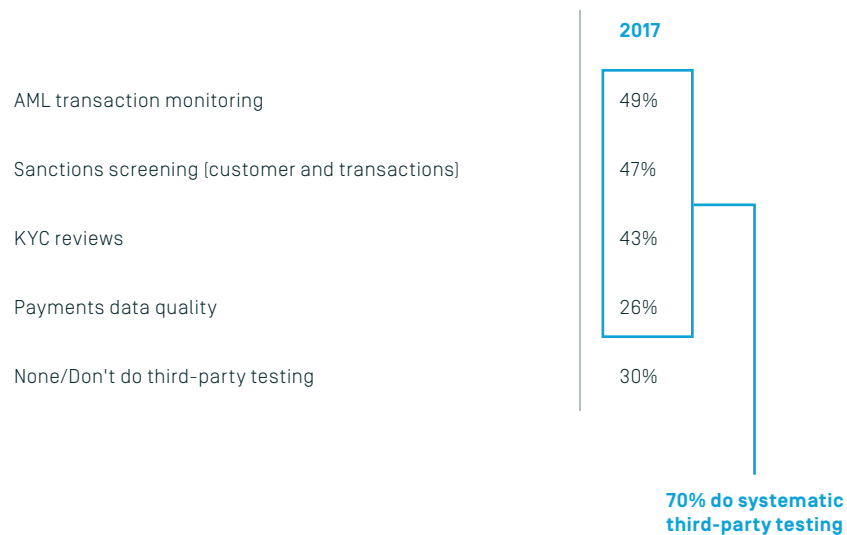
### AREAS IN WHICH REPORTS ARE AVAILABLE [AMONG THOSE GETTING BENCHMARK AND/OR PEER COMPARISON REPORTS]

	2017
AML transaction monitoring	72%
KYC reviews	61%
Sanctions screening (customer and transactions)	61%
Data quality	39%



## AREAS IN WHICH COMPANIES DO SYSTEMATIC THIRD-PARTY TESTING

Overall, 70% of respondents report their companies do some type of systematic third-party testing. Over 40% do testing related to AML transaction monitoring, sanctions screening and KYC reviews.



## Human Trafficking

### HUMAN TRAFFICKING INFORMATION AND ACTIONS

The proportion of respondents reporting their organizations have modified AML training and/or transaction monitoring to incorporate human trafficking and smuggling red flags and typologies decreases to 60% in 2017. Nearly 90% of respondents work in organizations that use information, usually multiple sources, to identify human trafficking and smuggling activities (a decrease from 2016).

#### ACTIONS TAKEN TO INCORPORATE TRAFFICKING AND SMUGGLING RED FLAGS AND TYPOLOGIES

	2016	2017
Have modified AML training	63%	57% ↓
Have modified AML transaction monitoring	58%	53%
Neither of these	31%	40% ↑

**60% did one or both ↓**

#### INFORMATION USED TO IDENTIFY HUMAN TRAFFICKING AND SMUGGLING ACTIVITIES

	2016	2017
FinCEN or other advisories	73%	58% ↓
Adverse media	65%	55% ↓
FATF reports	64%	64%
Other	6%	8%
None	5%	11% ↑

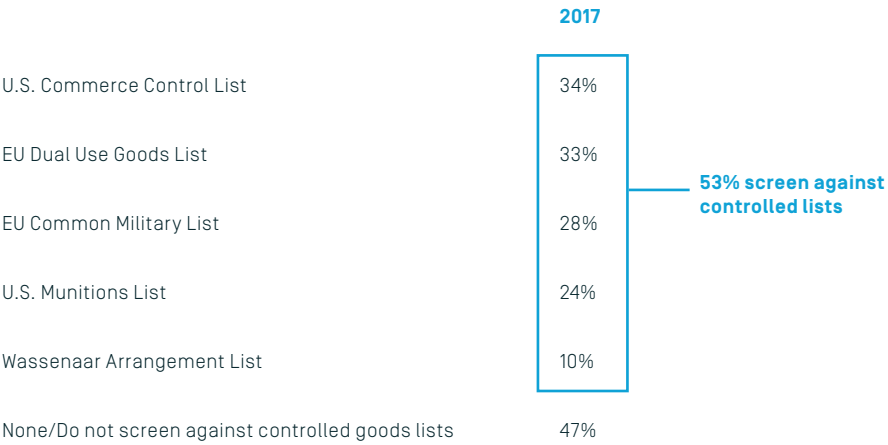
**89% use information ↓**

# Trade Compliance

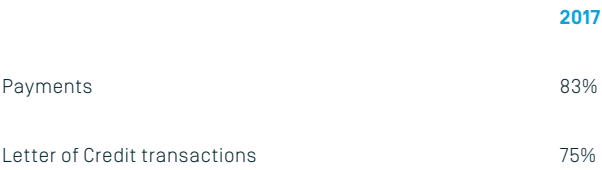
## SCREENING TRANSACTIONS AGAINST CONTROLLED GOODS LISTS

More than half of respondents report their organizations screen transactions against controlled goods lists, most often the U.S. Commerce Control List and EU Dual Use Goods List. Among those using controlled goods lists, both payments and Letter of Credit transactions are usually screened.

### CONTROLLED GOODS LISTS TRANSACTIONS SCREENED AGAINST



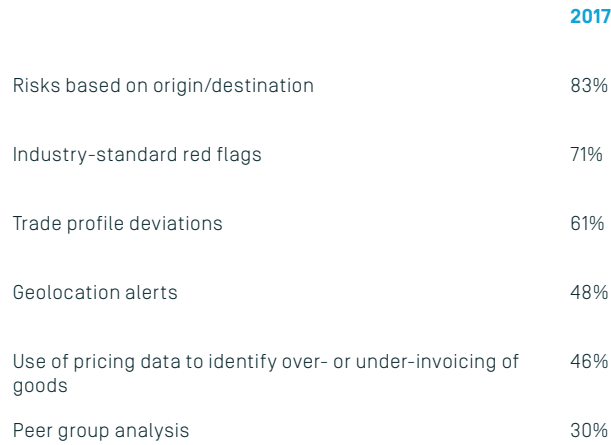
### [AMONG THOSE SCREENING AGAINST CONTROLLED GOODS LISTS] TYPES OF TRANSACTIONS SCREENED



## CONTROLS FOR DETECTING TRADE-BASED MONEY LAUNDERING

Among those screening against controlled goods lists, more than half use risk based on origin/destination, industry-standard red flags and trade profile deviations as controls to detect trade-based money laundering.

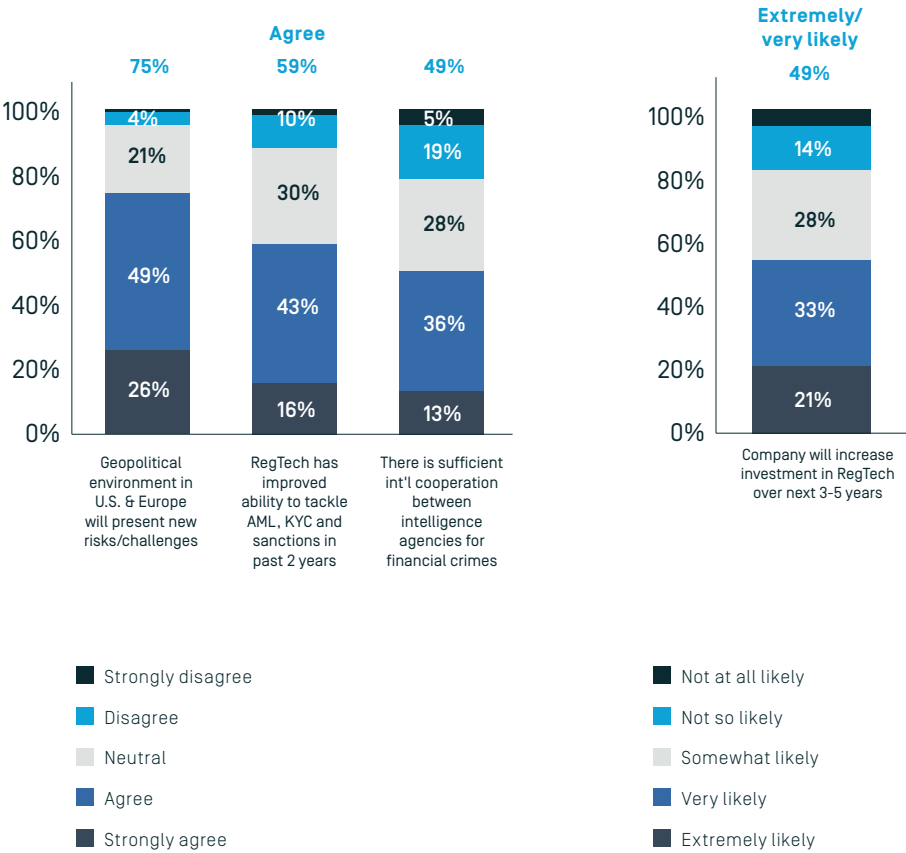
### [AMONG THOSE SCREENING AGAINST CONTROLLED GOODS LISTS]



# Regulatory Technology

## REGULATORY TECHNOLOGY IMPACT AND INVESTMENT

Three-fourths of respondents agree the geopolitical environment in the U.S. and Europe will present new risks and challenges for their organizations. Nearly 60% agree RegTech has improved their ability to handle AML, KYC and sanctions requirements. Nearly half agree international cooperation between intelligence agencies is sufficient to address financial crimes. More than half are likely to increase RegTech investments in the next 3-5 years.





## DOW JONES

Dow Jones Risk and Compliance is a global provider of risk management and regulatory compliance information, delivering targeted content to organizations around the world. Our market-leading data helps financial institutions and businesses have greater control managing Anti-Money Laundering, Anti-Bribery and Corruption, Economic Sanctions, Third Party Due Diligence and Commercial Risk operations. With a global team of expert researchers covering more than 60 languages, our risk and compliance data is information rich, accurate and timely, enabling our clients to make better quality decisions faster and with greater confidence.

For more information, visit [dowjones.com/risk](https://dowjones.com/risk)



SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance. Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way. As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

[www.swift.com/complianceservices](https://www.swift.com/complianceservices)