



2024-2025

Global Regulatory Climate

A Report on Trends for Marketplaces
and Payment Providers

TABLE OF CONTENTS

01

Introduction

02

Expanding the Scope of Responsibility for Marketplaces

- 2 How will marketplaces navigate increased accountability?
- 3 Recent and pending regulations that can significantly impact marketplaces

05

Increasing Accountability for Payment Providers

- 6 Recent and pending regulations that can significantly impact payment providers
- 8 FATF: Creating a Consistent Framework for Regulation
- 9 Key FATF Recommendations for the Payments Ecosystem

10

Regulatory Overview by Region

- 10 United States
- 12 European Union
- 13 United Kingdom
- 14 Canada
- 15 Asia-Pacific
- 19 Latin America

22

Conclusion

23

Partnering with EverC

2024-2025 Global Regulatory Climate

A Report on Trends for Marketplaces and Payment Providers

As online fraud intensifies to an unprecedented level, fueled by advancements in AI and an increasingly globalized economy, regulators are determined to find ways to keep it in check. The global regulatory push underscores a unified goal: Ensuring consumer safety.

But how can this be accomplished?

Many regulators have chosen to focus on expanding accountability all along the chain in ecommerce, pulling in players that were previously impervious to the type of scrutiny that typical financial institutions face.

Lawmakers across the globe push for expanded accountability

The rise of marketplaces and social media shopping created a gold rush that many platforms jumped on. They saw an opportunity that would boost customer stickiness and carve out a heaping slice of the online market share.

After all, 52 cents out of every dollar is spent online, and based on 2024's mashup of Black Friday/Cyber Monday, which had email inboxes overflowing with "BFCM" deals, online shopping is poised to overtake the annual ritual of standing in line in the wee hours for doorbuster deals – if it hasn't already.

Social media platforms continue to maintain the position that they bear limited (if any) responsibility for illicit activity in their shopping areas. But with 40% of Facebook's 3.07 billion monthly active users shopping on Facebook Marketplace, deniability is becoming less plausible.

Payments innovations drive the need for evolving regulation

The eager consumer uptake of Buy-now-pay-later (BNPL) and other payment innovations have also prompted the need for regulators to act, and act fast.

BNPL spending has surged, and it may put spenders at risk of overextending. The young, cash-poor "small basket" shoppers have made up the highest spending increase since BNPL became available. Without the typical consumer protection laws that govern credit cards and loans, this could have negative repercussions on a generation of consumers.

On Black Friday 2023, shoppers spent \$16.6 billion through BNPL, a 42.5% increase from Black Friday 2022 (\$11.64 billion). In the US alone, BNPL shoppers spent nearly fifty percent more on Black Friday than consumers using other payment methods.

BNPL usage did not slow down in 2024, with shoppers spending over \$991 million on Cyber Monday alone.

Regulation precedes enforcement

Lawmakers have significantly ramped up their efforts. Regulations are designed to protect consumers from today's sophisticated criminal networks, while keeping up with the innovations in purchasing and payments that consumers crave.

However, rules are not made in a vacuum – nor are they implemented in one. They are a framework created to guide behavior, and that framework includes enforcement. Over the past year, we have already seen this enforcement in the form of legal action such as changing designations, jurisdictional challenges, anti-money laundering actions, and fines.

Now, more than ever, ecommerce stakeholders must be aware of the regulations affecting them, and be prepared for increased requirements for compliance.

In the following pages, we will discuss new and ongoing regulations in the ecommerce space, highlighting potential impacts on marketplaces and payment providers, trending themes, examples of enforcement, and regional variations around the globe.

Now, more than ever, ecommerce stakeholders must be aware of the regulations affecting them, and be prepared for increased requirements for compliance.

Disclaimer: This report is not intended as legal or financial advice or counsel.

Regulatory Landscape for Marketplaces

The regulatory landscape for online marketplaces is evolving rapidly across the globe. As they redouble their efforts to hold platforms accountable for the content and commercial activities they facilitate, lawmakers are essentially reimagining and redefining the platforms' perceived position in the supply chain.

TikTok, for example, has been criticized for allowing its algorithms to promote harmful content and illicit products such as fake cosmetics, counterfeit perfumes, and unregulated prescription drugs, despite its official policy to ensure product safety and prevent user harm. This scrutiny has escalated to the point where TikTok is now facing a potential nationwide ban in the United States and Canada. Proponents of the ban have cited national security concerns over its data practices and the influence of its parent company, ByteDance, based in China.

This action represents a broader trend of lawmakers strengthening requirements for how online marketplaces and platforms handle user-generated content, user data, and commercial transactions.

The counterfeit products originating from Asian online marketplaces constitute a substantial share of the global trade in fake goods, an economic threat that cannot be ignored. And the potential impact on consumer safety underscores the problem even more. Therefore, regulators are developing creative strategies to tackle the influx of low-cost products entering domestic markets.

The groundswell of global regulation demonstrates a unified determination: holding platforms accountable for their role in digital commerce is an essential part of protecting people and the global economy.

Global regulatory overview

In June 2023, the **United States** implemented the **Integrity, Notification, and Fairness in Online Retail Marketplaces (INFORM) Consumers Act**, mandating online marketplaces to collect, verify, and disclose information about high-volume third-party sellers to curb the sale of counterfeit and stolen goods. Additionally, the Biden administration proposed **closing the de minimis exemption**, which allows imports valued under \$800 to enter duty-free—a loophole frequently exploited by platforms to bypass tariffs.

With the election of President Donald Trump in November 2024, it is anticipated that these efforts will not only continue but potentially intensify. Historically, the Trump administration adopted a stringent stance on trade, particularly concerning China, implementing substantial tariffs on Chinese imports. Recent reports suggest that the incoming administration plans to further restrict the de minimis exemption to address trade imbalances and protect domestic industries.

In a similar context, the **European Union's Digital Services Act (DSA)** enforces stringent obligations on online platforms to mitigate the dissemination of illegal goods and services. It requires platforms to implement mechanisms for users to report illicit content and mandates cooperation with "trusted flaggers." The EU is also scrutinizing Asian e-commerce platforms, considering measures like **new taxes and administrative fees** to address the surge of low-value parcels that often evade customs duties.



Enforcement Spotlight

Under the European Union's Digital Services Act (DSA), several online marketplaces were designated as Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) in 2024. These platforms, each exceeding 45 million monthly active users within the EU, are now required to comply with stricter DSA provisions, including enhanced content moderation, transparency in algorithms, and robust measures against illegal content and disinformation. Non-compliance can result in substantial fines, up to 6% of the platform's global annual revenue.

A notable case involves X (formerly Twitter), where the Commission, in December 2024, initiated formal infringement proceedings related to the platform's handling of illegal content and systemic risk assessments. This marked the first such action under the DSA, underscoring the EU's commitment to enforcing its digital regulations. The proceedings focus on X's compliance

with obligations related to countering the dissemination of illegal content, particularly in the context of events like the Hamas terrorist attacks against Israel, and the platform's risk assessment and mitigation measures. X is now required to provide detailed information and cooperate with the Commission's investigation.

Another significant example is Chinese e-commerce platform Temu. After its designation as a VLOP in May 2024, the Commission launched an investigation in October due to concerns that Temu was not adequately preventing the sale of non-compliant and potentially dangerous products, as well as issues related to addictive design and transparency in recommendation systems. Temu expressed its commitment to cooperating fully with the investigation and is considering joining a European anti-counterfeit group to bolster its compliance efforts.

In the **Asia-Pacific (APAC)** region, **China's** E-Commerce Law imposes comprehensive responsibilities on online marketplaces to prevent the sale of counterfeit goods and ensure consumer protection. Additionally, China has introduced regulations to combat unfair competition in the online sphere, targeting practices like price discrimination. In countries like **Vietnam**, authorities have mandated that online marketplace platforms register with the government or face blocking, addressing concerns over their impact on local markets and the sale of counterfeit products.

In **Latin America (LATAM)**, regulations impacting online marketplaces are evolving to regulate e-commerce growth while protecting local industries and ensuring transparent operations. In **Brazil**, a

20% tax on international purchases (up to \$50) was introduced to support local retailers against foreign e-commerce giants. **Mexico** has also tightened tax compliance for marketplace platforms, requiring VAT collection and registration with the Federal Taxpayers' Registry. In **Argentina**, the government increased duty-free import limits to \$3,000 and exempted personal use imports up to \$400 from tariffs, fostering trade liberalization.

Regulators worldwide are actively tackling the challenges brought on by the rapid expansion of e-commerce, especially on platforms with a high concentration of foreign sellers. As these frameworks continue to evolve, online platforms must adapt their operations to navigate varying regional requirements while maintaining the trust and safety of consumers.

This collective shift highlights a broader global consensus on the importance of responsible and transparent marketplace practices in fostering sustainable e-commerce growth.

Recent and pending regulations that can significantly **impact marketplaces**:

In this section, we will analyze the key recent and pending regulations that signal a surge of greater accountability for marketplaces:

European Union

The Digital Services Act (DSA) and Digital Markets Act (DMA) establish a unified regulatory framework across the EU to enhance user safety online and ensure fair competition in the digital market. The DSA focuses on protecting users' rights by imposing obligations on online intermediaries and platforms—such as social networks, content-sharing services, and online marketplaces—to manage illegal content, ensure transparency, and uphold accountability. The DMA targets "gatekeeper" platforms with significant market influence, setting rules to prevent unfair practices

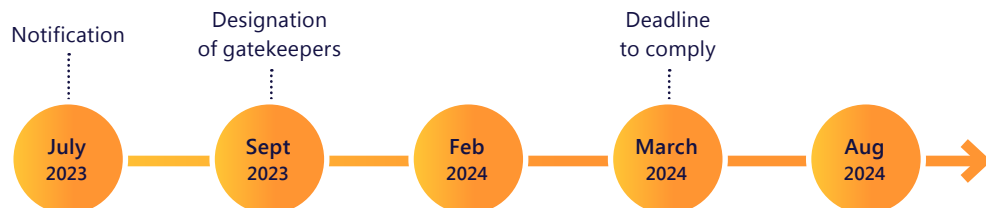
and promote a competitive digital environment. Not only do these designations impact the six gatekeepers and third-party companies using their core services, but the DMA is expected to have significant implications for the entire payments industry.

These regulations entered into force in November 2022. Rules under the DMA began applying to designated "gatekeeper" platforms starting in May 2023. Designations under the DSA began in August 2023 for Very Large Online Platforms (VLOPs) and February 2024 for all other platforms and services.

DMA Timeline

Digital Markets Act

Designation



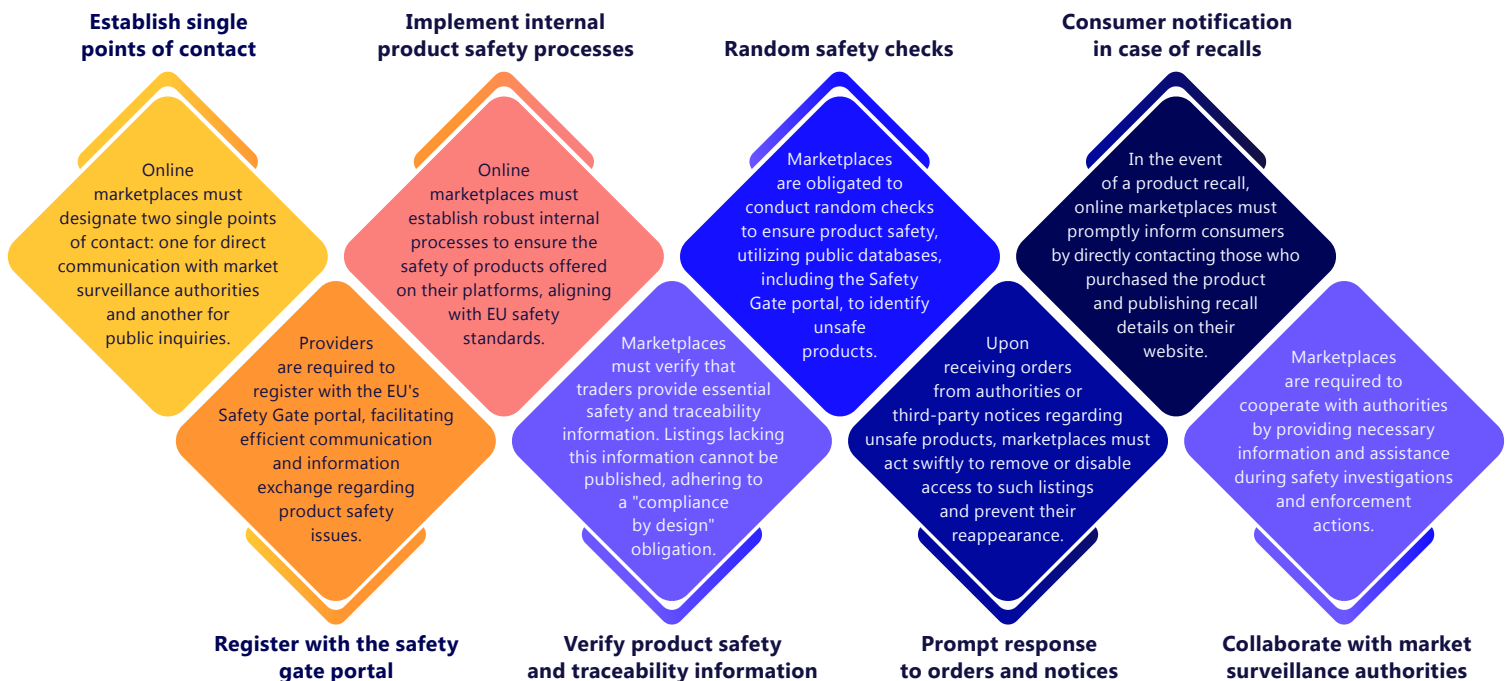
Market investigation on rebuttals

The General Product Safety Regulation (GPSR), officially known as Regulation (EU) 2023/988, modernizes the region's product safety framework to enhance consumer protection across all sales channels, including digital marketplaces. The regulation applies to all non-food consumer products in the EU market and serves as a safety net for products or risks not covered by other specific EU legislation. It imposes strict obligations

on manufacturers, importers, distributors, and online marketplaces to ensure products are safe before being marketed, requiring safety assessments, traceability, and clear consumer safety information. The GPSR holds online platforms accountable for proactively ensuring the safety of products sold through their channels.

The regulation became applicable on December 13, 2024

Key Obligations for Online Marketplaces under the GPSR



United States

The Stopping Harmful Offers on Platforms by Screening Against Fakes in E-Commerce (SHOP SAFE) Act has seen renewed legislative activity in 2023 and 2024. If enacted, the SHOP SAFE Act will establish trademark infringement liability for e-commerce platforms when a third-party seller uses a counterfeit mark in connection with the sale of goods that implicate health and safety. Online platforms will be obligated to verify sellers and their products, take action against repeat counterfeiters, and enable brands to hold them accountable for lapses in due diligence.

As of December 2024, both the Senate and House versions of the SHOP SAFE Act are under committee review. The legislative process requires approval from both chambers of Congress and the President's signature for the Act to become law.

United Kingdom

Reporting Rules for Digital Platforms mandate that UK-based online marketplaces facilitating the sale of goods or services collect and verify information about sellers and report these details to HM Revenue & Customs (HMRC). It aims to enhance tax transparency and ensure proper tax compliance within the digital economy. Platforms are required to identify reportable sellers—those residing in the UK or other participating jurisdictions who actively supply goods or services—and gather specific data, including personal and financial information.

While the regulation became effective on January 1, 2024, annual reports must be submitted to HMRC by January 31, 2025

The Online Safety Act 2023 establishes a comprehensive regulatory framework aimed at enhancing online safety by imposing duties on social media companies and search services to protect users from illegal and harmful content. This bill also affects ancillary services that support the entities mentioned, such as those facilitating fund transfers to regulated platforms and companies. This includes payment service providers, payment processors, banks, acquirers, and even SaaS-based tech platforms or fintech companies, all of which will fall within its scope and be required to comply.

In August 2024, Ofcom announced its preparedness to enforce the Online Safety Act, with content safety provisions set to come into force in March 2025



Singapore

In June 2024, Singapore introduced the **Code of Practice for E-Commerce Services** under the Online Criminal Harms Act 2023 to combat scams and malicious cyber activities on online marketplaces. The Code requires designated platforms to implement seller verification measures using government-issued records, such as SingPass, to ensure authenticity and deter fraudulent activities. Platforms must also offer payment protection mechanisms, ensuring payments are released only after goods or services are delivered. Additionally, they are required to establish proactive systems to detect and address scams, provide accessible user reporting tools, and cooperate with law enforcement by retaining and sharing relevant data.

Implementation of the Code began on June 26, 2024, with full compliance expected by December 31, 2024, and some measures like payment protection deferred to 2025

China

The Interim Provisions on Prohibiting Unfair Competition on the Internet aim to prevent and curb unfair competition in online activities. The provisions prohibit practices such as unauthorized use of business identifiers, false or misleading advertising, and the manipulation of rankings to mislead consumers. They also ban technological interference, such as traffic hijacking or malicious incompatibility, and the misuse of competitors' legally held data. Additionally, the rules address big data-enabled price discrimination, ensuring consumers are not unfairly treated based on their transaction history or profiles.

The interim provisions became effective on September 1, 2024

Regulatory Landscape for Acquiring Banks and Payment Providers

The regulatory landscape for acquiring banks and payment providers is evolving globally, with regions adopting distinct priorities to address technological advancements, financial stability, and consumer protection.

In the **United States**, changes are being driven by the implementation of rules under the **Anti-Money Laundering Act of 2020 (AML Act)**, with new proposals designed to modernize AML programs. One of the central developments in 2024 was the Financial Enforcement Network's (FinCEN) push to strengthen AML/CFT programs across financial institutions. Proposed regulations require these programs to be risk-based, tailored to each institution's unique profile, and subject to periodic review.

However, domestic politics in the US can significantly influence financial regulation and enforcement, with shifts in administration bringing changes in policy priorities. Following the November 2024 election, the incoming administration is signaling a shift towards deregulation in the financial sector. Key appointments, such as Paul Atkins as Chair of the Securities and Exchange Commission (SEC), indicate a move towards lighter regulatory oversight, particularly in sectors like cryptocurrency. According to proponents, this approach is intended to foster innovation; however, it raises concerns about regulatory ambiguities and enforcement challenges.

In contrast, the **United Kingdom and Europe** are advancing comprehensive regulation around consumer protections. The UK emphasizes operational resilience and fair competition in payment systems, while the EU is implementing the **6th Anti-Money Laundering Directive (AMLD6)** to expand liability for financial crimes and strengthen enforcement mechanisms. The directive emphasizes holding entities accountable for systemic AML

breaches and introduces harsh penalties for non-compliance. Beyond AML, initiatives like the **third Payment Services Directive (PSD3)** aim to enhance payment security and consumer rights, addressing technological advancements to protect Europe's payment system.

The **Asia-Pacific (APAC)** region is also prioritizing consumer protection and financial system integrity. **Singapore** has introduced rigorous licensing frameworks for payment providers, ensuring compliance with AML and counter-terrorism financing (CFT) standards, while **Australia** and others in the region are focusing on expanding the scope of AML compliance regimes to include more entities and ensuring consumer safety amid rapidly evolving payment ecosystems.

Meanwhile, **Latin America (LATAM)** is driving regulatory modernization to address the rapid adoption of digital payments. For example, open banking initiatives in **Brazil and Mexico** are meant to encourage innovation and promote competition among payment service providers while addressing systemic risks associated with financial inclusion efforts.

As these new rules are implemented, financial institutions must closely monitor the evolving regulatory framework, particularly as these changes will likely lead to increased compliance costs and a heightened focus on enforcement. Institutions will also need to stay engaged with card schemes given that non-compliance with card brand guidelines can result in fines or termination from accessing payment networks.

Payment providers must look to align their Acceptable Use Policies (AUPs) with card schemes rules, in addition to maintaining sufficient merchant monitoring and fraud detection mechanisms.

Recent and pending regulations that can significantly impact payment providers:

In this section, we will analyze key recent and pending regulations that payment providers should consider as they evaluate compliance processes:

United States

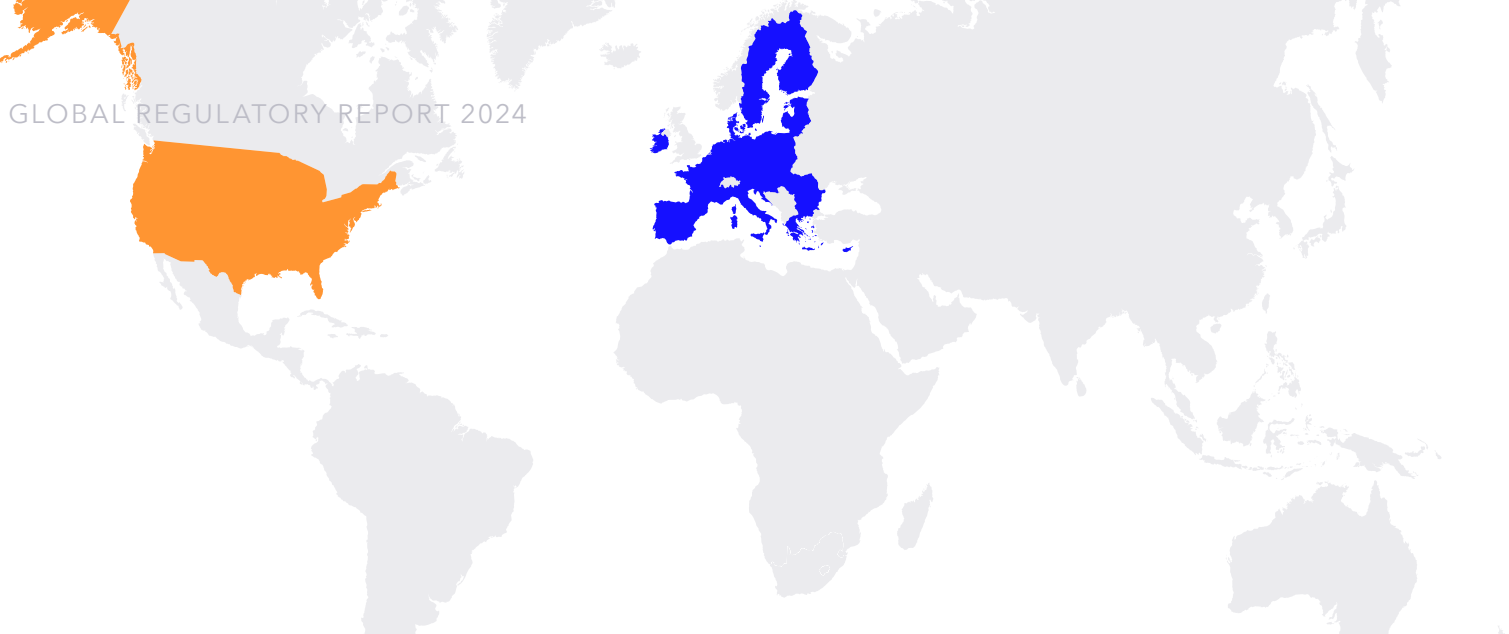
Notice of Proposed Rule Making (NPRM) to the Bank Secrecy Act, announced in June 2024, aim to enhance anti-money laundering and counter-terrorist financing (AML/CFT) programs across financial institutions, including payment providers. These proposed changes are designed to ensure that AML/CFT programs are effective, risk-based, and reasonably designed, aligning with mandates from the **Anti-Money Laundering Act of 2020**. Moreover, the proposed rules emphasize governance, requiring that AML/CFT programs be documented, approved by the board of directors, and overseen by senior management.

The public comment period for this proposed rule concluded on September 1, 2024. FinCEN has proposed that the final rule become effective six months after its issuance. Therefore, the exact compliance deadline will depend on the final rule's publication date, which has yet to be announced.

Enforcement Spotlight



In October 2024, Toronto-Dominion Bank (TD Bank) agreed to a historic settlement with US authorities, pleading guilty to conspiracy to commit money laundering and violations of the Bank Secrecy Act. **The bank was fined over \$3 billion, marking the largest penalty of its kind in U.S. history.** Investigations revealed that, between 2014 and 2023, TD Bank's inadequate anti-money laundering controls allowed criminal organizations to launder more than \$670 million through its systems. Notably, a Chinese drug trafficking group exploited these deficiencies to process over \$470 million linked to illegal drug sales. As part of the settlement, TD Bank is subject to a three-year independent monitorship, a five-year probation period, and restrictions on the growth of its US retail operations. In response, TD Bank has initiated significant reforms to its compliance programs and has made several high-profile hires to strengthen its financial crimes risk management.



On November 21, 2024, the Consumer Financial Protection Bureau (CFPB) published a **Final Rule on Federal Oversight of Popular Digital Payment Apps to Protect Personal Data, Reduce Fraud, and Stop Illegal “Debanking”**. This regulation targets Big Tech and peer-to-peer platforms processing over 50 million transactions annually, aiming to ensure compliance with federal consumer financial laws. The CFPB's oversight will focus on protecting personal data, reducing fraud, and preventing illegal account closures, commonly referred to as “debanking.” Given the evolving market for digital currencies, the CFPB also limited the rule's scope to count only transactions conducted in U.S. dollars.

The final rule will become effective 30 days after publication in the Federal Register

Final Rule 1033 of the Dodd-Frank Act mandates that financial institutions, including banks and credit unions, provide consumers and their authorized third parties with secure and reliable access to personal financial data upon request. This data includes information about transactions, costs, charges and usage related to consumer deposit accounts, credit cards and payment services. It also establishes obligations for third parties accessing consumer data, emphasizing privacy protections, and encourages the development of fair and inclusive industry standards.

Compliance deadlines are staggered based on institution size, with the largest institutions required to comply by April 1, 2026, and smaller institutions by April 1, 2030.

The Secure and Fair Enforcement Regulation (SAFE) Banking Act is a proposed US federal law aimed at protecting financial institutions that provide services to state-legal cannabis businesses from federal penalties. If enacted, the law would allow legal cannabis businesses to access traditional banking services, reducing reliance on cash transactions and enhancing financial transparency and security within the industry.

As of December 2024, the Act has progressed through several legislative stages but has not yet been enacted into law. The bill requires approval from both the Senate and the House, followed by the President's signature.

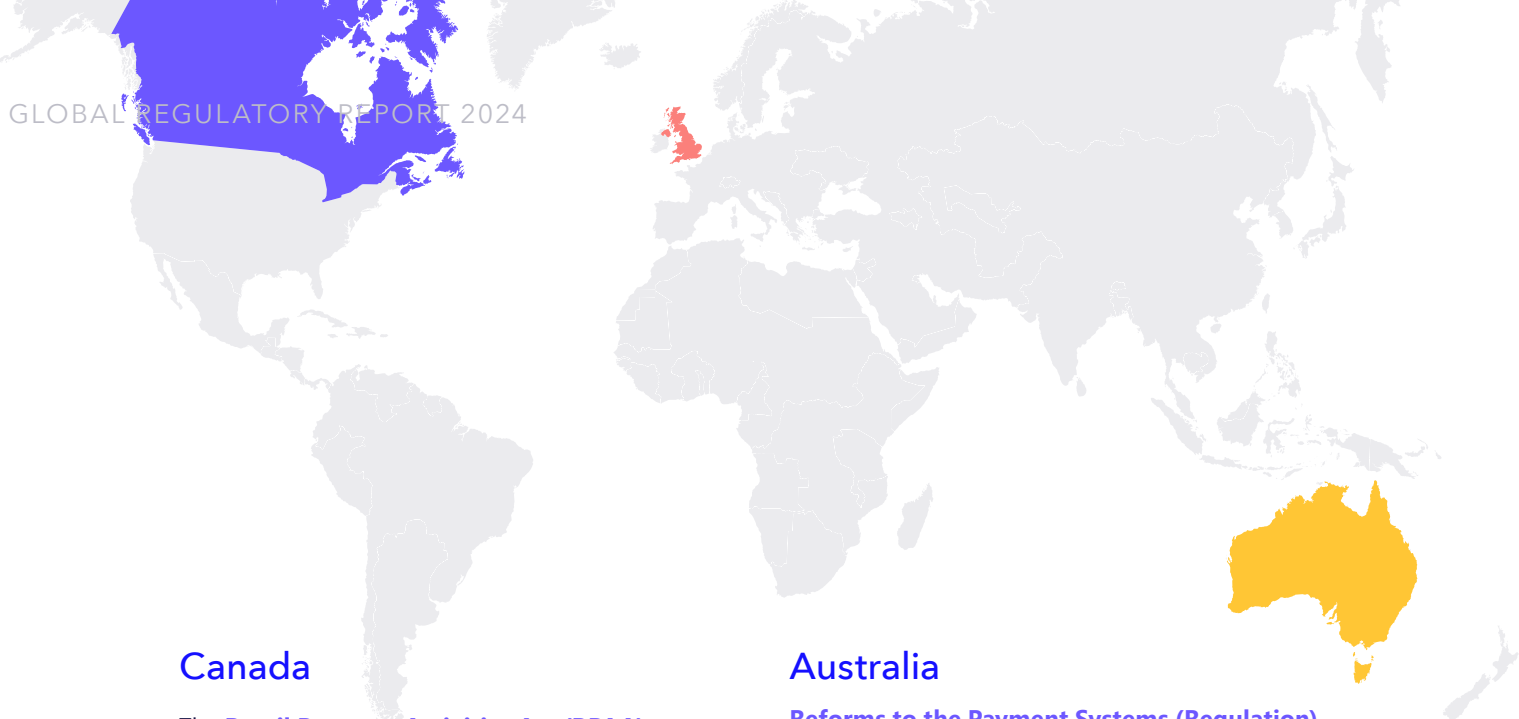
European Union

The **Anti-Money Laundering and Anti-Terrorism Financing Package** represents a significant overhaul of the EU's regulatory framework to combat financial crimes more effectively. Key measures include the establishment of the Anti-Money Laundering Authority (AMLA), a new EU-level body based in Frankfurt, to directly supervise high-risk financial entities and coordinate national authorities. The package introduces a new AML regulation with standardized rules and enhanced transparency requirements for beneficial ownership. **The 6th AML Directive (6AMLD)** updates national obligations, focusing on supervision and financial intelligence units, and updates the list of predicate offenses – a crime which is a component of a larger crime generating monetary proceeds.

The new “AML Package” was formally adopted by the Council of the EU in May 2024

22 predicate offenses listed under 6AMLD

Participation in an organized criminal group and racketeering	Corruption
Trafficking in human beings and migrant smuggling	Murder and grievous bodily injury
Terrorism	Kidnapping, illegal restraint and hostage-taking
Cybercrime	Robbery or theft
Illicit trafficking in narcotic drugs and psychotropic substances	Smuggling
Illicit arms trafficking	Tax crimes relating to direct and indirect taxes
Illicit trafficking in stolen and other goods	Extortion
Environmental crime	Sexual exploitation
Fraud	Piracy
Counterfeiting of currency	Insider trading and market manipulation
Counterfeiting and pirating of products	Forgery



Canada

The **Retail Payment Activities Act (RPAA)** establishes a comprehensive supervisory framework for retail payment activities in Canada, mandating that payment service providers (PSPs)—including card networks, payment processors, and digital wallet operators—implement robust measures to manage operational risks, respond to incidents, and safeguard end-user funds. Under this framework, the Bank of Canada is designated as the supervisory authority responsible for overseeing PSPs to ensure the safety, reliability, and resilience of electronic payment functions. These requirements aim to bolster consumer confidence, promote innovation, and maintain the integrity of Canada's payment ecosystem.

Effective November 16, 2024, PSPs must register with the Bank of Canada before conducting retail payment activities. From September 8, 2025, PSPs are required to submit annual reports to the Bank of Canada, detailing compliance with operational risk management, incident response, and fund safeguarding frameworks.

Australia

Reforms to the Payment Systems (Regulation) Act 1998 (PSRA) were announced by the Reserve Bank of Australia (RBA) in February 2024. Key recommendations include expanding the definitions of "payment system" and "participant" to encompass all entities involved in enabling payments, including fintech firms and digital wallet providers. The proposed reforms also grant government powers to address significant payment issues outside the jurisdiction of existing regulatory bodies and introduce court-enforceable undertakings to strengthen enforcement.

Specific compliance deadlines have not been established, as the legislative process is ongoing.

United Kingdom

The Digital Markets, Competition and Consumers Act 2024 is a landmark legislation to enhance competition and strengthen consumer protections, particularly among Payment Service Providers (PSPs) and other digital payment platforms with strategic market status (SMS). The Act also introduces significant reforms to consumer protection laws, including bans on subscription traps, fake reviews, and drip pricing, aiming to eliminate unfair practices and promote transparency.

The legislation is scheduled to come into force on January 1, 2025

Global Regulatory Authorities

The regulatory environment surrounding the payments industry is extensive and involves numerous agencies, legal frameworks, and standards both at the national and international levels. Whether you are looking for anti-money laundering and counter-terror financing compliance, consumer protection, data security, or other payments standards, these organizations and their frameworks are critical to understanding the global regulatory landscape.

Financial Action Task Force (FATF)

FATF sets international standards for combating money laundering, terrorist financing, and other financial crimes. The FATF Recommendations are a series of internationally endorsed global standards that serve to increase transparency and empower countries to act against illicit use of their financial

systems. There are 40 AML + 9 CTF Recommendations in total, and countries are rated according to their level of compliance with each one. The full document can be downloaded [here](#).

Additionally, the organization undertakes country-specific assessments of anti-money laundering and counter-terrorist financing regulatory compliance and effectiveness. These Mutual Evaluation Reports (MERs) are conducted in partnership with FATF member countries.

Naturally, the FATF expects regulators to closely align their own AML-CTF regimes with the recommendations. While regulations may vary by jurisdiction, the themes in these guidelines echo throughout regional frameworks: risk assessment, privacy, security, and due diligence

7 Key FATF Recommendations for the Payments Ecosystem

- 1 Recommendation 1**
Assessing risk and applying a risk-based approach
 Countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.
- 2 Recommendation 10**
Customer Due Diligence (CDD)
 Financial institutions should be required to conduct due diligence on new customers, as well as existing customers, on a periodic or situational basis.
- 3 Recommendation 12**
PEPs
 Financial institutions should be required to have measures in place to determine if customers or beneficial owners are Politically Exposed Persons (PEP) and apply risk management accordingly.
- 4 Recommendation 15**
New Technologies
 Financial institutions should be required to adequately assess and mitigate the potential risk in implementing new technologies.
- 5 Recommendation 17**
Reliance on third parties
 Financial institutions can rely on a third party to conduct CDD, provided that the criteria are met. (Note: risk still resides with the institution itself, not the third party.)
- 6 Recommendation 19**
Higher-risk countries
 Financial institutions should be required to perform enhanced due diligence that is effective and proportional to the risks of business relationships with entities and individuals in higher-risk countries.
- 7 Recommendation 20-21**
Reporting suspicious transactions
 Financial institutions that have reasonable suspicion of illicit activity should be required to report it to the financial intelligence unit (FIU) promptly, confidentially, and without notifying the suspicious entity.

Europol

WHO	WHY DO WE CARE?
<p>United Nations Office on Drugs and Crime (UNODC)</p> <p>The UNODC provides insights into regulations that combat financial crimes globally, including those affecting the payments industry.</p>	<ul style="list-style-type: none"> Regulatory Frameworks for Financial Crimes: Reports and analysis on international regulations against money laundering and terrorist financing that impact payments services.
<p>Global: Bank for International Settlements (BIS)</p> <p>BIS is an international financial institution that provides regulatory frameworks and guidelines for financial institutions, including those within the payments industry. Their Committee on Payments and Market Infrastructures (CPMI) offers global standards for payment systems.</p>	<ul style="list-style-type: none"> Principles for Financial Market Infrastructures (PFMI): Global standards for payment systems, securities settlement systems, and central counterparties. Reports on Cross-Border Payments: Analyzes trends and offers regulatory guidance for managing cross-border payment systems and financial transactions.
<p>International Organization for Standardization (ISO)</p> <p>ISO sets international standards for various industries, including financial services and payments. Their widely adopted ISO 20022 standard governs messaging and communication protocols for payments systems.</p>	<ul style="list-style-type: none"> ISO 20022 Standard: A globally accepted messaging standard used in payment transactions, which ensures compliance, transparency, and efficiency across borders. SWIFT Integration: The ISO 20022 standard is being adopted for cross-border payments via the SWIFT network.
<p>Global: Payment Card Industry Data Security Standard (PCI DSS)</p> <p>PCI DSS is a set of security standards designed by a global forum to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.</p>	<ul style="list-style-type: none"> PCI DSS Compliance Guidelines: The core standards for protecting cardholder data, which is critical for payment service providers, fintech, and banks. Self-Assessment Questionnaire (SAQ): A tool that payment providers can use to ensure compliance with PCI DSS.

Regulatory Overview by Topic

Artificial Intelligence

Artificial Intelligence (AI) refers to the simulation of human intelligence by machines, enabling them to perform tasks such as learning, reasoning, and problem-solving. AI has transformed the world, reshaping industries by streamlining operations, driving innovation, and improving decision-making. In e-commerce, AI has revolutionized how businesses and consumers interact, enhancing customer experiences, optimizing operations, and enabling highly personalized and efficient services.

However, there is a dark side to AI. Malicious actors are leveraging the technology to commit crimes at a speed and scale never seen before. AI-powered crimes exploit the interconnected nature of the digital world and allow criminals to operate across borders with anonymity and precision, targeting individuals, businesses, and financial institutions. Transnational crime groups, for instance, are using generative AI to enhance operations related to money laundering, smuggling, and even activities that fuel armed conflicts.

This showcases the urgent need for robust safeguards against AI-enabled threats, and regulators are responding.

Lawmakers around the world are increasingly focused on addressing the rapid evolution of AI technologies, with many enacting or considering laws to govern their use. In September 2024, the world's first AI Treaty was signed by the European

Union, United States, United Kingdom, and several other nations. This groundbreaking agreement seeks to ensure that AI systems are developed and deployed in ways that respect human rights, uphold democratic values, and adhere to the rule of law. In the United States alone, nearly 700 AI-related bills have been introduced in state legislatures, covering topics ranging from safety standards to deepfake regulation.

The payments industry faces significant challenges from this increasing regulatory pressure, which requires robust safeguards against criminal activities are now more widespread through AI-driven fraud tools. For example, the US Department of Justice (DOJ) updated its Evaluation of Corporate Compliance Programs guidance in September 2024. The revised guidance advises prosecutors to assess whether companies have implemented effective governance and risk management strategies for AI and other new technologies.

In the risk management context, leveraging AI to enhance systems and processes can be highly effective. For instance, the US Treasury Department's "technology and data-driven" approach enabled the prevention and recovery of over \$4 billion in fraud and improper payments in 2024, a significant increase from \$652 million in 2023.

Below, we highlight a few recent and pending regulations related to AI:

European Union

The Artificial Intelligence Act (AI Act), establishes a comprehensive legal framework for the development and deployment of artificial intelligence across the EU. It classifies AI systems into three risk levels: unacceptable risk, high risk, and limited or minimal risk. Applications in the unacceptable risk category, such as those that manipulate behavior or compromise fundamental rights, are prohibited. The Act seeks to ensure AI is developed and used responsibly, balancing innovation with the protection of fundamental rights and societal values, and it sets a global benchmark for AI governance. The AI Act entered into force on August 1, 2024.

As of September 25, 2024, over 100 companies have signed the EU Artificial Intelligence (AI) Pact and its voluntary pledges. These signatories include a mix of multinational corporations and European small and medium enterprises (SMEs) from various sectors such as IT, telecommunications, healthcare, banking, automotive, and aeronautics. The Pact promotes voluntary industry commitments to begin adhering to the principles of the AI Act ahead of its formal implementation, while fostering collaboration between the EU AI Office and key stakeholders, including industry, civil society, and academia.

United Kingdom

The United Kingdom is actively developing a regulatory framework for AI that balances innovation with safety and ethical considerations. In March 2023, the government released a white

paper titled "**A Pro-Innovation Approach to AI Regulation,**" outlining five key principles: safety, security, and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress. By May 2024, key regulators, including the Information Commissioner's Office (ICO) and the Competition and Markets Authority (CMA), had published their strategic approaches to AI, aligning with the government's framework.

Canada

Canada is working on finalizing AI regulation to ensure its responsible development and deployment. In June 2022, the government introduced the **Artificial Intelligence and Data Act (AIDA)** as part of Bill C-27, the Digital Charter Implementation Act, 2022. The legislation adopts a risk-based approach, focusing on "high-impact" AI systems to balance technological advancement with public safety and ethical standards. In November 2023, the Minister of Innovation, Science and Industry proposed substantial amendments to address concerns regarding the initial draft. These amendments have not yet been officially adopted.

China

China's Cyberspace Administration, in collaboration with six other government agencies, issued the **Interim Measures for the Management of Generative Artificial Intelligence Services.** These measures establish a regulatory framework for generative AI services accessible to the Chinese public, emphasizing adherence to existing laws, respect for social ethics, and the protection of national security and public interests. These measures took effect on August 15, 2023.

Cryptocurrency

Cryptocurrencies are digital tokens that operate on decentralized blockchain technology, enabling secure, peer-to-peer transactions without the need for intermediaries such as banks. Since its inception, cryptocurrency has revolutionized finance, providing new opportunities for investment, payment solutions, and global commerce.

However, the anonymity enabled by cryptocurrency makes it particularly appealing to criminals, as they

bypass the identification requirements typically associated with conventional payment systems. Additionally, the volatility of crypto markets and high-profile collapses of exchanges have highlighted risks to consumer protection and financial stability. This, combined with fragmented regulatory oversight, has also made crypto a useful tool to launder money, evade taxes, and conduct a myriad of other financial crimes.

How cryptocurrency crime funds are acquired and reused

1. CRYPTOCURRENCY EXCHANGES

- a. Criminals deliberately seek out exchanges that have weak or no KYC requirements.
- b. These exchanges are used in jurisdictions that may not be regarded as high-risk for crypto asset laundering.
- c. Criminals present fraudulent documents, or use money mules, at legitimate exchanges to add credence to their operations.

2. PEER-TO-PEER PLATFORMS

Depending on their jurisdiction, some P2P platforms may not be subject to KYC regulations, allowing criminals to engage in illicit transactions without the involvement of centralized intermediaries

3. DECENTRALIZED EXCHANGE SERVICES (DEX)

Criminals can bypass compliance controls by making real-time crypto asset exchanges using a DEX, which lacks a central administrator with oversight of user accounts, records, or identities.

4. CRYPTOCURRENCY ATMS

Largely unregulated across the globe, criminals use these to convert large amounts of cash into cryptocurrencies, or vice versa.

5. ONLINE CASINO AND GAMING SERVICES

Criminals exploit lacking KYC protocols of many sites to swap cryptocurrencies for credits or in-game currencies to clean their illicit funds.

6. PRE-PAID CARDS

Criminals load pre-paid cards with illicitly procured cryptocurrency to make purchases or swap it with fiat currency.

7. MIXING SERVICES AND PRIVACY WALLETS

Allows criminals to operate with increased anonymity as these services break the chain of end-to-end traceability around cryptocurrency transactions.

8. TOKENS

Criminals can purchase tokens without providing identifying information and clean illicit funds.

The Markets in Crypto Assets (MiCA)

Implementation timeline Last updated: 9 June 2023



In response, lawmakers worldwide are implementing diverse approaches to regulating the rapidly evolving crypto landscape. Some, like the European Union with its MiCA framework and the United Arab Emirates through its VARA licensing, have established comprehensive regulations to foster innovation while ensuring compliance. Others, such as China, have taken a restrictive stance by banning crypto activities entirely, while countries like India impose heavy taxes and consider stricter oversight. Innovation-driven jurisdictions like Singapore and certain US states aim to attract blockchain companies with crypto-friendly policies, though federal oversight in the US remains fragmented. Collectively, these approaches illustrate the global effort to balance fostering innovation, protecting consumers, and addressing financial crime within the crypto sector.

Below, we highlight a few recent and pending regulations in the crypto space:

European Union

Introduced by the European Union, the **Markets in Crypto Assets (MiCA) framework** provides a comprehensive regulatory structure for crypto-assets not already governed by existing financial legislation. It established clear rules for the issuance, trading, and management of crypto-assets and their underlying assets. MiCA also introduced requirements for crypto service providers, including the implementation of Know Your Customer (KYC) protocols, sanctions screening, and measures to ensure consumer protection and market integrity.

In December 2024, the European Banking Authority (EBA) launched a public consultation on draft Regulatory Technical Standards (RTS) to clarify when crypto-asset service providers (CASPs) should appoint a central contact point. This aims to enhance AML/CFT oversight for CASPs operating in EU member states. The consultation runs until February 4, 2025.

United Arab Emirates

The **Virtual Assets and Related Activities Regulations 2023** establish a comprehensive framework for regulating virtual assets in Dubai, excluding the Dubai International Financial Centre (DIFC). Overseen by the Virtual Assets Regulatory Authority (VARA), the regulations require entities involved in virtual asset activities, such as issuance, exchange, custody, and broker-dealer services, to obtain proper licensing and comply with operational, governance, and financial standards. The framework includes strict anti-money laundering (AML) and counter-terrorism financing (CFT) obligations, requiring customer due diligence and reporting processes.

*In September 2024, the Securities and Commodities Authority (SCA) and Dubai's VARA **announced** enhancements to its crypto regulatory framework by establishing a unified supervisory authority over virtual asset firms, streamlining licensing requirements across the country. Under this framework, virtual asset service providers (VASPs) operating in Dubai can now obtain a license from VARA, which automatically grants recognition from the SCA, eliminating the need for multiple approvals across different jurisdictions.*

South Korea

The **Virtual Asset User Protection Act** established the country's first comprehensive regulatory framework for cryptocurrency to safeguard consumer assets and maintain market integrity. The act requires VASPs to segregate customer funds from corporate assets, mandating that a substantial portion of customer deposits be stored in cold wallets to reduce the risk of hacking. VASPs are also required to secure insurance or reserves to compensate users in case of theft or cyberattacks. Furthermore, the law empowers financial regulators to supervise and enforce compliance, introducing severe penalties for violations, including imprisonment and significant fines for illicit activities. The Act became effective from July 19, 2024.

*Starting in the second half of 2025, regulators will implement **new regulations** targeting cross-border cryptocurrency transactions. These measures are designed to address the growing prevalence of foreign exchange-related crimes, particularly those involving virtual assets. Under the framework, businesses engaged in cross-border crypto transactions will be required to register with regulatory authorities and provide detailed monthly transaction reports to the Bank of Korea.*

Canada

In August 2024, authorities initiated **a consultation** on proposed amendments to the Pillar 3 Disclosure Guidelines for banks, focusing on the public disclosure of crypto-asset exposures. This initiative aims to enhance compliance and transparency among cryptocurrency service providers, including brokers and exchanges. The proposed guidelines are scheduled to take effect in the first quarter of 2026, with OSFI planning to begin publishing relevant crypto-asset regulatory data for all institutions around the same time.

India

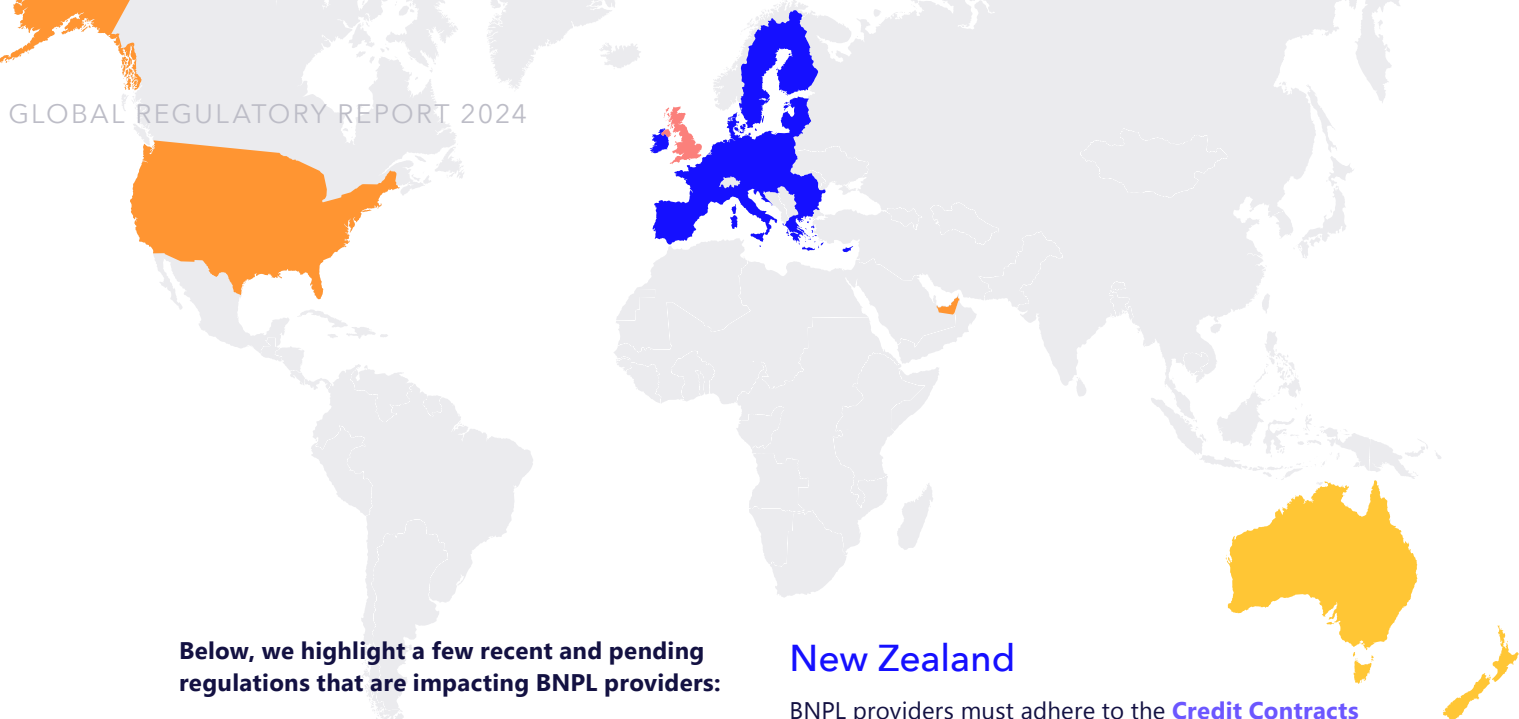
The Securities and Exchange Board of India (SEBI) **proposed** a multi-regulatory framework for overseeing cryptocurrency trading in May 2024, diverging from the Reserve Bank of India's (RBI) longstanding preference for a complete ban on private digital currencies. SEBI's approach suggests that various regulators should supervise crypto-related activities within their respective domains, aiming to provide comprehensive oversight and enhance investor protection. This proposal has been met with optimism within India's crypto community, with experts highlighting that such a framework could foster a more transparent and secure environment for digital asset transactions.

Buy Now Pay Later

Buy Now, Pay Later (BNPL) services have surged in popularity in recent years, offering consumers the ability to purchase goods or services upfront while spreading the cost into interest-free installment payments. However, these services have come under increasing regulatory scrutiny due to their operation outside traditional credit frameworks, raising significant concerns about oversight, compliance, and consumer protection.

Furthermore, the rapid adoption of BNPL services has highlighted the risk of over-indebtedness, particularly among younger users, as many providers lack transparency in disclosing fees, terms, and penalties, leaving consumers vulnerable to hidden costs. Lawmakers are also troubled by insufficient credit checks and due diligence, which further expose users to financial overextension. These shortcomings not only threaten individual financial stability but also present systemic risks, as BNPL providers often operate across jurisdictions with inconsistent regulatory oversight.

Authorities have already begun cracking down on the way BNPL providers do business. For example, **Sweden's** financial supervisory authority recently issued Klarna Bank AB a formal remark and an administrative fine of 500 million SEK (approximately \$50 million USD) for significant deficiencies in its anti-money laundering (AML) compliance. The investigation revealed that Klarna's general risk assessment lacked evaluations of how its products and services could be exploited for money laundering or terrorist financing, and the bank failed to implement adequate procedures and guidelines for customer due diligence.



Below, we highlight a few recent and pending regulations that are impacting BNPL providers:

United States

The Consumer Financial Protection Bureau (CFPB) issued an **interpretive rule** clarifying that lenders providing digital user accounts to access credit, including BNPL services, are considered "card issuers" under Regulation Z of the Truth in Lending Act. This designation subjects these lenders to specific requirements, such as issuing periodic statements and adhering to billing dispute protocols, thereby extending consumer protections traditionally associated with credit cards to BNPL products. This became effective in July 2024, but the CFPB has **stated** that it is giving BNPL providers time to comply with consumer protection rules.

Australia

Regulators are **proposing changes** to the National Consumer Credit Protection Act 2009 (NCCP Act) to bring BNPL providers under its scope. This could require BNPL providers to perform credit assessments, obtain credit licenses, and ensure compliance with responsible lending standards.

European Union

The European Union adopted **Directive (EU) 2023/2225** in October 2023, revising its Consumer Credit Directive to enhance consumer protection in the evolving credit market. This updated legislation expands its scope to include BNPL services, which were previously unregulated under the former directive. Member States are mandated to transpose the directive into national law by November 20, 2025, with full application required by November 20, 2026.

New Zealand

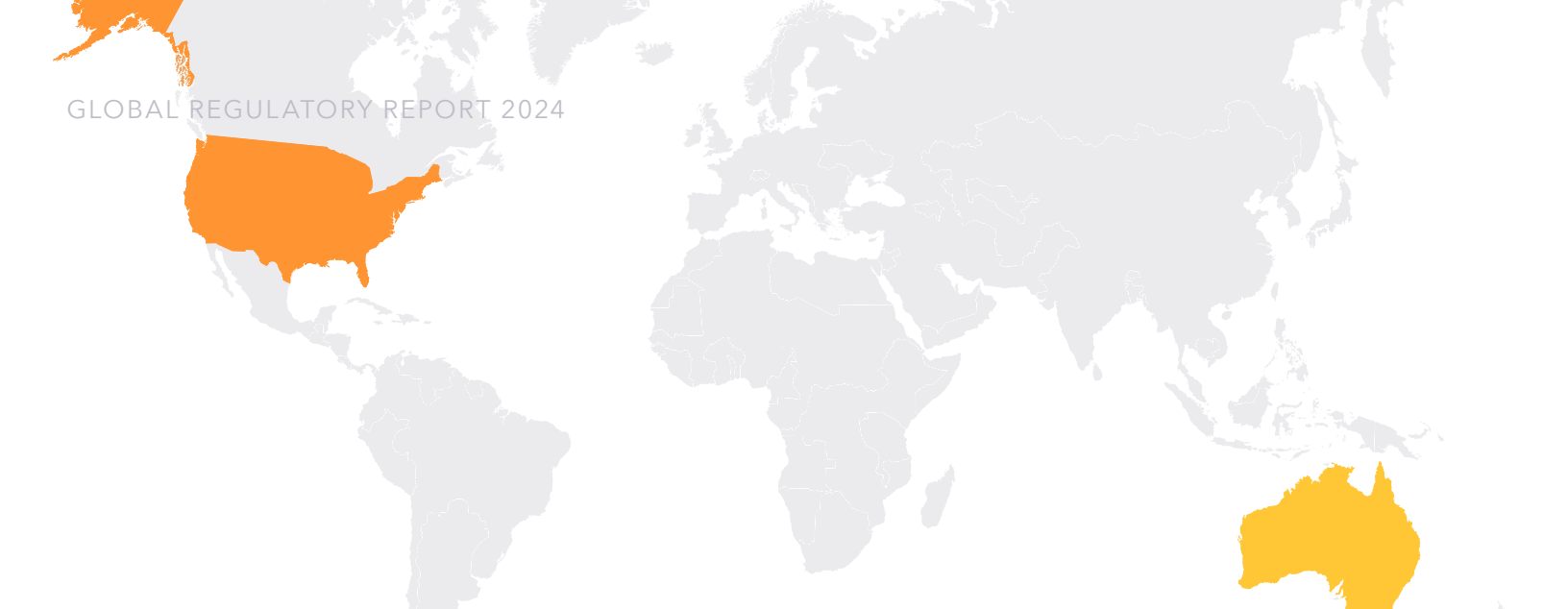
BNPL providers must adhere to the **Credit Contracts and Consumer Finance Act 2003 (CCCFA)**, which mandates clear disclosure of terms, responsible lending practices, and fair treatment of consumers. The law came into effect on September 2, 2024.

United Kingdom

Lawmakers initiated a **consultation** on draft legislation to bring BNPL providers under the supervision of the Financial Conduct Authority (FCA), mandating affordability checks and clear disclosures of loan terms to prevent consumer over-indebtedness. The consultation period concluded on November 29, 2024, and the government is currently reviewing feedback to finalize the legislation. Implementation is anticipated by 2026, providing BNPL firms time to align with the new regulatory framework.

United Arab Emirates

In September 2023, the Central Bank of the United Arab Emirates (CBUAE) introduced the **Finance Companies Regulation**, establishing a comprehensive framework for short-term lending products, including BNPL services. This regulation mandates that BNPL providers operating in mainland UAE must either obtain a 'Restricted License' from the CBUAE or partner with a licensed financial institution.



Social Media

Governments worldwide have expressed concerns about the immense power of social media. Its influence extends far beyond user-generated videos, images, or comments shared among friends, but can shape the social dynamics of entire populations. Social media serves as a platform for individuals and businesses to build thriving enterprises, it drives technological innovation and democratizes access to information across the world.

However, widespread use of social media also carries significant risks. Platform algorithms are exploited to deceive consumers, they negatively impact users' mental health and can be used to sow doubt and spread disinformation. Social media has become a tool that nefarious actors leverage to threaten individuals, communities, and even entire countries.

And, while regulators recognize the immense challenge social media companies face in moderating vast volumes of user-generated content, they will continue pushing for these companies to be liable for their impact on the world. In the European Union, the Digital Services Act (DSA) is clear in holding social media platforms accountable for risk management, content moderation, advertising transparency, and more. The United States and United Kingdom both pushed online safety regulations in the last year, both with the aim of protecting underage users from harmful online content. And in Australia, the government recently banned social media access for all users under the age of 16.

It's clear that social media companies can no longer cite free-speech protections or claim lack of awareness about the activities taking place on their platforms. Social media executives are either actively collaborating with regulators to design better protection features or resisting increased regulation, arguing for freedom of expression or advocating for self-regulation as alternatives to government mandates that vary across jurisdictions.

Below, we highlight a few recent and pending regulations related to social media:

Australia

In November 2024, approved a **groundbreaking law** prohibiting users under 16 from using major social media platforms, with non-compliant companies facing fines up to 50 million Australian dollars. The government also introduced a **News Bargaining Incentive**, mandating large tech firms to negotiate commercial agreements with news publishers or incur substantial fines, aiming to support Australian journalism and address digital platforms' responsibilities.

United States

The Kids Online Safety Act (KOSA) is a bipartisan legislative proposal in the United States aimed at enhancing online safety for minors. It seeks to establish a "duty of care" for online platforms, requiring them to implement measures to prevent and mitigate harm to users under 17, such as cyberbullying, sexual exploitation, and exposure to content promoting self-harm or substance abuse.

United Kingdom

The Online Safety Act 2023 establishes a comprehensive regulatory framework aimed at enhancing online safety by imposing duties on social media companies and search services to protect users from illegal and harmful content.

Malaysia

Malaysia plans to address issues like financial scams and cyberbullying by **mandating** that social media and messaging platforms with at least 8 million users obtain regulatory licenses by January 1, 2025. However, concerns have been raised about the clarity and potential impact on digital innovation.

European Union

The Digital Services Act, which came into effect in 2023, imposes stricter obligations on online platforms to protect minors. It requires platforms to assess and mitigate risks to children, including exposure to harmful content and advertising.

Regulatory Overview by Region

While the Financial Action Task Force (FATF) Recommendations provide the benchmark for anti-money laundering and counter-terrorism financing (AML/CTF) regulations, regional frameworks must adapt to jurisdictional nuances. Factors such as economic conditions, population size, cultural dynamics, and even geographical terrain influence a region's capacity to design and enforce effective regulations.

Our experts at EverC continuously monitor and analyze emerging regulations as they are implemented. This section offers a comprehensive overview of critical regulations in major jurisdictions that may impact payment providers and online marketplaces.

Trending Focus Area: Asia Pacific

The financial services industry is increasingly shifting its focus to the Asia-Pacific (APAC) region, driven by its rapid economic growth, digital innovation, and expanding consumer base. With countries like China, India, and Southeast Asian nations leading the way, APAC has become a global hub for fintech advancements, mobile payments, and e-commerce. Favorable regulatory environments, progressive policies, and efforts to promote financial inclusion are attracting significant investments and partnerships from global payment providers and financial institutions, positioning APAC as a key player in the industry's future.

That said, APAC continues to be a focal point for money laundering activities, particularly through shell companies and trade-based schemes, driven by the region's substantial volume of cross-border trade. This is reflected by several high-profile enforcement actions in recent years. In 2023, Singapore uncovered a historic money laundering scandal involving SGD 2.8 billion (2 billion USD) in illicit funds, with wealthy individuals exploiting luxury assets to launder proceeds of crime. Similarly, the Hong Kong Monetary Authority (HKMA) fined DBS Bank HKD 10 million (1.3 million USD) for AML compliance failures, highlighting systemic gaps in financial oversight.

In addition, cyber-enabled fraud is expanding rapidly in Southeast Asia. A [2024 report](#) by the United Nations Office on Drugs and Crime (UNODC) revealed estimated losses of \$18–37 billion in 2023 due to advanced tactics such as generative AI and deepfakes. These technologies are fueling a criminal service economy, exploiting underregulated online gambling platforms and unauthorized virtual asset service providers (VASPs) for money laundering.

This evolving threat landscape calls for urgent action. Governments across APAC are responding by enhancing their AML/CTF frameworks, including extending regulations to cover emerging platforms like cryptocurrency exchanges and fintech startups. These reforms aim to create a less hospitable environment for money laundering and terrorist financing while reinforcing the region's financial integrity.

United States

The US has a strong regulatory framework that continues to broaden its focus and reach through rules and enforcement. In recent years, the government has introduced measures to reduce compliance burdens and support initiatives such as FedNow, a real-time payments system. This push for innovation is balanced by robust anti-money laundering (AML) measures, including the Corporate Transparency Act (CTA) and updates to the Bank Secrecy Act, which mandate enhanced transparency and monitoring to combat financial crime.

Enforcement remains strong in areas like AML compliance and cryptocurrency oversight, with agencies such as the Financial Crimes Enforcement Network (FinCEN), the Securities and Exchange Commission (SEC), and the Department of Justice (DOJ) actively pursuing violations. The regulatory framework, however, is fragmented, creates complexities for businesses with overlapping federal and state jurisdiction issues. While the federal government will likely increase its focus on deregulatory policies, states like New York and California are advancing their own regulations, particularly in fintech, which may result in a patchwork regulatory environment.

Looking forward, the US aims to lead in tech innovation while addressing risks associated with emerging technologies. Following national elections in November 2024, the incoming administration's pro-business stance may further streamline regulations, but bipartisan support for AML and consumer protection measures will likely ensure continued oversight in critical areas.

The primary regulatory bodies are:

- Financial Crimes Enforcement Network (FinCEN)
- Federal Trade Commission (FTC)
- Office of Foreign Assets Control (OFAC)
- Consumer Financial Protection Bureau (CFPB)

- Securities and Exchange Commission (SEC)
- National Automated Clearing House Association (NACHA)
- The Federal Reserve

Key AML/CTF regulation:

The Bank Secrecy Act (BSA) is a foundational piece of AML legislation in the United States. It requires financial institutions to establish and maintain AML programs, file Suspicious Activity Reports (SARs) and report large cash transactions.

Notice of Proposed Rule Making (NPRM) to the Bank Secrecy Act, announced in June 2024, aim to enhance anti-money laundering and counter-terrorist financing (AML/CTF) programs across financial institutions, including payment providers. These proposed changes are designed to ensure that AML/CTF programs are effective, risk-based, and reasonably designed, aligning with mandates from the Anti-Money Laundering Act of 2020. Moreover, the proposed rules emphasize governance, requiring that AML/CTF programs be documented, approved by the board of directors, and overseen by senior management.

The public comment period for this proposed rule concluded on September 1, 2024. FinCEN has proposed that the final rule become effective six months after its issuance. Therefore, the exact compliance deadline will depend on the final rule's publication date, which has yet to be announced.

The Foreign and Corrupt Practices Act prohibits the bribery of foreign government officials and has implications for AML efforts, as money laundering can be used to facilitate bribery.

The PATRIOT Act expanded the AML requirements for financial institutions and gave law enforcement and intelligence agencies enhanced tools to combat money laundering and terrorist financing.

Anti-Money Laundering Act of 2020 established uniform beneficial ownership reporting requirements for corporations, limited liability companies, and other similar entities formed or registered in the United States.

The Corporate Transparency Act (CTA) is closely tied to the AMLA as a key component to combat money laundering and enhance financial transparency. Beginning January 1, 2024, the CTA required companies to report their beneficial ownership information (BOI) to the Financial Crimes Enforcement Network (FinCEN), addressing gaps that allow shell companies to obscure illicit activities.

For most eligible businesses, the filing deadline is slated for January 1, 2025. However, in December 2024, a US District Court in Texas issued a nationwide preliminary injunction against enforcement of the CTA, questioning its constitutionality and impact on small businesses. It is possible that the inbound administration will direct the Treasury Department to review the CTA, delaying enforcement.

Recent and pending regulation:

On November 21, 2024, the Consumer Financial Protection Bureau (CFPB) published a **Final Rule on Federal Oversight of Popular Digital Payment Apps to Protect Personal Data, Reduce Fraud, and Stop Illegal “Debanking”**. This regulation targets Big Tech and peer-to-peer platforms processing over 50 million transactions annually, with the goal of ensuring compliance with federal consumer financial laws. CFPB oversight will focus on protecting personal data, reducing fraud, and preventing illegal account closures, commonly referred to as “debanking.” Given the evolving market for digital currencies, the CFPB also limited the rule’s scope to count only transactions conducted in U.S. dollars.

The final rule will become effective 30 days after publication in the Federal Register.

Final Rule 1033 of the Dodd-Frank Act mandates that financial institutions, including banks and credit unions, provide consumers and their authorized third parties with secure and reliable access to personal financial data upon request. This data includes information about transactions, costs, charges and usage related to consumer deposit accounts, credit cards and payment services. It also establishes obligations for third parties accessing consumer data, emphasizing privacy protections, and encourages the development of fair and inclusive industry standards.

Compliance deadlines are staggered based on institution size, with the largest institutions required to comply by April 1, 2026, and smaller institutions by April 1, 2030.

The Credit Card Competition Act of 2023 is a bipartisan legislative proposal aimed at enhancing competition and reducing transaction fees in the credit card industry. The act mandates that large financial institutions—those with assets exceeding \$100 billion—must enable at least two unaffiliated payment card networks on their credit cards. At least one of these networks must be independent of the two largest networks by market share, effectively requiring options beyond Visa and Mastercard. By providing multiple network options, merchants gain the ability to choose the network through which a credit card transaction is processed. This choice is intended to encourage competition among networks, potentially leading to lower interchange fees—also known as “swipe fees”—which are charges that merchants incur for each credit card transaction.

As of December 2024, the legislation remains under consideration in Congress. The bill has been introduced and referred to the appropriate committees but has not yet been enacted into law.

European Union

The EU has long upheld a robust framework of anti-money laundering (AML) and counter-terrorist financing (CTF) measures, setting minimum standards for member states while allowing them to enact stricter laws on a national level. The centerpiece of this framework is the **"AML Package,"** formally adopted in May 2024, which includes a new single rulebook and the **sixth AML Directive (6AMLD)**. These regulations aim to harmonize AML efforts across the EU, expand the list of predicate offenses, increase transparency, and strengthen enforcement. EU agencies also collaborate with other international bodies to combat cross-border financial crime; their approach to consumer protections enforcement often serves as a model for other nations.

The primary regulatory bodies are:

- European Commission (EC)
- European Banking Authority (EBA)
- European Central Bank (ECB)
- European Securities and Markets Authority (ESMA)
- Anti-Money Laundering Authority (AMLA) - expected launch in Summer 2025

Key AML/CTF regulation:

The EU Anti-Money Laundering Directives are a series of regulatory responses to the misuse of the global financial network by criminal and terrorist actors. In essence, the evolution of these regulations over the last 30+ years obliges players in the payments space to develop systems for monitoring transactions and reporting suspicious financial activity. Furthermore, the AMLDs gradually moved toward a more cohesive regulatory framework and enhanced authorities' enforcement capabilities.

In May 2024, the EU adopted a regulation establishing a uniform cash payment limit of

€10,000 across all member states. As part of the broader implementation of the AMLDs, this latest measure aims to combat money laundering and terrorist financing by reducing the anonymity associated with large cash transactions. It extends the anti-money laundering rules to new obliged entities, such as most of the crypto-sector, traders of luxury goods and football clubs and agents. The regulation also sets tighter due diligence requirements and regulates beneficial ownership.

Regulation (EU) 2015/847 on Information Accompanying Transfers of Funds sets rules for financial institutions to include specific information when funds transfers occur within the European Union. This includes the name of the payer and payee, account numbers, and other transaction details. The regulation's primary purpose is to enhance the traceability of such transactions.

The Second Payment Services Directive (PSD2) requires banks and other financial institutions to open their payment infrastructure to third-party providers through application programming interfaces (APIs), fostering the development of new payment services and FinTech innovation. PSD2 also introduces strong customer authentication (SCA) requirements to enhance the security of electronic payments.

Recent and pending regulation:

The Third Payment Services Directive (PSD3) is a proposed update to the regulatory framework governing payment services in the EU, building on the foundation of PSD2. Key areas of focus include stronger fraud prevention measures, improved transparency in payment transactions, and increased oversight of third-party providers. It should be noted that the PSD3 proposes to further tighten the requirements for platforms and marketplaces using

the commercial agent exemption: further conditions must be met for a company to execute payment services without requiring a license as a payment service provider (PSP).

This directive is expected to take hold in late 2025 or early 2026

The Payment Services Regulation (PSR) is intended to complement the PSD3, focusing on aligning and streamlining the regulation of payment services across the EU. Unlike PSD3, which provides a framework for member states to implement through national laws, the PSR will directly apply to all EU countries, ensuring uniform rules. Key features include enhanced consumer protection, stricter anti-fraud measures, and improved operational resilience for payment providers. The regulation also seeks to address emerging challenges like the integration of open banking, digital wallets, and new payment methods, fostering a more competitive and secure payments ecosystem.

This directive is expected to take hold in late 2025 or early 2026

The Instant Payment Regulation (IPR) aims to make instant payments in euros universally accessible and secure across the EU. It seeks to modernize the payments ecosystem, enhancing the speed and efficiency of transactions within the Single Euro Payments Area (SEPA). Payment service providers (PSPs) must offer instant payment services within 10 seconds and make them available 24/7 for all euro transactions.

Compliance deadlines vary based on payment services provided, but begin as early as January 9, 2025

The Digital Operational Resilience Act (DORA)

is a pivotal regulation designed to enhance the financial sector's digital resilience. It establishes IT security standards, focusing on information and communication technology (ICT) risk management, incident reporting, and oversight of third-party ICT service providers. Firms will be mandated to evaluate "concentration risk" associated with outsourcing critical or significant operational functions to external providers. Financial firms that violate the new rules may face fines of up to 2% of their annual global revenue. Additionally, individual managers can be held personally accountable for breaches, with sanctions reaching up to 1 million euros (\$1.1 million).

The EU's General Data Protection Regulation (GDPR) mandates that companies process personally identifiable information (PII) with consent and implement adequate safeguards to minimize the risk of data breaches or leaks. In contrast, DORA shifts the focus to banks' digital supply chains, introducing a new and potentially more challenging legal framework for financial institutions. The regulation aims to help firms prevent major outage events, such as those caused by critical software updates that disrupt global IT systems. Recent incidents have left banks, payment providers, and investment companies unable to deliver services, requiring several hours to restore functionality for consumers. Under the EU's upcoming rules, similar service disruptions would be subject to heightened scrutiny and regulatory oversight.

Although DORA officially came into force on January 17, 2023, its full application will take effect on January 17, 2025.

United Kingdom

As a leading global financial center, the UK's anti-money laundering (AML) framework has evolved over several decades. The regulatory framework is largely governed by the Money Laundering Regulations (MLRs), which were recently amended to incorporate standards from the Financial Action Task Force (FATF) and recommendations from the EU's Fifth Money Laundering Directive. While Brexit impacted the UK's ability to cooperate and exchange information with EU member states, the UK reaffirmed its commitment to fighting financial crime and continues to collaborate with international organizations like FATF to uphold strong AML standards.

The primary regulatory bodies are:

- Financial Conduct Authority (FCA)
- Bank of England (BoE)
- National Crime Agency (NCA)

Key AML/CTF regulation:

The Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations

requires financial institutions and certain businesses to implement robust customer due diligence measures, maintain records of financial transactions, and report suspicious activities to the authorities. The regulations also emphasize the need to verify the identity of customers and monitor their transactions to prevent illicit fund transfers and terrorist financing.

After receiving Royal Assent in October 2023, the [Second Economic Crime \(Transparency and Enforcement\) Bill](#) strengthened the United Kingdom's AML framework by introducing additional transparency measures and enforcement mechanisms to tackle economic crime. It included new regulatory powers to recover crypto assets derived from financial crimes, introduced a beneficial ownership register of foreign entities owning property in the UK, and made several

discrete changes relating to money laundering, terrorist financing and the regulation of legal services. In November 2024, the UK Foreign Office pledged that the government is firmly supporting the establishment of fully public registers.

The Sanctions and Anti-Money Laundering Act

is designed to enable authorities to impose and enforce financial sanctions against individuals, entities, and countries involved in illicit activities. It provides the legal framework for the UK to implement sanctions in alignment with international obligations, and it includes provisions for freezing assets and imposing financial restrictions.

The Proceeds of Crime Act (POCA) provides a framework for the UK law enforcement asset claims program. However, the legislation requires businesses within the "regulated sector" (credit institutions, financial institutions, certain legal institutions, etc.) to report suspicions of money laundering and other financial crimes. These regulated entities are also required to report on suspicious activity relating to gains from conduct carried out abroad, which would be criminal if it took place in the UK.

Recent and pending regulation:

The Financial Services and Markets Act 2023 is a significant piece of UK legislation designed to modernize and strengthen the country's post-Brexit financial services framework. It introduced measures to enhance regulatory flexibility, promote innovation, and improve consumer protection in financial services. The legislation also includes **mandatory reimbursement rules** for victims of Authorized Push Payment (APP) fraud to take place within 5 days of a submitted claim, with a maximum amount of £85,000.

The mandatory reimbursement rule applies to all UK bank transfers using the Faster Payments System beginning October 7, 2024.



Enforcement Spotlight

In September 2024, the UK's Financial Conduct Authority (FCA) fined Starling Bank £29 million for significant deficiencies in its financial crime controls, particularly concerning financial sanctions screening. Despite agreeing to a restriction in 2021 that prohibited opening new accounts for high-risk customers until improvements were made, Starling Bank violated this agreement by opening over 54,000 accounts for 49,000 high-risk customers between September 2021 and November 2023. Additionally, an internal review in January 2023 revealed that since 2017, the bank's automated screening system had only checked customers against a fraction of the full list of individuals subject to financial sanctions, leading to multiple potential breaches reported to the relevant authorities. The FCA criticized Starling's financial sanctions screening controls as "shockingly lax," exposing the financial system to criminals and sanctioned individuals. Starling Bank accepted the FCA's findings, apologized for the shortcomings, and has since implemented extensive measures to enhance its financial crime control framework.

In October 2024, UK regulators enacted the Payment Services (Amendment) Regulations, introducing additional measures to combat fraud. These amendments empower payment service providers (PSPs) to delay outbound payments by 72 hours where there are reasonable grounds to suspect fraud or dishonesty. Combined with the mandatory reimbursement rule, these regulations incentivize payment providers to significantly enhance fraud detection and other tools designed to protect consumers.

The Digital Markets, Competition and Consumers Act 2024 is a comprehensive UK legislation aimed at regulating digital markets, enhancing competition, and strengthening consumer protection. It includes establishing a framework for designating firms with "Strategic Market Status" (SMS) in digital markets, imposing conduct requirements, and enabling pro-competition interventions to address market power and promote fair competition. The Act introduces specific requirements for cancelling subscriptions, bans practices such as "drip pricing," where additional fees are disclosed late in the purchasing process, and the use of fake reviews. The DMCCA grants the Competition and Markets Authority (CMA) direct enforcement powers to address breaches of consumer protection laws, including the authority to impose fines up to 10% of global turnover.

The regulation comes into force on January 1, 2025

Canada

Canada has established a comprehensive regulatory framework to combat money laundering and terrorist financing, supported by active collaboration with international organizations such as the Financial Action Task Force (FATF). In 2019, the U.S. State Department identified Canada as a "major money laundering country," citing foreign-generated criminal proceeds and the role of professional third-party launderers. Since then, Canada has undertaken several measures to enhance its anti-money laundering (AML) and counter-terrorist financing (CTF) framework, aiming to strengthen financial system integrity and improve its international standing.

The primary regulatory bodies are:

- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
- Financial Consumer Agency of Canada (FCAC)
- Office of the Superintendent of Financial Institutions (OSFI)

Key AML/CTF regulation:

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) is Canada's principal AML/CTF legislation. This regulation specifically applies to "reporting entities" and obliges them to establish an AML compliance program, Know Your Customer (KYC) protocols, recordkeeping, and reporting suspicious transactions. PCMLTFA regulations also require reporting entities to conduct ongoing monitoring of clients and continuously reassess the risk level associated with transactions and other activities.

In July 2024, the Canadian government announced [amendments](#) to the PCMLTFA that include additional registration requirements for money service businesses (MSBs) and reporting requirements for certain high-risk industries, such as casinos and real estate. This amendment reflects the government's broader strategy to address serious AML/CTF vulnerabilities within its financial system,

especially the pervasiveness of trade-based money laundering.

Additionally, government officials published its [Fall Economic Statement](#) on December 16, 2024, which includes several proposals, such as strengthening the power of enforcement agencies and increasing all individual administrative monetary penalty (AMP) amounts by 40 times the current amount. Furthermore, regulators propose establishing criminal offenses for false or incomplete information by a reporting entity and a 10-fold fine increase for all criminal offenses.

Canada's Criminal Code is the second major statute related to the country's AML/CFT regime. It applies to all individuals and businesses prohibiting them from knowingly conducting any financial or related service for any terrorist activity or group, as well as any "listed entity" (by the government). For example, Part XII under "Offenses Relating to Currency" stipulates regulations regarding fraud and dealing in counterfeit money. While a number of possible predicate crimes may result in money laundering, possession of the proceeds of crime and money laundering are in and of themselves criminal acts under the Criminal Code.

Recent and pending regulation:

Canada developed a new Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy (2023-2026) to address the global trend towards financial sector digitalization, which includes the growing use of virtual currencies and other emerging technologies. The strategy also addresses several regulatory gaps and establishes the creation of a new Canada Financial Crimes Agency which will become the country's lead enforcement agency against financial crime.

The strategy's implementation is ongoing, and the Financial Crimes Agency is slated to be operational in 2026



Enforcement Spotlight

In May 2024, FINTRAC fined Binance, a leading cryptocurrency exchange, approximately \$4.4 million for violations of Canadian money laundering and terrorist financing laws. This penalty marked one of the most significant enforcement actions by FINTRAC against a virtual asset service provider, highlighting the agency's commitment to regulating the rapidly evolving digital asset sector and ensuring compliance with Canada's AML/CTF regulations. This fine against Binance was in addition to penalties from other jurisdictions. Notably, in November 2023, Binance and its CEO, Changpeng Zhao, pleaded guilty to federal charges in the United States, resulting in a combined financial penalty exceeding \$4 billion.

Bill C-42 is an amendment to the Canada Business Corporations Act, introducing reporting requirements for individuals with significant control of businesses and a publicly accessible registry of beneficial owners. It aims to enhance corporate transparency and combat financial crimes such as money laundering and tax evasion. Penalties for directors and officers who knowingly authorize, permit, or fail to act against a corporation's non-compliance will be raised to a fine of up to C\$1 million and/or imprisonment for up to five years. This represents a substantial increase from the current maximum penalty of a C\$200,000 fine and/or six months of imprisonment.

| *The regulation took effect on January 22, 2024*

Under the Retail Payment Activities Act, Payment Service Providers (PSPs) providing retail payment activities in Canada are now required to register with the Bank of Canada. This is intended to increase transparency of PSPs and obligate them to uphold robust risk management frameworks, including safeguarding end-user funds. That said, the legislation accounts for several exclusions, including banks, credit unions, and insurance companies which are regulated under alternate legislation.

| *This regulation took effect in November 2024. Requirements to establish risk management and funds safeguarding frameworks will come into effect on September 8, 2025*

Asia-Pacific

The Asia-Pacific (APAC) region is a vast and diverse area that includes a mix of developed and developing economies, spanning East Asia, Southeast Asia, South Asia, Oceania, and parts of Central Asia. It is characterized by its cultural, economic, political, and geographic diversity, and is a significant driver of global economic growth and technological innovation.

That said, APAC remains a hotspot for money laundering, particularly through shell companies and trade-based schemes, driven by the region's high volume of cross-border trade. While several countries are addressing regulatory gaps, inconsistent enforcement across jurisdictions continues to pose challenges. A July 2024 FATF report revealed that 75% of assessed jurisdictions were only partially or non-compliant with global AML/CTF standards.

To combat these issues, APAC countries are prioritizing digital finance, cross-border transactions, and public-private collaboration to close loopholes and enhance enforcement. A key trend is the integration of crypto assets into regulatory frameworks. For instance, in October 2024, South Korea announced plans to regulate cross-border transactions involving virtual assets, aligning with FATF's updated standards, including Recommendation 15, which applies AML/CTF measures to virtual assets and VASPs.

These developments reflect the region's efforts to adapt to the dynamic financial crime landscape. Below, we examine the regulatory regimes of a few major APAC economies:

Singapore

Singapore is a leading financial hub in the APAC region, renowned for its stable economy, advanced infrastructure, and strong regulatory environment.

Strategically located at the crossroads of major global trade routes, Singapore is a key player in global finance, wealth management, and fintech innovation. Its commitment to high regulatory standards and a business-friendly environment has made it a preferred destination for multinational corporations, financial institutions, and investors.

While the country's robust regulatory framework is widely praised, the city-state faces challenges such as the growing sophistication of financial crimes, including cyber-enabled fraud and the use of shell companies. In response, Singapore continues to develop and expand its regulatory framework, adopting advanced technologies like artificial intelligence for transaction monitoring and strengthening public-private partnerships.

The primary regulatory bodies are:

- Monetary Authority of Singapore (MAS)
- Suspicious Transaction Reporting Office (STRO)
- Commercial Affairs Department (CAD)

Key AML/CTF regulation:

The Corruption, Drug Trafficking, and Other Serious Crimes Act (CDSA) provided the legal framework for identifying, tracing, freezing, and confiscating benefits from serious crimes, ensuring that such proceeds cannot be used to fund further illegal activities or enjoy undue advantages. The CDSA covers a wide range of predicate offenses, including corruption, drug trafficking, terrorism financing, fraud, and other severe crimes. The list of designated offenses is periodically updated to address emerging threats. The Act also mandates reporting of suspicious transactions by financial institutions and designated non-financial businesses and professions.

Authorities *amended the CDSA to introduce new offenses, including criminalizing rash or negligent money laundering, where individuals deal with*

property despite suspicions it may be proceeds of crime, and assisting others in retaining benefits from criminal conduct. Additionally, the misuse of Singapore's national digital identity system, Singpass, was addressed, making it an offense to disclose or misuse credentials for unlawful purposes.

These amendments became effective from February 8, 2024

The Terrorism (Suppression of Financing) Act (TSOFA) criminalized the provision or collection of funds with the knowledge or reasonable belief that they will be used to commit terrorist acts, regardless of whether the acts occur. It granted authorities the power to freeze and confiscate assets linked to terrorism and mandates financial institutions to conduct due diligence, monitor transactions, and report suspicious activities. The TSOFA also applies to offenses committed outside Singapore if the offender or the funds have a connection to Singapore, indicating an effort to discourage transnational crime.

Payment Services Act 2019 is a comprehensive regulatory framework that governs payment systems and payment service providers in Singapore. It mandated all payment service providers to adhere to anti-money laundering (AML) and counter-terrorism financing (CTF) requirements, including customer due diligence (CDD), record-keeping, and reporting suspicious transactions. Additionally, the regulation established safeguards, such as limits on stored value balances and protections for funds held by payment service providers, to reduce risks to consumers as well as granted the Monetary Authority of Singapore (MAS) oversight authority.

In 2024, MAS expanded the Payment Services Act to cover digital payment token (DPT) service providers, imposing stricter AML obligations. This expansion ensures that all digital payment services, including cross-border transfers and custodial services for digital tokens, are regulated, aligning with FATF standards.

Entities conducting newly regulated activities were required to notify MAS by 4 May 2024 and submit a license application by 4 October 2024 to continue operations while their applications are under review.

Financial Services and Markets Act 2022

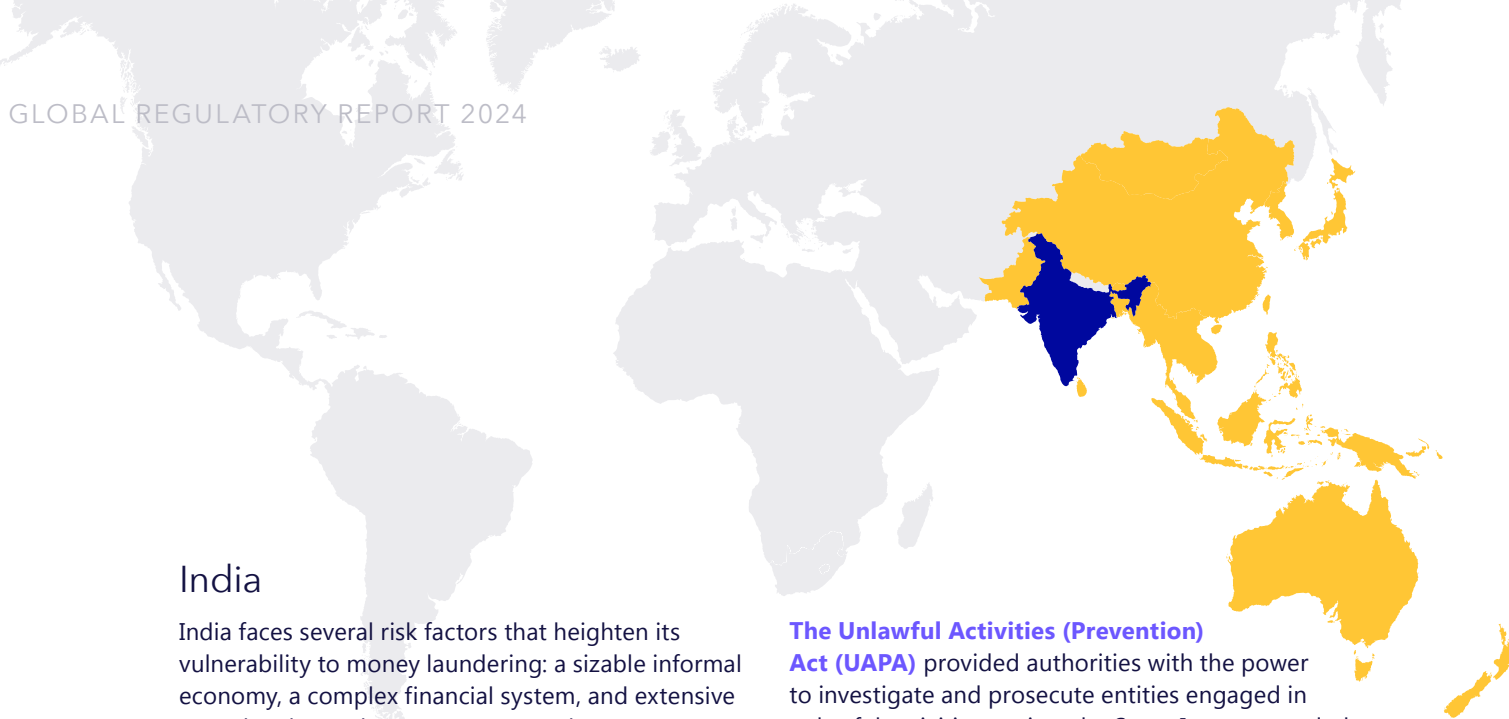
streamlined MAS regulatory oversight and expanded it to include entities offering cross-border financial services and digital token-related activities. It also established a unified licensing framework for financial institutions, simplifying the process and ensuring consistency across different financial services sectors.

Recent and pending regulation:

The Monetary Authority of Singapore launched the Collaborative Sharing of Money Laundering/ Terrorism Financing Information & Cases (COSMIC)

platform in April 2024, which facilitates secure information sharing between banks to detect suspicious activities. The platform operates under the amended Financial Services and Markets Act 2022 (FSMA), which provides the legal basis and safeguards for information sharing. This collaboration between MAS and several major banks enhances AML efforts across borders, focusing on key risks like misuse of legal entities and trade finance.

On October 18, 2024, MAS published guidelines to assist Prescribed FIs in complying with Notice FSM-N02, which outlines requirements for sharing AML/CTF information through COSMIC. These guidelines provide clarity on key concepts, internal policies, procedures, and controls necessary for effective information sharing.



India

India faces several risk factors that heighten its vulnerability to money laundering: a sizable informal economy, a complex financial system, and extensive cross-border trade. In recent years, the country has established a robust regulatory framework supported by effective implementation and strong enforcement agencies. Significant progress has been made in enhancing India's anti-money laundering (AML) regime, aligning it with international standards, and bolstering enforcement capabilities.

The primary regulatory bodies are:

- Reserve Bank of India (RBI)
- India Enforcement Directorate (ED)
- Financial Intelligence Unit – India (FIU-IND)
- Securities and Exchange Board of India (SEBI)

Key AML/CTF regulation:

The Prevention of Money Laundering Act (PMLA)

obliged banking and other financial institutions to implement comprehensive AML procedures. It also defines money laundering offenses and outlines protocols for the investigation, prosecution, and confiscation of proceeds of crime. Furthermore, this legislation established regulatory authorities, such as the Financial Intelligence Unit – India (FIU-IND), to oversee and enforce anti-money laundering measures in the country.

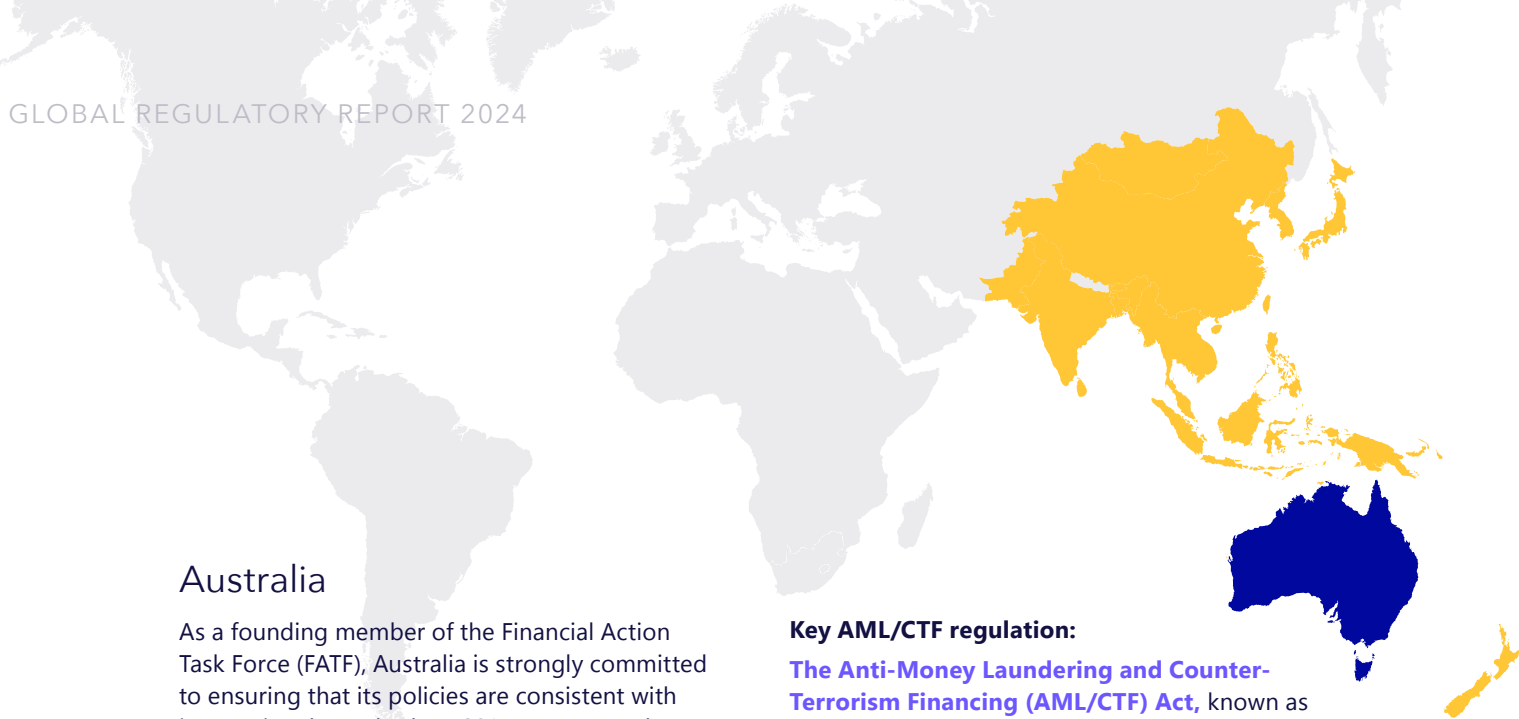
In 2023, Indian authorities widened the scope of the PMLA to cover a much wider range of professional service providers obligated to uphold the legislation, as well as added crypto entities to AML regulation. Subsequently, in June 2024, Binance was fined \$2.25 million USD for operating in India in violation of local AML regulations.

The Unlawful Activities (Prevention)

Act (UAPA) provided authorities with the power to investigate and prosecute entities engaged in unlawful activities against the State. It was amended in 2004 to criminalize terrorist financing in accordance with international standards.

The Consumer Protection (E-Commerce) Rules

lay out the requirements for general e-commerce, and specifically for marketplaces, mainly regarding the information they must collect from sellers, the protections given to consumers, and safeguards against repeated bad actors.



Australia

As a founding member of the Financial Action Task Force (FATF), Australia is strongly committed to ensuring that its policies are consistent with international standards. A 2015 FATF Mutual Evaluation Report identified significant deficiencies in Australia's anti-money laundering (AML) and counter-terrorist financing (CTF) framework, leading to several high-profile regulatory compliance breaches.

In response, Australian authorities introduced new AML/CTF regulations, including requirements for financial institutions to conduct risk-based customer due diligence (CDD) and enhance information sharing between the public and private sectors.

Regulatory updates are anticipated to further simplify and strengthen AML/CTF rules. In November 2024, the Australian Parliament passed the AML/CTF Amendment Bill, which seeks to modernize the country's regulatory framework. Australia is also focusing on strengthening digital transaction monitoring, addressing the risks posed by crypto-assets and ensuring that service providers are fully compliant. Failure to pass these reforms could risk Australia being "grey-listed" by FATF, which could have a negative impact on the economy by discouraging foreign investment.

The primary regulatory bodies are:

- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Reserve Bank of Australia
- Australian Prudential Regulation Authority (APRA)

Key AML/CTF regulation:

The Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act, known as Tranche 1, sets out key obligations for regulated entities and established the authority of AUSTRAC.

*In November 2024, the Australian Parliament passed the **Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Amendment Bill**. The amended regulation aims to simplify, clarify, and modernize the AML/CTF regime, making it more effective and fit-for-purpose while reducing regulatory burdens. It also extends AML regulations to cover high-risk services provided by lawyers, accountants, trust and company service providers, real estate professionals, and dealers in precious metals and stones (known as 'tranche 2' entities).*

AML/CTF Rules Instrument provides specific details and requirements for how businesses and reporting entities are to implement AML/CTF measures. This includes customer due diligence (CDD), transaction monitoring, record keeping, cross-border transfers, risk assessment, and training and compliance programs.

As a complement to the AML/CTF Act, the AML/CTF (Prescribed Foreign Countries) Regulation aims to strike a balance between reducing regulatory burdens for certain international transactions and maintaining effective AML/CTF measures. It allows Australian officials to designate certain countries as high-risk, thus requiring financial institutions to conduct enhanced due diligence on individuals or entities located those countries.

China

China has a strong grasp of the financial crime risks it faces, but the fragmented nature of its multiple regulatory bodies presents challenges to effective prevention of money laundering, particularly with cross-border fund transfers. Following criticism from the Financial Action Task Force (FATF) in 2019 regarding its anti-money laundering (AML) shortcomings, Chinese authorities revised and expanded their regulatory framework, introducing stricter penalties for financial crimes.

This effort culminated in the launch of the **Three-Year Action Plan for Combating Money Laundering Violations and Crimes**, with the goal of enhancing China's AML framework. Running from 2022 to December 2024, the initiative exhorts 11 government departments to tighten compliance requirements and strengthen financial crime investigation protocols. As the campaign nears its end, the Supreme People's Procuratorate (SPP) has emphasized the importance of accurately applying the newly revised Anti-Money Laundering Law, set to take effect on January 1, 2025. This includes deepening the current anti-money laundering campaign and ensuring that relevant criminals are punished in accordance with the law.

The primary regulatory bodies are:

- People's Bank of China (PBOC)
- China Anti-Money Laundering Monitoring and Analysis Center (CAMLMAC)
- National Internet Finance Association of China (NIFA)
- China Securities Regulatory Commission (CSRC)

Key AML/CTF regulation:

PRC Anti-Money Laundering (AML) Law provides the legal basis for AML requirements to be placed on all financial institutions established within China. It also includes non-financial institutions obliged to maintain AML protocols.

Article 191 of PRC Criminal Law pertains to the crime of concealing, transferring, or assisting in the transfer of proceeds of crime. It encompasses activities that help individuals or entities hide or move money or assets obtained through criminal activities, such as embezzlement or corruption, officially making money laundering a criminal offense.

PRC Counter-Terrorism Law is a comprehensive legal framework aimed at addressing and preventing terrorism within the country and deterring terrorist financing. While it was enacted to enhance national security, it has also raised questions and concerns regarding its broad definition of terrorism and potential impact on civil liberties and human rights.

The "Administrative Rules" essentially require financial institutions and payfacs to implement comprehensive customer verification protocols and ongoing monitoring under a unified mechanism which the PBOC oversees. The "administrative rules", as well as the subsequent **"measures"** established in 2021, expanded the scope of China's AML/CTF framework, calling for these financial institutions and non-bank institutions to maintain stronger internal controls and risk management protocols.

The E-Commerce Law is a comprehensive regulatory framework designed to oversee the growing e-commerce sector and address issues such as counterfeit goods, consumer protection, and unfair competition. It applies to all e-commerce activities conducted within China, including platform operators (e.g., Alibaba, JD.com), third-party merchants, and individual sellers.

Since its implementation in 2019, the law has undergone several updates to address emerging challenges in the ecommerce space. In June 2024, the Ministry of Commerce released draft regulations aimed at promoting cross-border ecommerce. These rules focus on the development of overseas warehouses and the expansion of cross-border online businesses, in addition to strengthening consumer protections. The new regulations explicitly ban practices such as forging user evaluations, promoting bundled sales without consent, and engaging in big data-enabled price discrimination.

These came into effect on July 1, 2024.

The Anti-Telecom and Online Fraud Law requires telecom operators, financial institutions, and internet services providers to maintain internal systems to prevent fraud risks. This includes conducting due diligence on clients, identifying beneficial owners, and monitoring for suspicious transactions. The law also extends its legal authority beyond Chinese borders to cover foreign entities or individuals who engage in online fraud targeting China's mainland territory or offer support for such fraudulent activities.

In November 2024, China's Ministry of Public Security (MPS), in collaboration with three other government agencies, announced the **"Joint Punishment Measures for Telecom and Internet Fraud and Related Crimes"** to facilitate the enforcement of the Anti-Telecom and Online Fraud Law.

The new measures took effect on December 1, 2024.

Recent and pending regulation:

In September 2024, China introduced amendments to its Anti-Money Laundering Law, marking the first revision since 2007. The amendments broadened the definition of money laundering to include any activity concealing the proceeds and profits from any criminal activity, including terrorist financing. Additionally, the regulation proposes to establish a beneficial ownership registration system and expand AML compliance obligations to "specific non-financial institutions", such as real estate developers and notaries, accounting firms, law firms, securities managers, and dealers in precious metals and gemstones. Notably, the amended AML will have extraterritorial application, meaning that it will extend China's jurisdiction to investigate and prosecute any overseas money laundering and terrorist financing activity that poses a national security threat.

The amendments to China's AML Law are scheduled to take effect on January 1, 2025.

Hong Kong

Hong Kong is a leading financial hub in the Asia-Pacific (APAC) region, known for its strategic location, sophisticated infrastructure, and robust regulatory framework, which aligns with international standards set by the Financial Action Task Force (FATF). However, Hong Kong's open financial system and high volume of cross-border transactions make it susceptible to money laundering risks. Cyber-enabled fraud and the exploitation of shell companies are emerging concerns due to the fact that the city serves as a gateway between mainland China and international markets, making it a critical node for global trade and finance.

The primary regulatory bodies are:

- Hong Kong Monetary Authority (HKMA)
- Securities and Futures Commission (SFC)
- Customs and Excise Department (C&ED)
- Companies Registry (CR)
- Joint Financial Intelligence Unit (JFIU)

Key AML/CTF regulation:

Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) governs the AML/CTF obligations of financial institutions and designated non-financial businesses and professions (DNFBPs), including customer due diligence (CDD) and record-keeping requirements. It also introduced a licensing regime for trust or company service providers (TCSPs), requiring them to apply for a license from the Registrar of Companies and satisfy a "fit-and-proper" test before they can provide trust or company services as a business in Hong Kong.

The Securities and Futures Commission (SFC) issued [updated guidelines](#) on June 1, 2023, introducing a licensing regime for virtual asset service providers (VASPs) and detailing AML/CTF obligations for licensed corporations and SFC-licensed VASPs. These

guidelines emphasized customer due diligence, ongoing monitoring, and suspicious transaction reporting, in addition to regular training programs.

Drug Trafficking (Recovery of Proceeds)

Ordinance (DTROPO) aims to combat drug trafficking by enabling the authorities to trace, confiscate, and recover proceeds derived from drug-related crimes. It also officially criminalized the handling, possessing, or dealing with proceeds from drug trafficking with the intent to conceal or disguise their origin.

Organized and Serious Crimes Ordinance

(OSCO) is a cornerstone of Hong Kong's legislative framework to combat organized crime and serious offenses. It empowered authorities to investigate, prosecute, and confiscate the proceeds of crime, targeting not only direct criminal activities but also addresses their financial and operational underpinnings. The OSCO criminalized money laundering, including the handling or dealing with proceeds derived from organized or serious crimes.

United Nations (Anti-Terrorism Measures)

Ordinance (UNATMO) implements UN Security Council resolutions on counterterrorism and ensures Hong Kong complies with international standards, particularly those set by FATF. It also mandated that financial institutions and designated non-financial businesses and professions (DNFBPs) report suspicious transactions related to terrorism to the Joint Financial Intelligence Unit (JFIU).

South Korea

South Korea's Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulatory framework is robust and aligns with international standards set by the Financial Action Task Force (FATF). It complies with United Nations Security Council Resolutions (UNSCRs) and works closely with global organizations to combat financial crimes, including the proliferation of weapons of mass destruction.

However, South Korea's geographical position near China and North Korea heightens its exposure to cross-border financial crime risks, including trade-based money laundering and illicit financial flows. These risks are compounded by its proximity to major financial hubs like Hong Kong, which has intensified its AML efforts, potentially pushing illicit activities into other Asia Pacific (APAC) jurisdictions like South Korea.

Additionally, North Korea poses unique challenges, as the regime is known to engage in cybercrime and the use of front companies to circumvent international sanctions, funneling illicit funds through regional financial systems. The rise of virtual assets also presents a growing risk, with cryptocurrencies being exploited for laundering illicit proceeds and financing unlawful activities. South Korea actively addresses these challenges by continually enhancing its legal framework, including incorporating Virtual Asset Service Providers (VASPs).

The primary regulatory bodies are:

- Korea Financial Intelligence Unit (KoFIU)
- Financial Services Commission (FSC)
- Financial Supervisory Service (FSS)
- Korean National Police Agency (KNPA)
- Ministry of Economy and Finance (MOEF)

Key AML/CTF regulation:

The Proceeds of Crime Act (POCA) is a cornerstone of the country's AML framework, aimed at combating money laundering and confiscating criminal proceeds.

The Act criminalizes activities that disguise the origin, ownership, or use of illicit funds and provides legal authority to freeze and confiscate assets derived from criminal activities. Financial institutions are required to monitor transactions, perform customer due diligence, and report suspicious activities. The POCA also addresses cross-border money laundering risks, empowering authorities to take action against trade-based laundering and illicit financial flows.

The Financial Transaction Reports Act (FTRA)

mandates that financial institutions implement preventive measures such as Customer Due Diligence (CDD), Suspicious Transaction Reports (STRs), and Currency Transaction Reports (CTRs). It also led to the establishment of the Korea Financial Intelligence Unit (KoFIU), which oversees AML/CFT compliance and serves as a liaison between financial institutions and law enforcement agencies.

In October 2024, South Korea [announced](#) plans to regulate cross-border transactions involving virtual assets, such as cryptocurrencies. This initiative aims to address the significant amount of foreign exchange-related crimes, with 81.3% involving virtual assets in recent years.

Starting from the second half of 2025, businesses engaged in these activities will be required to register with authorities in advance and report their monthly transactions to the Bank of Korea.

Act on Prohibition against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (PFOPIA)

criminalizes the financing of terrorism and the proliferation of weapons of mass destruction. It also outlines procedures for designating individuals and entities involved in such activities, prohibiting financial institutions from conducting transactions with them without prior approval from the Financial Services Commission (FSC).

Latin America

In recent years, many of the 18 countries in Latin America have made efforts to strengthen their AML/CFT frameworks. The region's diverse population, predominantly comprising unbanked or underbanked consumers, along with a demand for efficient cross-border money transactions, creates significant opportunities for new financial products to flourish.

However, the region continues to face a complex and challenging financial crime environment. Security issues that enable violence to take place also make it easier for illicit funds to move across borders and re-enter local economies. This often leads to more violence and instability in the region. Corruption, the most common financial crime, is a major obstacle to enforcing the law.

Many Latin American countries are classified as "emerging economies," which partially explains why their AML protocols often fall short of international standards. Below, we examine the regulatory regimes of some of the region's major economic powerhouses.

Argentina

As a member of the Financial Action Task Force (FATF), Argentina is committed to implementing the organization's 40 Recommendations, which serve as the global benchmark for AML/CFT measures. In 2010, the FATF's mutual evaluation identified several deficiencies in the country's money laundering and counter-terrorism financing regime. Since then, Argentina's regulatory landscape has evolved significantly, with continuous efforts to strengthen its framework in line with FATF recommendations, which led to another mutual evaluation **announced** in October 2024.

Nevertheless, Argentina continues to grapple with significant challenges, particularly in addressing corruption and money laundering linked to unregulated financial sectors. Additionally, the country is contending with severe inflation, despite aggressive fiscal measures implemented by President Javier Milei, including a 50% devaluation of the peso and substantial government spending cuts. As a result, businesses and consumers are seeking alternatives to local markets plagued by inflation and supply constraints, leading to a spike in cross-border e-commerce.

The primary regulatory bodies are:

- Financial Information Unit (Unidad de Información Financiera - UIF)
- Central Bank of the Republic of Argentina (BCRA)
- National Securities Commission (CNV)

Key AML/CTF regulation:

Law 25.246 is an amendment to Argentina's Criminal Code and serves as the primary AML/CFT regulation. It established the country's main regulatory authority, the Financial Information Unit (UIF), and provides detailed definitions of money laundering crimes, and in particular, which entities are obliged to report to the UIF. The law and its amendments require all financial entities to carry out Customer Due Diligence (CDD), maintain recordkeeping on clients, and report suspicious transactions to the UIF within 150 days of detection.

In 2011, legislators approved Law 26.683

amending Argentina's existing AML/CFT framework (Law 25.246). It strengthened the role of the UIF and its supervisory powers, as well as expanded the list of entities required to comply with AML/CFT regulations. These laws include the following requirements: A Suspicious Operation Report (similar



to a Suspicious Activity Report – SAR) must be submitted to the UIF within 150 days of detection by a regulated entity for potential money laundering activity; and in the case of terrorist financing, within 48 hours of detection. Furthermore, regulated entities are required to submit systematic operations reports to the UIF on a monthly basis. This includes financial services companies (“Companies dedicated to the transportation of cash”) as well as operations carried out with virtual currencies.

The Central Bank’s Communiqué A 6859/6885 regulated Payment Service Providers (PSPs) for the first time beginning in 2020. The communiqué defines PSPs as legal entities that, without being financial institutions, perform at least one function within a retail payment scheme. This includes offering payment accounts (virtual wallets) that enable customers to make and receive payments. PSPs must ensure that customer funds credited to payment accounts are available at all times and can be immediately accessed upon demand. Additionally, customer funds must be held in accounts at local financial institutions, separate from the PSP’s operational accounts, to protect customer assets.

Recent and pending regulation:

Resolution UIF No. 169/2023 introduced new guidelines for managing money laundering and terrorist financing risks. These guidelines apply to companies engaged in capitalization and savings operations, mandating a risk-based approach in line with FATF Recommendations.

The resolution became effective on November 1, 2023

Resolution UIF No. 194/2023 overhauled previous AML/CFT regulations applicable to the gambling sector, updating compliance requirements to address evolving financial crime risks. This includes liability placed on obligated entities regardless if Know Your Customer (KYC) and due diligence are conducted by third-party services. The resolution became effective on December 1, 2023, however there are certain provisions regarding some of the new obligated entities, such as online gaming/gambling providers.

Online gaming providers are required to implement KYC and due diligence measures by March 1, 2024

Obligated entities are also required to submit an Annual Systematic Report (ASR) between January 2 and March 15, 2025

All obligated entities, including online gaming/gambling providers, are required to submit a self-assessment risk report by April 30, 2026

Brazil

As South America's most populous nation and a regional e-commerce powerhouse, Brazil faces significant challenges in combating financial crimes. Criminal networks take advantage of the country's vast size, diverse economy, and intricate financial structure to launder illicit proceeds.

However, Brazil continues to make progress in strengthening its AML/CFT framework and addressing key regulatory shortcomings. Given its vast coastline and extensive shared borders with several countries, Brazil's authorities must continue fostering international cooperation to effectively combat cross-border financial crimes.

The primary regulatory bodies are:

- Central Bank of Brazil (BACEN)
- Financial Activity Control Council (COAF)
- Private Insurance Superintendence (SUSEP)
- National Anti-Piracy Council for the Ministry of Justice (CNCP)
- Securities and Exchange Commission (CVM)

Key AML/CTF regulation:

Law 9.613/1998 and later iterations (known as the "AML Law") established the framework for Brazil's AML protocols for a wide range of financial institutions. Introduced and enforced by the country's supervisory authorities, the law includes basic requirements for financial institutions, such as conducting customer due diligence and reporting suspicious transactions. The AML Law was revised in 2012 to eliminate the list of predicate offenses connected to money laundering.

*Amending Brazil's "AML Law", authorities passed **Law No. 14,478/2022** (Cryptocurrency Law) to define virtual assets and designate the Central Bank of Brazil (BCB) as the authority to license and supervise Virtual Asset Service Providers (VASPs). It also includes enhanced penalties for money laundering offenses involving virtual assets.*

The law became effective in June 2023

Law 10.701/2003 includes terrorist financing as a predicate offense for money laundering and enforces the requirement for all financial institutions to report transactions suspected of being related to financing terrorism. The subsequent laws, **13.260/2016** and **13.810/2019**, relate to the prohibition of terrorism and enforce the immediate freezing of terrorist assets in compliance with the United Nations Security Council sanctions.

Law No. 12.865/2013 represented a significant step in modernizing and regulating Brazil's payment system, encompassing electronic payments, financial services, and consumer protection. It established that payment schemes and institutions become part of the Brazilian Payments System (Sistema de Pagamentos Brasileiros). The law also requires that all payment schemes and institutions implement a risk-based approach.

In October 2023, the Central Bank of Brazil issued Resolution No. 343, establishing procedures for financial institutions, payment providers, and other authorized entities to share data related to fraud detection and reporting. Entities are required to implement measures to detect and report signs of fraud in various activities, including account opening, payment services, and credit transactions. Additionally, entities must retain specific data regarding the identities of fraud perpetrators and details of fraudulent transactions.

The resolution's compliance deadline was on February 1, 2024

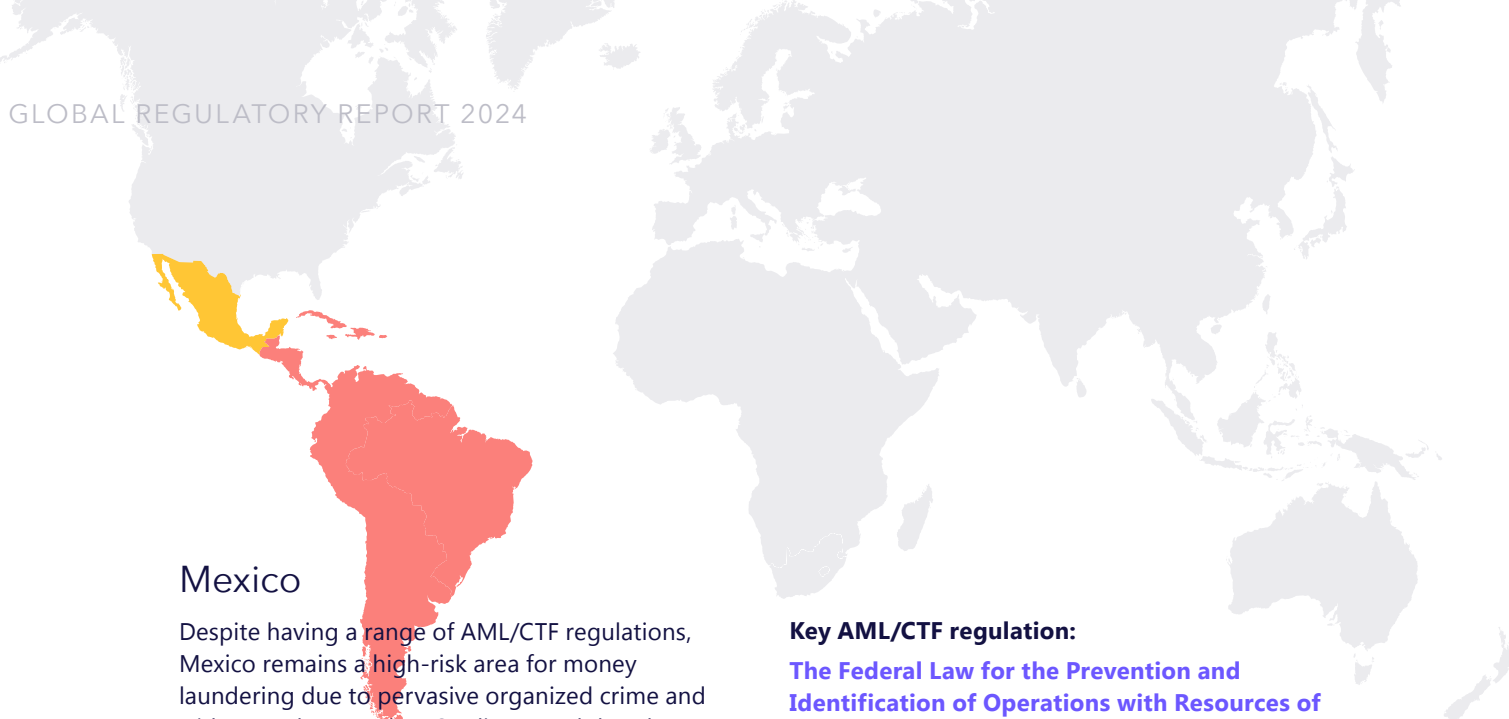


The Consumer Defense Code is the basis for any consumer relationship in Brazil— e-commerce or not. It is applied to both B2B relationships and B2C relationships. As it relates to e-commerce, the most important provisions relate to deceptive marketing practices (article 6) for advertised products or services.

Recent and pending regulation:

While traditional casinos and gambling in most forms has been prohibited in Brazil since 1946, lawmakers enacted **Bill No 3626/23** to regulate online betting (“games of chance”) companies. Authorized companies must register for a betting license with the Ministry of Finance and permanently comply with federal rules to prevent fraud, money laundering, and abusive advertising. Additionally, **Normative Ordinance No 1,207** permits online slots, card games such as blackjack and poker, roulette, and crash games but prohibits the use of credit cards and cryptocurrencies for wagering.

The regulation will be effective starting January 1, 2025



Mexico

Despite having a range of AML/CTF regulations, Mexico remains a high-risk area for money laundering due to pervasive organized crime and widespread corruption. Studies reveal that drug cartels rank as among the largest employers in the country, comparable to sectors like general medicine and coffee/tobacco cultivation. These criminal networks utilize sophisticated methods for laundering money within and beyond the Mexican economy while obscuring the true beneficiaries of their activities.

Over the past decade, Chinese criminal syndicates have expanded their operations in Mexico, supplying fentanyl precursors for cartels to produce narcotics and engaging in crimes like illegal wildlife trafficking. Although there is no direct evidence of Chinese government involvement, ongoing corruption among Mexican authorities raises concerns that officials from both nations may be indirectly benefiting or, at a minimum, turning a blind eye to these activities. That said, President Claudia Sheinbaum has intensified efforts to combat fentanyl production in Mexico since entering office in October 2024. Her administration promises to implement a data-driven strategy that includes enhanced policing, social spending, and the deployment of specialized task forces to regions like Sinaloa to dismantle cartel operations.

The primary regulatory bodies are:

- National Banking and Securities Commission (Comisión Nacional Bancaria y de Valores – CNBV)
- Attorney General's Office (Procuraduría General de la República – PGR)
- Secretariat of Finance and Public Credit (Secretaría de Hacienda y Crédito Público – SHCP)
- National Commission for the Protection and Defense of Users of Financial Services (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros – Condusef)

Key AML/CTF regulation:

The Federal Law for the Prevention and Identification of Operations with Resources of Illicit Origin is a crucial component of Mexico's AML framework, focusing on identifying and preventing financial transactions associated with illegal or criminal sources. The law imposes legal obligations on individuals and entities to comply with AML/CTF measures, including the requirement for financial institutions, casinos, notaries and other designated entities to conduct customer due diligence and report any suspicious transactions to the country's Financial Intelligence Unit.

The National Law for Asset Forfeiture established a legal process for the identification, seizure, and forfeiture of assets that are proven to be derived from illegal activities. An essential tool in Mexico's fight against money laundering, it enables authorities to pursue the finances of Mexico's drug cartels, disrupting their ability to enjoy the financial benefits of their illicit operations.

Middle East and North Africa

The Middle East and North Africa (MENA) region presents a diverse landscape in its approach to anti-money laundering (AML) and counter-terrorist financing (CTF) regulation, reflecting varying levels of alignment with international standards set by the Financial Action Task Force (FATF).

Countries like the **United Arab Emirates (UAE)**, **Saudi Arabia**, and **Qatar** have demonstrated strong commitments to align with FATF recommendations, developing strategies to address financial crime risks and implementing national action plans. Several MENA countries, including **Egypt**, **Jordan**, and **Bahrain**, have shown moderate progress in establishing foundational AML/CTF frameworks and participate in regional coordination efforts through the Middle East and North Africa Financial Action Task Force (MENAFATF). However, challenges such as regulatory gaps, limited resources, and inconsistent enforcement hinder full compliance with FATF standards.

Other nations in the region, particularly those with ongoing political instability or weak governance, struggle to execute effective AML/CTF measures. In fact, 17 out of 24 countries on FATF's "grey list" are in the MENA region. Countries like Libya, Yemen, and Syria face significant challenges due to limited institutional capacity, corruption, and lack of international cooperation due to western-imposed sanctions. Some jurisdictions have resisted full alignment with FATF standards, prioritizing economic growth or regional political considerations over stringent compliance. This divergence creates vulnerabilities in the financial system and opportunities for illicit activities to exploit these gaps.

United Arab Emirates

The United Arab Emirates (UAE) has significantly improved its anti-money laundering (AML) and counter-terrorist financing (CTF) regulatory framework in recent years. In March 2022, the Financial Action Task Force (FATF) placed the UAE on its "grey list,"

citing strategic deficiencies in AML/CTF measures. The UAE responded by implementing comprehensive reforms, including enhanced oversight of financial institutions, improved transparency of legal persons, and strengthening investigations of terrorist financing. These efforts led to the UAE's removal from the FATF "grey list" in February 2024, reflecting its commitment to strengthening its financial system's integrity.

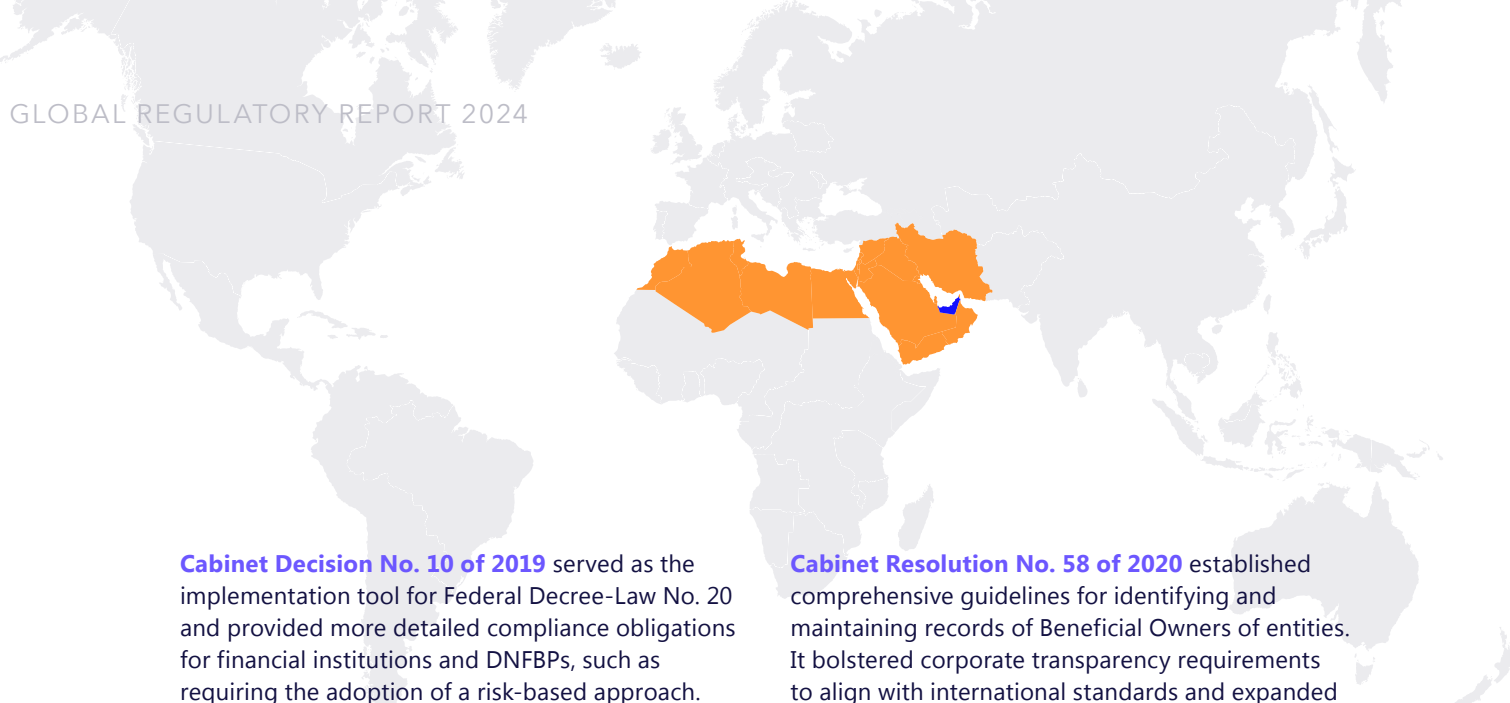
However, the UAE's position as a major financial center continues to make it susceptible to sophisticated money laundering schemes, including trade-based money laundering and the misuse of virtual assets. Additionally, significant quantities of gold from conflict zones are smuggled into the country and individuals linked to criminal activities regularly invest in UAE real estate. These highlight some of the vulnerabilities in the Emirati financial system, which pose serious risks of money laundering and terrorist financing.

The primary regulatory bodies are:

- Executive Office of Anti-Money Laundering and Combatting Financing of Terrorism and Financing (EO AML/CTF)
- Central Bank of the UAE (CBUAE)
- Financial Intelligence Unit (FIU)
- Dubai Financial Services Authority (DFSA)
- Abu Dhabi Global Market (ADGM)

Key AML/CTF regulation:

Federal Decree-Law No. 20 of 2018 established the legal framework for combating money laundering and terrorist financing in the UAE. It outlined penalties for individuals and entities involved in money laundering and terrorist financing, mandated the establishment of an Emirati Financial Intelligence Unit (FIU), and required financial institutions and non-financial businesses and professions (DNFBPs) to implement robust AML measures, such as conducting customer due diligence (CDD) and reporting suspicious transactions.



Cabinet Decision No. 10 of 2019 served as the implementation tool for Federal Decree-Law No. 20 and provided more detailed compliance obligations for financial institutions and DNFBPs, such as requiring the adoption of a risk-based approach.

*The Central Bank of the UAE (CBUAE) issued **new guidance** for Licensed Financial Institutions (LFIs) on AML/CTF, aligning with FATF standards to ensure effective compliance. The guidance emphasized the development of internal policies, controls, and digital CDD procedures to ensure effective transaction monitoring and sanctions screening, aligning with FATF standards.*

The guidance became effective immediately after being announced in 2023

Cabinet Resolution No. 74 of 2020 established a comprehensive framework for implementing United Nations Security Council Resolutions (UNSCRs) related to combating terrorism, terrorist financing, and the proliferation of weapons of mass destruction (WMDs). It also outlines sanctions repercussions for entities and individuals which fail to adhere to compliance obligations related to terror financing, such as conducting CDD and transaction monitoring.

Circular No. 24/2019 serves as the regulatory guideline for Hawala providers in the UAE. Hawala—an informal method of transferring funds—is regulated in accordance with Federal Decree-Law No. 20 of 2018 to ensure transparency and prevent misuse for illicit activities. Individuals or entities wishing to conduct Hawala activities must obtain a Hawala Provider Certificate from the CBUAE, ensuring they are listed in the official Hawala Providers Register. Furthermore, Registered Hawala Providers (RHPs) are prohibited from accepting deposits, exchanging currencies, buying or selling travelers' checks, and engaging in activity with unregistered Hawala providers in the UAE.

Cabinet Resolution No. 58 of 2020 established comprehensive guidelines for identifying and maintaining records of Beneficial Owners of entities. It bolstered corporate transparency requirements to align with international standards and expanded the scope of the regulation to apply to all corporate entities incorporated in the UAE mainland and non-financial free zones (Commercial Free Zones).

Cabinet Resolution No. 109 of 2023 superseded the previous Cabinet Resolution No. 58 of 2020, introducing more robust measures for identifying and maintaining records of Beneficial Owners and broadened enforcement mechanisms.

The Resolution became effective from November 16, 2023

Recent and pending regulation:

In September 2024, the UAE launched its 2024-2027 National Strategy for Anti-Money Laundering, Countering the Financing of Terrorism, and Proliferation Financing (AML/CFT/CPF). This strategy introduces 11 strategic goals, including enhanced risk-based compliance, sustainability of the national framework, and international cooperation. The strategy also focuses on combating emerging threats such as cybercrime and trade-based money laundering.

In line with this strategy, the Emirati government amended some of the provisions in the Federal Decree-Law on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations (Federal Decree-Law No. 20). It enhanced authoritative powers of agencies charged with combating financial crimes and included establishing national and supreme committees to oversee the implementation of the UAE's AML/CTF efforts.

These amendments were announced in August 2024

Conclusion

As platforms and payments continue to evolve, bringing more of our lives online, and fraudsters exploit these opportunities, regulators will continue to create structures that protect consumers. But regulations are only one step in the process.

Where there is regulation, enforcement follows. It has already begun, and it will continue to escalate as lawmakers prioritize protecting consumers.

Regulation enforcement creates a feedback loop: patterns of compliance and violation often inform further adjustments. However, marketplaces and payment providers can choose to see this as an opportunity, rather than a punishment.

It is essential for ecommerce stakeholders to become involved in this process, especially early on, so they can offer an understanding of the industry and help shape regulatory guidelines.

An opportunity to participate in good faith

When regulations are drafted with input from industry experts, they are more likely to align with how the industry operates, minimize unintended consequences, and address key priorities, resulting in beneficial outcomes for businesses and society as a whole.

As one of our customers said recently, “The best advice I can give you is to get to know your regulators and develop a relationship with them. They will invite you to round tables where they discuss how to structure these regulations. And it's imperative that the industry stakeholders – content moderators, analysts, and technologists -- are at those tables.”

By becoming involved in the process, our industry can show good faith and help ensure that new regulations are realistic, balanced, and effective. Everyone in the ecommerce chain has the opportunity to effect positive change.

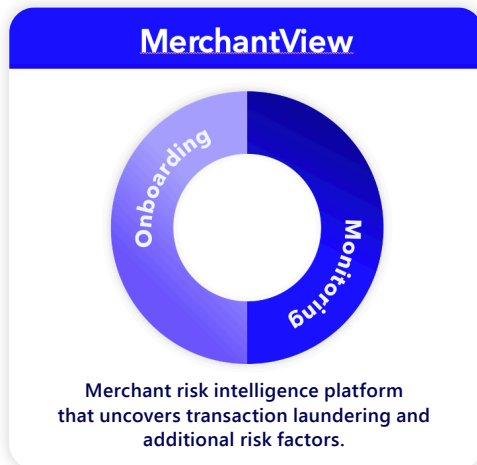
Ultimately, regulations serve a vital purpose: to protect the consumer. It is a goal that demands commitment and effort. And it is a goal worth working toward – together.

Partnering with EverC

EverC is focused on powering safe, scalable growth for the ecommerce ecosystem.

Our team comprises domain experts in risk intelligence, open-source, deep, and dark web, and online fraud detection. EverC is equipped to provide comprehensive risk assessment strategies that can help support regulatory compliance for your organization. Our AI-powered solutions can help institutions or obligated entities protect against fraudulent activities that would potentially risk non-compliance. We also offer robust screening for KYB, sanctions and watchlists, and adverse media, all of which are essential for regulatory compliance throughout the merchant lifecycle.

EverC solutions and services can enable you to protect your business from fraudsters and illicit behavior, and provide a safe, secure experience for your customers.



EverC: securing ecommerce growth with trust and confidence
Learn more at everc.com