THETARAY

The ThetaRay U.S. Banking & Fintech Trust Report 2025

How consumers perceive financial crime risk

Table of Contents

Esteemed Compliance Leader,

In 2025, cross-border payments are instant. Criminal networks are agile. Customer expectations are unforgiving. And regulators are demanding smarter controls. Compliance leaders aren't just contending with regulatory frameworks—they're navigating a storm of complexity, speed, and reputational risk.

That's why I'm sharing with you The ThetaRay U.S. Banking & Fintech Trust Report 2025, a first-of-its-kind view into how consumers perceive financial crime risk, and how that perception translates into loyalty, advocacy, and brand value.

This report goes beyond metrics. It unpacks what customers expect after a failure—and why smart technology, not just headcount, is becoming a trust signal.

At ThetaRay, we work with institutions that understand compliance is a brand promise. This report is designed to support your mission: protecting trust, managing risk, and enabling growth in a world that moves faster than regulation.

If you're looking to reduce noise, surface real threats, and keep your institution one step ahead, this is your read.

With respect and partnership,

Yaron Hazan
Vice President of Regulatory Affairs

THETARAY

Introduction

In 2025, the stakes for financial institutions are higher than ever. Financial crime, beyond a regulatory risk, is a brand risk, a growth risk, and a customer trust risk. Institutions that allow their platforms to be exploited for money laundering, terrorist financing, drug or human trafficking face more than billion dollar fines. They face lasting reputational damage that can erode market share and customer loyalty. The ThetaRay U.S. Banking & Fintech Trust Report 2025 reveals a hard truth:

84% of consumers would switch banks if theirs were linked to financial crime.

87% would actively warn family and friends.

For leaders at banks and fintechs, this means compliance is no longer just a defensive function; it's a business-critical strategy. Basic checklists and outdated detection systems won't cut it in an era of digital and instant payments, growing regulatory scrutiny, and cross-border criminal networks.

This report offers a data-driven look at where banking and fintech brands stand today, what consumers expect, and how forward-thinking institutions are using AI-driven solutions to not just meet regulatory requirements, but protect trust, brand equity, and long-term growth.

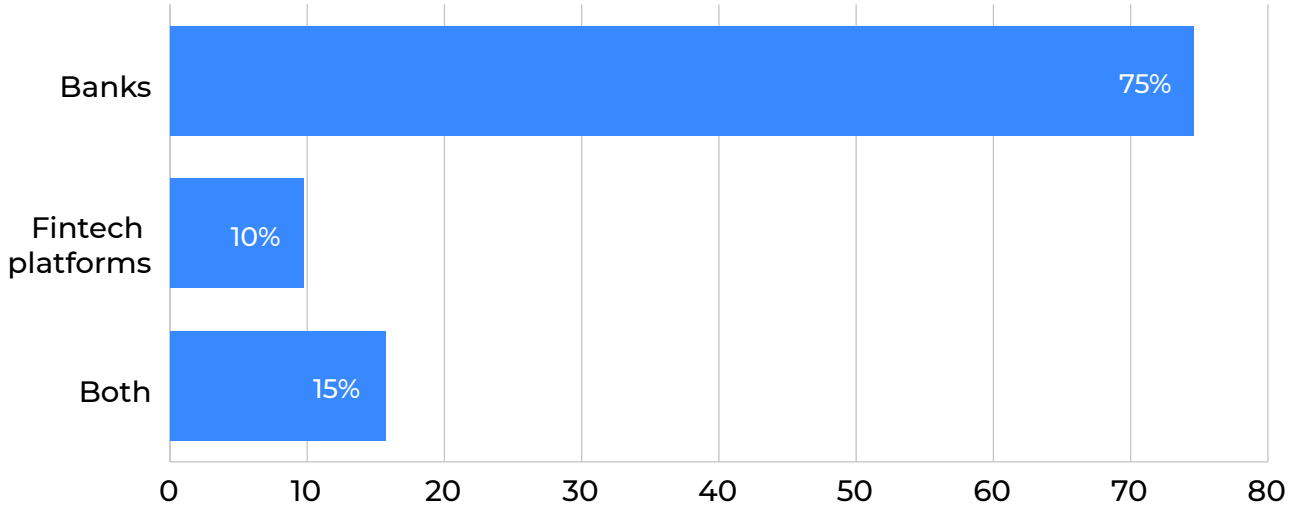
Methodology

This research report is based on a quantitative survey conducted with over 780 respondents, all of whom actively use financial services through traditional banks (75%), fintech platforms (10%) or both (15%). The survey captured user perceptions, expectations, and experiences related to financial institutions' anti-money laundering (AML) practices.

To complement the survey data, the report includes a qualitative, research-driven analysis of the current AML landscape, identifying systemic gaps, operational inefficiencies, and reputational risks faced by financial institutions. Drawing on both user insights and industry data, the report proposes a strategic path forward for institutions seeking to strengthen AML compliance while minimizing regulatory penalties and safeguarding brand equity.

This blended methodology ensures the findings are grounded in real user experience while being contextualized within the broader regulatory and operational environment.

Q1 Please select the financial institutions you use



783 answered		Counts
Banks	75%	**584**
Fintech platforms (e.g payment apps and digital wallets)	10%	**76**
Both	15%	**123**

The majority of respondents (75%) report using traditional banks as their primary financial institution, highlighting the continued dominance of established banking providers. In contrast, just under 10% rely exclusively on fintech platforms, such as payment apps and digital wallets. Interestingly, 15% of users engage with both banks and fintech solutions, suggesting a growing segment that blends legacy and modern financial services.

Banking & Fintech's Status Quo

AML's Broken Status Quo

Anti-money laundering (AML) rules in the US are nothing new, having existed since the 1970s with the adoption of the Banking Secrecy Act and evolving ever since. The 1986 U.S. Money Laundering Control Act, the 1989 formation of the Financial Action Task Force (FATF) to coordinate global efforts, its 40 recommendations from 1990, and its subsequent updates after 9/11, all show an evolving framework to combat money laundering. While the fight has always been a game of cat and mouse, with ever-evolving criminals on one side and legislation struggling to keep pace on the other, recent changes and conditions have largely upended the balance between bad actors and financial institutions. Implementing an effective first line of defense depends on the accuracy and timeliness of compliance reports, such as SARs, CTRs, and 314(a) responses, and requires a radical departure from the status quo.

Shortcomings of Legacy Rule-Based AML Approaches

What actually gets flagged using a rule-based approach isn't a victory, as the false positive rate hovers around 90%-95%[1].

In virtually no other context would such a high rate of failure be tolerated and practically speaking, it means that highly-skilled financial analysts who are overworked and in short supply, end up with even more pressure.

Though FinCen estimates it takes two hours to file a suspicious activity report (SAR), recent data suggests the true average is closer to 22 hours[2], nearly 10 times traditional estimates.

On the other side of the equation are money laundering activities that slip through undetected by rule-based approaches. It's not just financial institutions that are well aware of the rules; bad actors follow them too. From splitting up payments to be under the minimum flagging threshold and using third parties, to simply avoiding geographies or specific entities that may arouse suspicion, they know how to remain undetected. Since the rules are rigid, financial institutions overwhelmingly don't or aren't able to look for patterns beyond their proscribed limits, such as low-value payments and suspicious behaviors that in isolation look legitimate, but through context-aware advanced AI and data analysis are discovered to be hidden relationships by criminal networks operating with high sophistication and complex schemes.

Growing Sophistication of Financial Criminals

It's not that financial institutions are "standing still" when it comes to identifying bad actors while facilitating legitimate transactions; it's that bad actors have rapidly evolved in their sophistication. Layering techniques that spread payments across multiple jurisdictions and institutions are exceedingly difficult to identify. Complex corporate structures are easier to create than they were five to ten years ago, and sophisticated tools are available on the dark web for reasonable sums, complete with product reviews and even customer service. With technological advances, it has become too easy for bad actors to scale complex schemes and act globally under the radar.

A Changing World: The Rise of Digital Assets

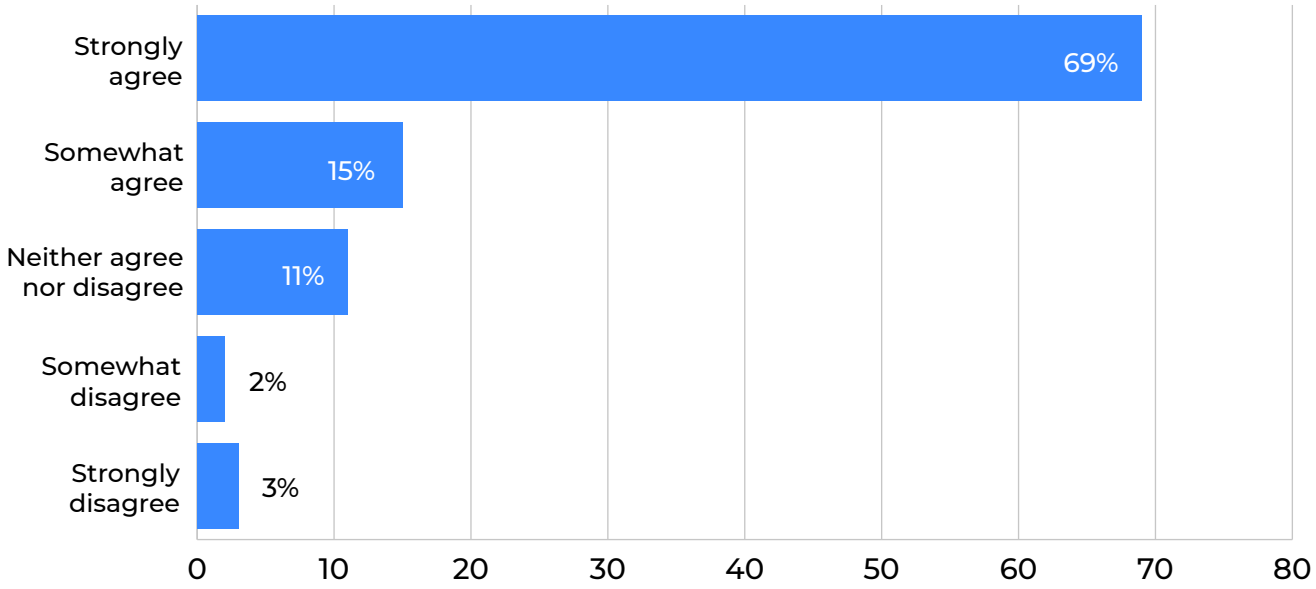
One of the most impactful changes that has taken place when it comes to money laundering is the emergence and widespread adoption of digital assets. While many of these assets, especially those built on blockchain infrastructure, tout public ledgers that make all transactions transparent and traceable, the reality is that individual identities are exceedingly easy to obscure. Some privacy-enhancing digital assets, such as those with protocols like ring signatures, stealth addresses, and zero-knowledge proofs, are intentionally designed to make tracing nearly impossible, posing significant challenges for compliance teams.

Even traditional financial institutions face exposure when digital asset transactions intersect with fiat systems. While digital assets can be transferred directly between wallets, the corresponding fiat payments are typically conducted through traditional bank transfers, making them appear indistinguishable from ordinary transactions between two parties [3]. For banks and other regulated entities, digital assets introduce new layers of complexity into Know Your Customer (KYC) and AML practices. Understanding customer behavior, the platforms they use, and the evolving regulatory landscape across jurisdictions is essential—but increasingly difficult. As regulations continue to develop unevenly across regions, effective monitoring and compliance require more agility than ever before.

1 Are You Too Negative About False Positives?, AML Datos Insights Survey, 2023. 2 FinCEN Understimates Time Required to File Suspicious Activity Report, Banking Exchange, 2024. 3 Banking, Professional Perspective- AML Issues in Cryptocurrency and Blockchain Technology, Bloomberg Law, 2021

First Look:
Consumer Insights on Impact of Compliance Issues

Q2 I would consider switching banks if mine was reported to have been involved in money laundering, terrorist financing, or human trafficking

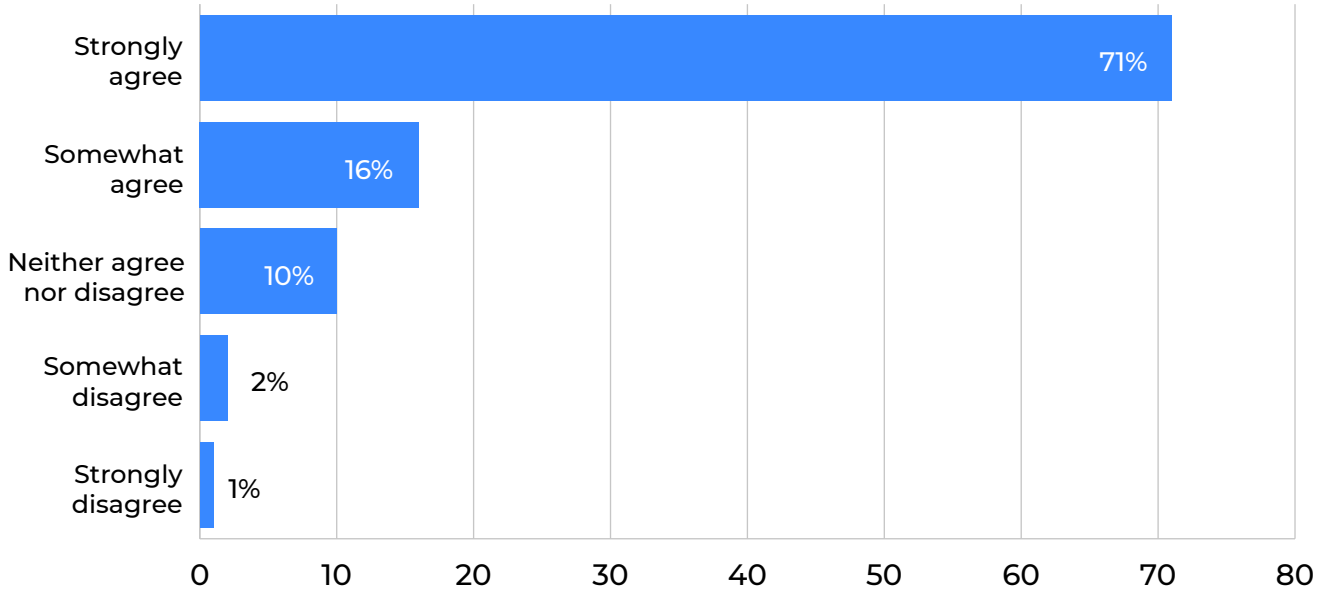


783 answered		Counts
Strongly agree	69%	**542**
Somewhat agree	15%	**116**
Neither agree nor disagree	11%	**87**
Somewhat disagree	2%	**16**
Strongly disagree	3%	**22**

A substantial majority, more than **84%**, would switch banks in response to serious ethical or legal violations, with approximately 70% saying they "strongly agree" with the statement that they would switch. This response clearly links major fines with reputational damage, highlighting that anti-money laundering risk extends far beyond the visible 'tip of the iceberg' financial penalties.

Fewer than 5% of respondents would not consider switching banks in the wake of AML violations, a clear indication of the importance of robust AML practices and proactive risk mitigation not only due to regulatory necessity, but also maintaining customer trust and loyalty.

Q3 I would actively discourage firends or family from using a bank linked to money laundering, terrorist financing.



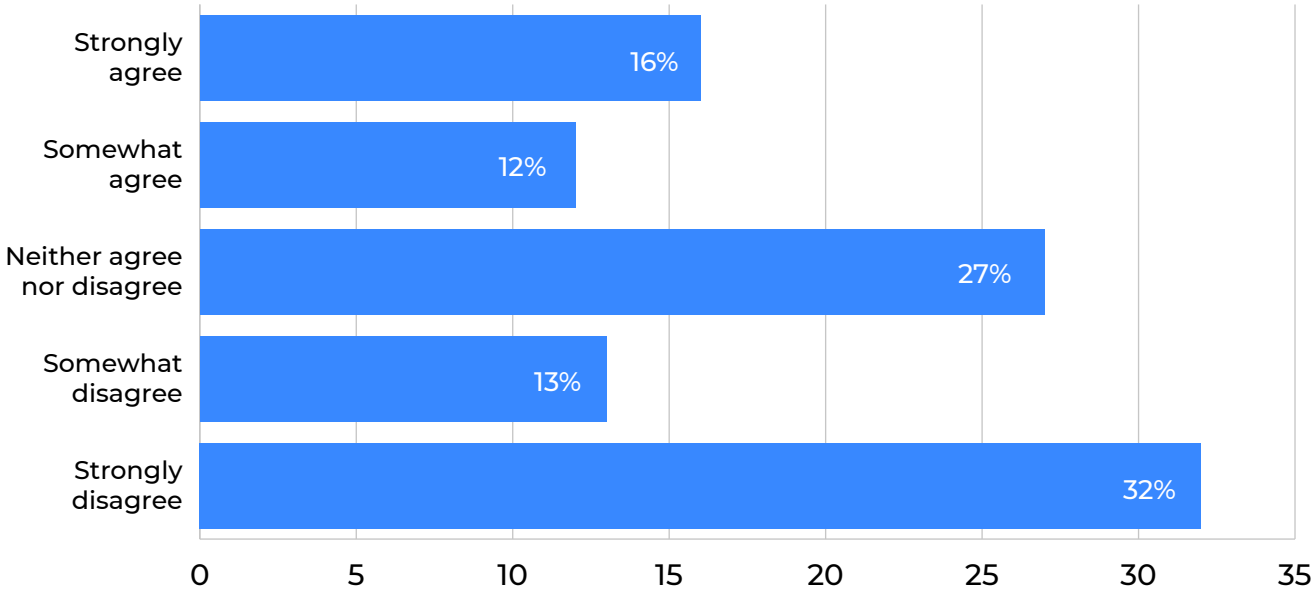
783 answered		Counts
Strongly agree	71%	**556**
Somewhat agree	16%	**124**
Neither agree nor disagree	10%	**76**
Somewhat disagree	2%	**16**
Strongly disagree	1%	**11**

The reputational damage of AML violations has a significant ripple effect for brands extending not only to the bank's customers made aware of the issues, but their social groups as well.

87% of participants would take personal action to dissuade close contacts from engaging with compromised institutions.

The data reveals a strong collective intolerance for weak AML controls and unethical banking practices, highlighting the significant reputational damage associated with AML failures.

Q4 I have been actively influenced by friends telling me about money laundering, terrorist financing or human trafficking when choosing where to bank

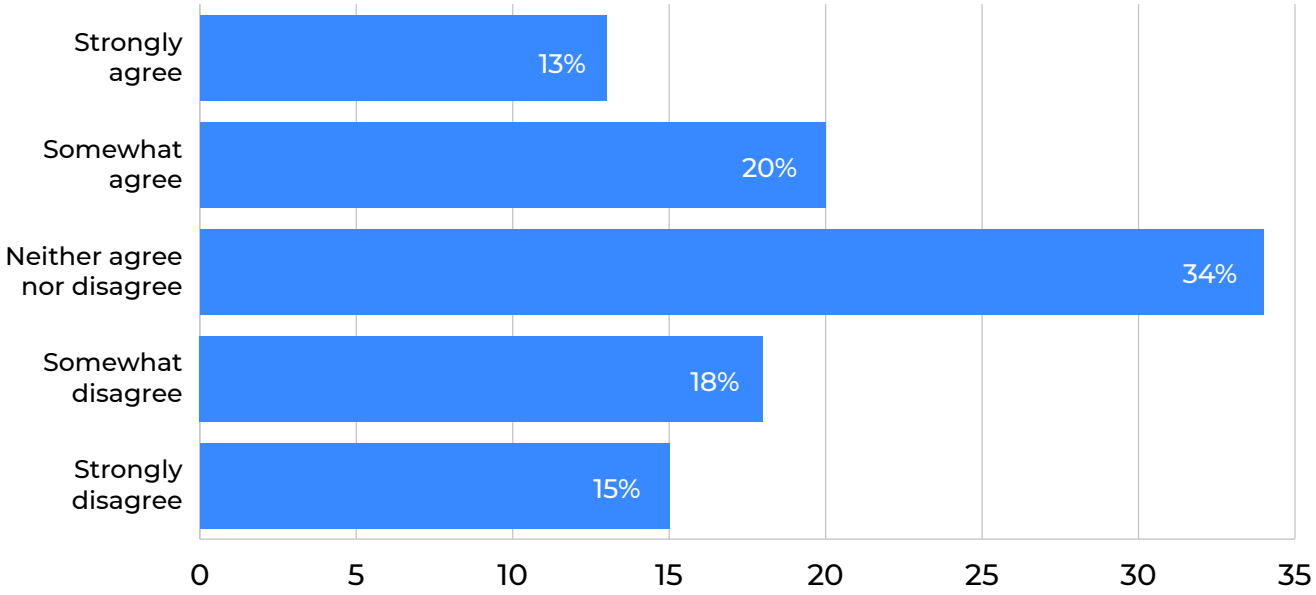


783 answered		Counts
Strongly agree	16%	**125**
Somewhat agree	12%	**91**
Neither agree nor disagree	27%	**213**
Somewhat disagree	13%	**101**
Strongly disagree	32%	**253**

While 28% of respondents acknowledge that peer opinions on illicit activity have influenced their banking decisions, a larger share (32%) strongly disagree, and another 27% remain neutral. This highlights a familiar behavioral gap: many consumers are vocal about discouraging unethical banks (as seen in Q3), yet fewer openly admit to being directly influenced by peers in their own financial choices. Even assuming respondents' self-reports are accurate, despite our natural bias toward seeing ourselves as independent decision makers, the fact remains that over a quarter say peer input does influence their decisions. For banks, this is commercially significant.

Losing the trust of even a fraction of customers due to reputational fallout could translate into tens or even hundreds of millions of dollars in lost deposits and revenue, depending on the customer scale.

Q5 I believe most large banks are equally likely to be involved in financial crimes, so fines don't influence my choice

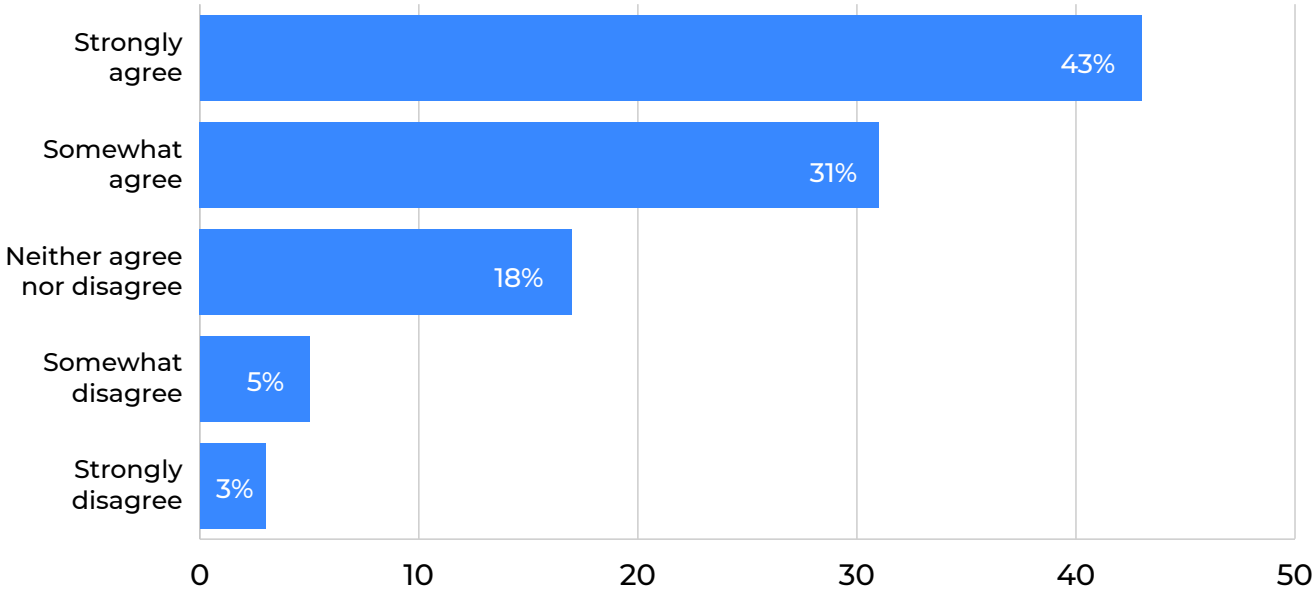


783 answered		Counts
Strongly agree	13%	**99**
Somewhat agree	20%	**160**
Neither agree nor disagree	34%	**263**
Somewhat disagree	18%	**144**
Strongly disagree	15%	**117**

Responses to this question show a divided customer base. While 34% remain neutral, 13% strongly agree and 20% somewhat agree that all large banks are equally likely to be involved in financial crimes, while 33% actively disagree. This polarization highlights two key dynamics. On the one hand, a segment of customers believes AML violations are widespread and unavoidable. On the other hand, a significant portion still perceives meaningful differences between banks and may be willing to change providers if they see a more ethical alternative. For institutions, this points to a growing need to move beyond reactive, check-the-box compliance.

Clear differentiation on financial crime compliance is increasingly becoming a competitive advantage in attracting and retaining trust-conscious customers.

Q6 When I choose a financial institution, ethics and compliance with laws are top priorities for me.

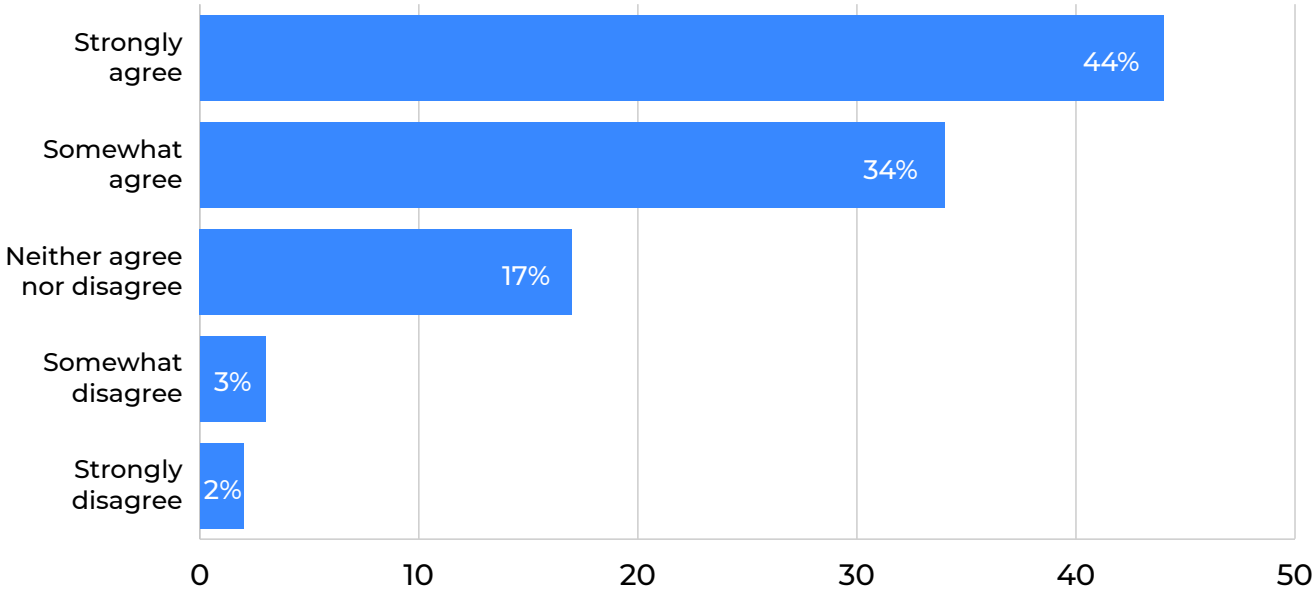


783 answered		Counts
Strongly agree	43%	**340**
Somewhat agree	31%	**244**
Neither agree nor disagree	18%	**137**
Somewhat disagree	5%	**41**
Strongly disagree	3%	**21**

A strong majority of respondents prioritize ethics and legal compliance when selecting a financial institution. With 43% strongly agreeing and 74% agreeing to some degree, it clearly indicates that ethical conduct and regulatory compliance, including robust AML frameworks, are not just background expectations but decisive factors in consumer choice. Only 8% disagreed, highlighting how small the tolerance is for perceived ethical lapses.

For financial institutions, this presents both a challenge and an opportunity: those that can credibly demonstrate leadership in integrity, transparency, and proactive compliance are far more likely to earn and retain customer trust in an increasingly scrutinized sector.

Q7 News of a major financial crime fine would lead me to research alternative banks or fintech options.

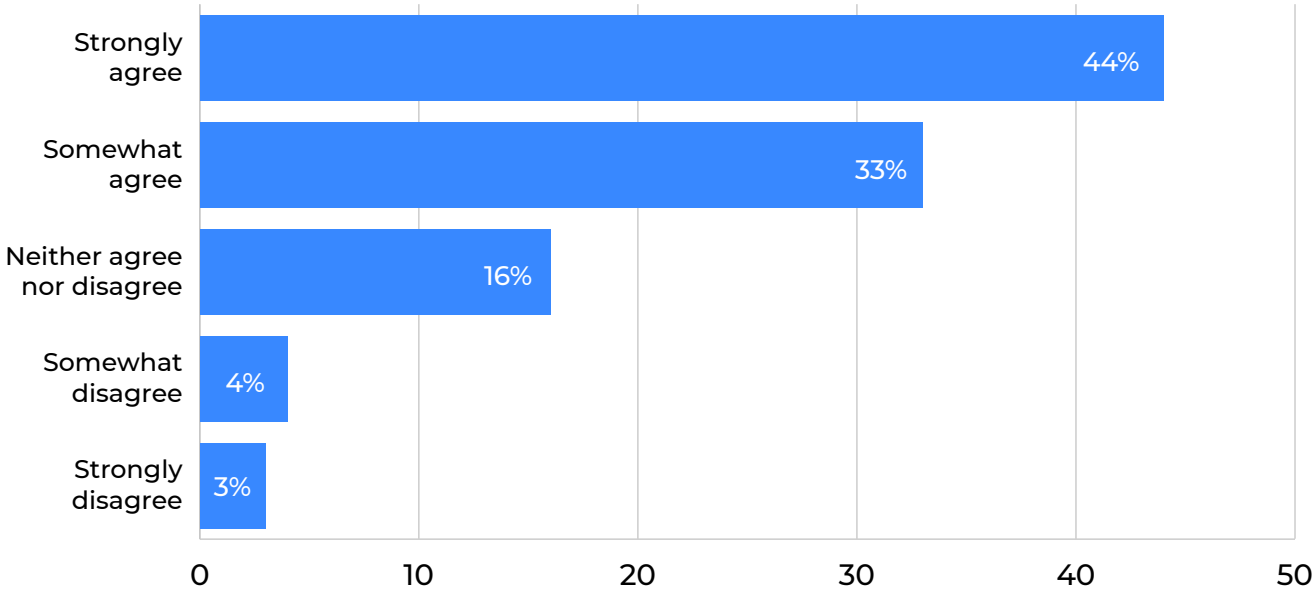


783 answered		Counts
Strongly agree	44%	**344**
Somewhat agree	34%	**264**
Neither agree nor disagree	17%	**133**
Somewhat disagree	3%	**25**
Strongly disagree	2%	**17**

Public enforcement actions for AML or financial misconduct have a direct and measurable impact on consumer behavior. An overwhelming 78% of respondents say that news of a major financial crime fine would prompt them to explore alternative banking or fintech providers. In contrast, only 5% of respondents said they would not react at all. These findings underline that a bank's compliance record is not just a regulatory requirement; it's a strategic asset tied directly to customer trust, retention and competitive positioning.

In today's digital banking environment, maintaining a strong AML and financial crime prevention track record is as much about protecting market share as it is about meeting regulatory obligations.

Q8 I believe the financial institution(s) I use are trustworthy.

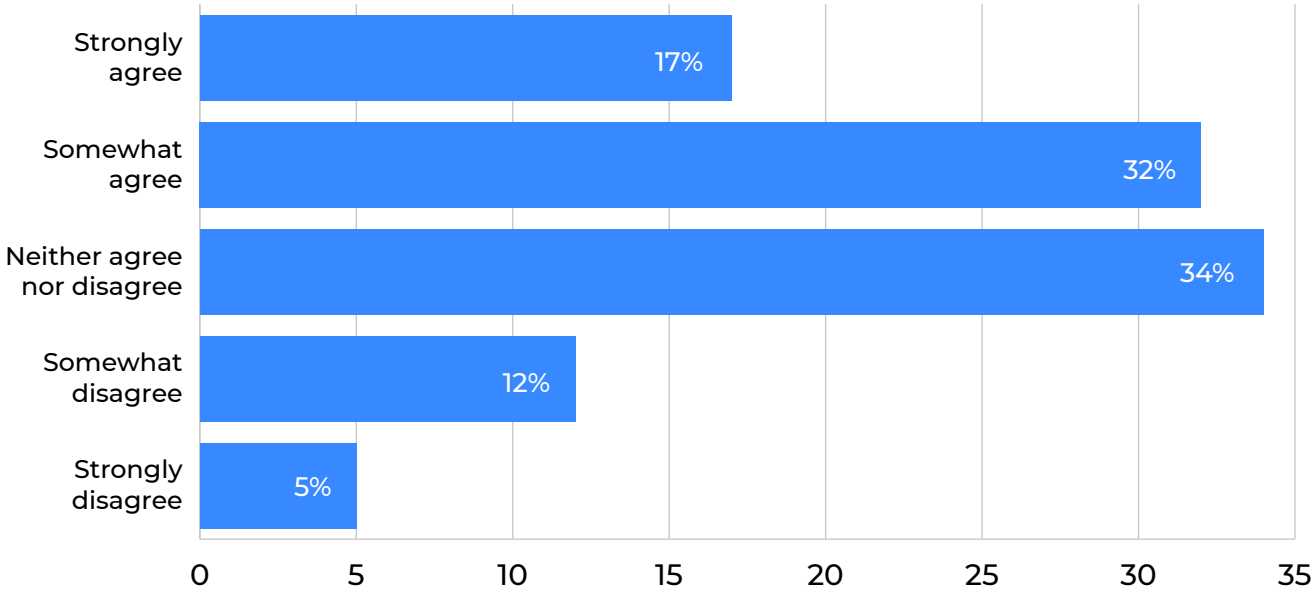


783 answered		Counts
Strongly agree	44%	**341**
Somewhat agree	33%	**258**
Neither agree nor disagree	16%	**128**
Somewhat disagree	4%	**34**
Strongly disagree	3%	**22**

Building and maintaining brand trust can be a long-term, resource-intensive endeavor for financial institutions. Encouragingly, nearly 77% of respondents express trust in their current financial providers, with 44% strongly agreeing and 33% somewhat agreeing. Another 16% remain neutral, signaling a group that could shift perceptions quickly in response to future events. While these results point to a relatively strong baseline of institutional trust, the data also reinforces that such trust is conditional and closely linked to perceptions of ethical conduct and regulatory compliance.

Maintaining consumer trust is much cheaper and easier than attempting to earn it back after bad publicity due to a major financial crime fine.

Q9 If my financial institution issued a public apology and outlined corrective actions after a fine, I would be willing to continue banking with them.

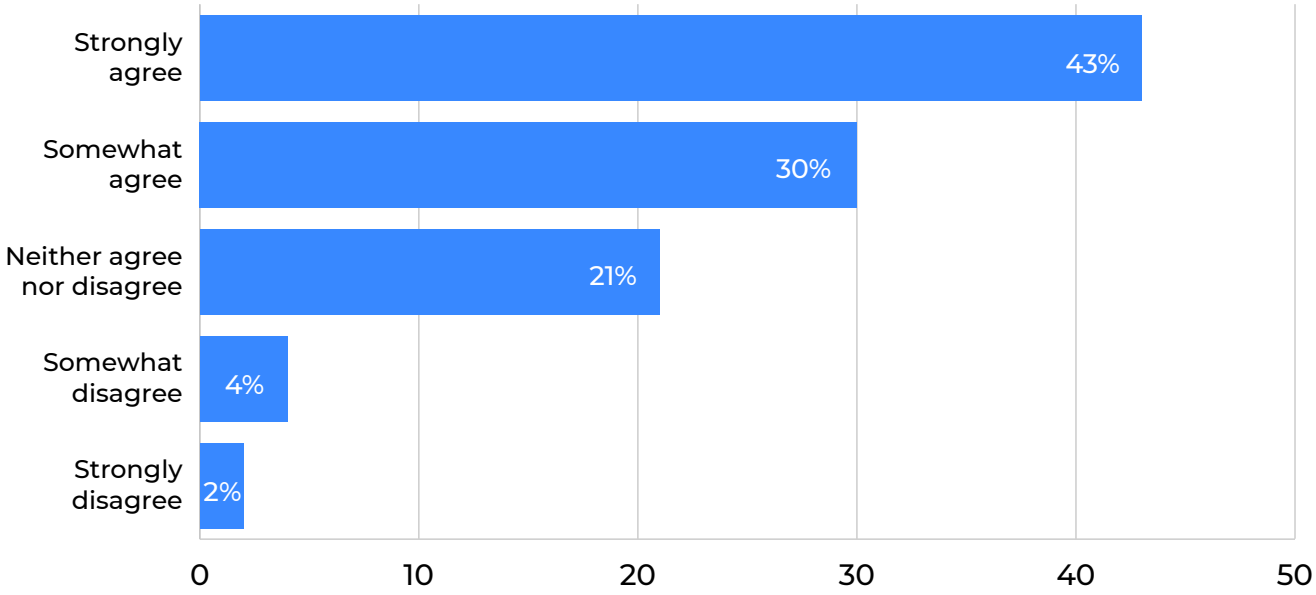


783 answered		Counts
Strongly agree	17%	**137**
Somewhat agree	32%	**247**
Neither agree nor disagree	34%	**268**
Somewhat disagree	12%	**92**
Strongly disagree	5%	**39**

While a simple apology won't resolve AML failures, transparent communication and visible corrective action can play a crucial role in managing reputational damage. Survey responses reveal cautious consumer openness to institutional accountability, with 49% of respondents saying they would continue banking with a provider that issues a public apology and outlines corrective steps following a regulatory fine. However, the remaining 51% who are neutral or actively disagree signal skepticism about the sincerity or effectiveness of such gestures.

These findings emphasize that post-incident trust recovery requires more than messaging; it hinges on credible, measurable improvements in compliance practices, particularly around AML and financial crime controls.

Q10 If my financial institution's security measures against money laundering and terrorist financing impacted my user experience (e.g., payment delays or ID verification), I would consider other options.

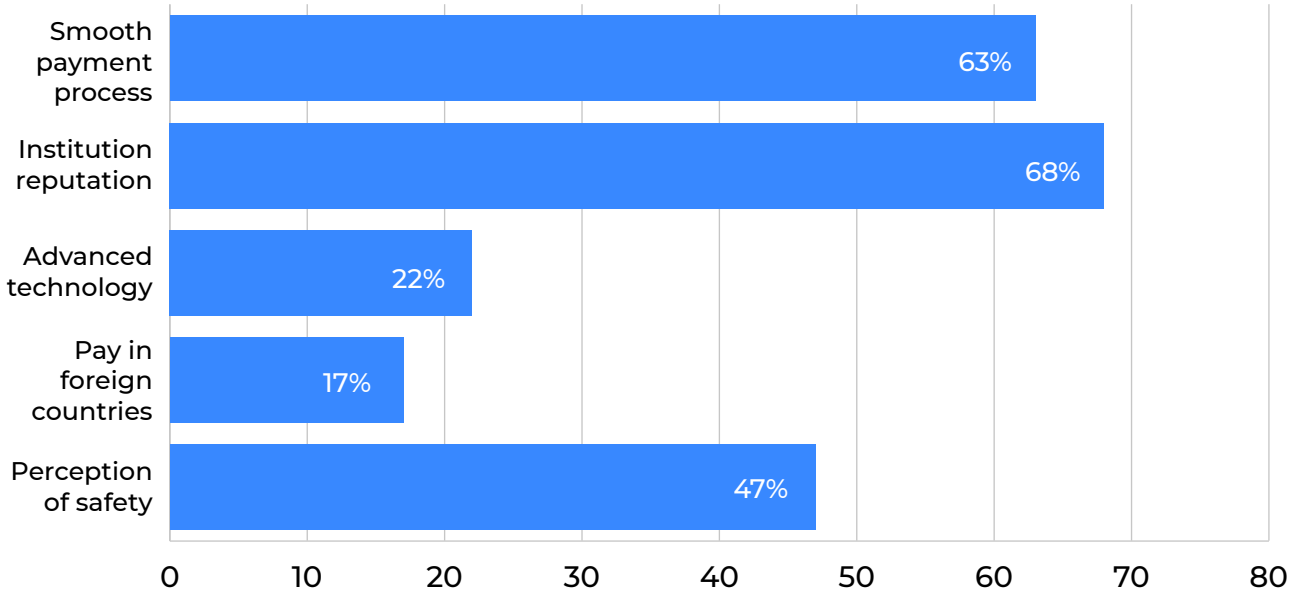


783 answered		Counts
Strongly agree	43%	**337**
Somewhat agree	30%	**238**
Neither agree nor disagree	21%	**162**
Somewhat disagree	4%	**32**
Strongly disagree	2%	**14**

While respondents expect their financial institutions to fight criminal activity they're unwilling to tolerate a compromised user experience as the price of security. An overwhelming 73% of respondents say they would consider switching providers if AML-related controls, such as payment delays or burdensome security checks, negatively affected their user experience. This highlights a dual expectation: consumers expect strong AML protections, but they also expect these measures to be seamless and minimally intrusive. For financial institutions, the challenge is clear: compliance cannot come at the expense of customer satisfaction. Institutions must strike a careful balance between compliance and convenience.

Investing in smarter, more adaptive, and frictionless AML compliance technologies will be essential to retaining trust and reducing churn.

Q11 The following strongly influence my decision to be a customer of my current financial institution: (Select all that apply)

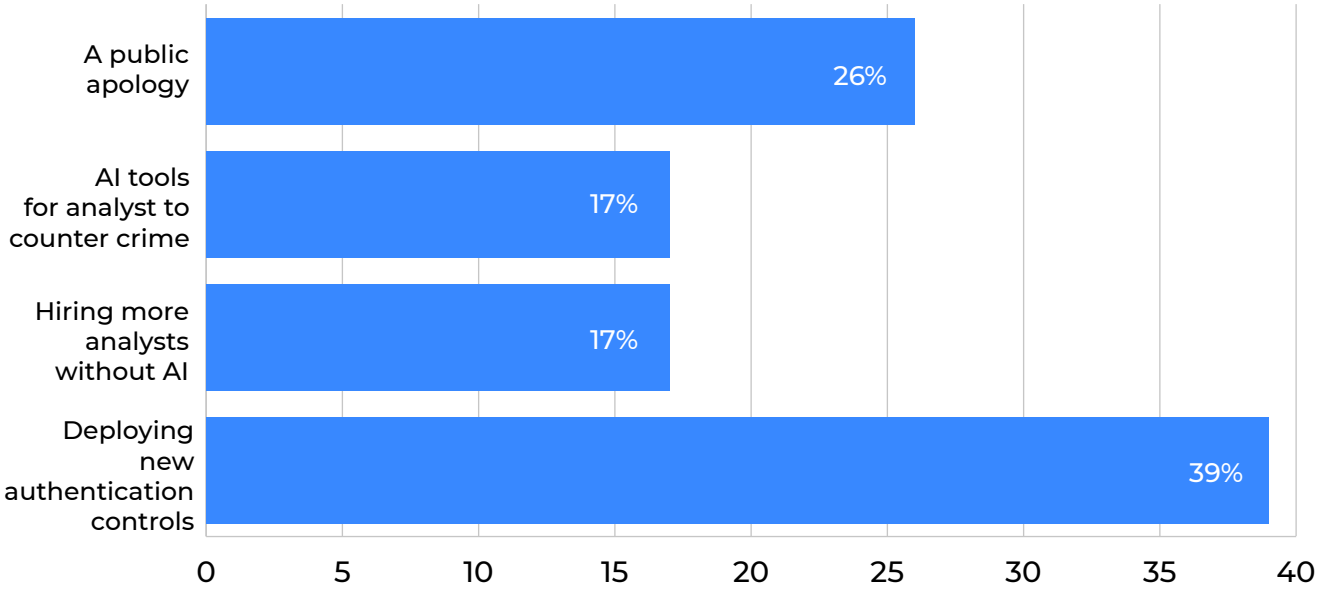


783 answered		Counts
Smooth payment process (my purchases and payments are not stopped)	63%	**494**
The financial institution's reputation	68%	**535**
Their deployment of advanced technology such as AI solutions	22%	**172**
They allow me to pay in foreign countries where others give me trouble	17%	**135**
Perception of safety	47%	**371**

Customer trust and loyalty are shaped by a combination of reputation and experience. Over 68% of respondents cite their financial institution's reputation as a key driver in their decision to remain a customer, followed closely by a smooth payment process (63%). Perception of safety also plays a significant role, influencing almost half of respondents (47%). While fewer respondents (22%) explicitly selected advanced technology such as AI is a decision driver, what many may not realize is that such technology is often the engine behind both seamless customer experiences and strong AML regulatory compliance.

AI-driven AML solutions enable financial institutions to deliver smooth, efficient operations while also enhancing their ability to detect and report financial crime, protecting both customers and institutional reputation.

Q12 Which of the following actions would most improve your trust in a financial institution fined for serious compliance failures?



783 answered		Counts
A public apology	26%	**206**
AI tools for analyst to counter crime	17%	**133**
Hiring more analysts without AI	17%	**135**
Deploying new authentication controls	39%	**309**

When asked what would most improve their trust in a financial institution fined for serious compliance failures, respondents prioritized visible action over words. While 26% said a public apology would help, far more (39%) selected the deployment of new KYC tools that improve security while reducing friction, and offer seamless customer journeys as the most trust-restoring step. Interestingly, technology-driven solutions are gaining traction: 17% said the use of AI tools for financial crime detection would increase their trust, equal to the percentage who favored simply hiring more human analysts. This signals a shift in consumer mindset: while traditional remediation efforts still matter, customers increasingly expect modern, technology-led solutions that deliver both stronger security and a better user experience.

Financial institutions that proactively invest in advanced, AI-driven compliance tools signal to customers that they are serious about preventing future failures and safeguarding customer trust.

Future Outlook:
Safeguarding Brand & Mitigating Risk

Financial institutions today face an undeniable reality: manual monitoring alone is no longer a viable defense against financial crime. As the survey shows, brand reputation, trust, ethical conduct, and visible compliance leadership are now decisive factors for consumers who expect both frictionless banking experiences and airtight compliance. They are no longer willing to overlook failures in AML and financial crime compliance and expect accountability, transparency, and meaningful action. When those expectations are mired in controversy, customers are ready to explore alternatives.

Relying solely on human analysts for financial crime detection and reporting without the support of advanced AI leads to employee burnout, customer dissatisfaction, missed criminal activity, and escalating regulatory and reputational risk.

> Institutions that can optimize compliance to offer security without sacrificing user experience and risking employee burnout, will lead the next era of financial services.

ThetaRay stands at the forefront of this transformation. Its Cognitive AI, end-to-end financial crime compliance platform empowers financial institutions to earn and maintain regulator and customer trust while enhancing their experience. By delivering high-precision transaction monitoring, watchlist screening, and dynamic customer risk assessment, ThetaRay enables financial institutions to uncover hidden threats without compromising the speed or quality of customer service.

The message is clear: compliance is a core pillar of brand integrity and customer loyalty. And with ThetaRay, forward-looking institutions are not only safeguarding against financial crime; they're future-proofing their business for a new, more vigilant era in financial services.