

EU Crypto Regulation Explained: An Essential Guide (2025)

Jul 31, 2025 · 15 min read



Crypto and Blockchain



Payment Services

Regulatory Strategy

ESMA

FINMA

BaFin

PSD2

MiFID II

AIFMD

MiCA

Contents

What Is EU Crypto Regulation?

Why EU Crypto Regulation Matters for Fintech and Crypto Startups

Key Frameworks Under EU Crypto Regulation

MiCA (Markets in Crypto-Assets Regulation)

The EU Crypto Travel Rule (Transfer of Funds Regulation)

AMLD5 and AMLD6

DORA (Digital Operational Resilience Act)

E-Money and Payment Rules

Taxation and Reporting (CARF and Beyond)

Who Regulates Crypto in the EU?

Which Businesses Fall Under EU Crypto Regulation?

Crypto Exchanges, Custodians, Wallet Providers

Token Issuers, Stablecoin Projects, and NFT Platforms

DeFi Protocols and Cross-Border Players

Who's Exempt (for now)

Timeline: EU Crypto Regulation in Effect (2024–2026)

Common Compliance Challenges for Crypto Startups

Misconceptions Founders Have About EU Crypto Regulation

Looking Ahead: What's Next for EU Crypto Regulation?

EU crypto regulation is no longer a distant concept or a future concern. It is currently enforceable and already reshaping how crypto and fintech companies operate across the European Union.

With **MiCA**, the **Travel Rule**, and related frameworks rolling out, the **EU** now has one of the most **comprehensive regulatory environments** for crypto assets in the world.

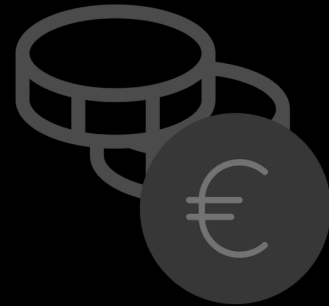
This guide breaks down what EU crypto regulation entails, what matters most to fintech and crypto firms, and how to navigate the evolving rules.



InnReg is a global regulatory compliance and operations consulting team serving financial services companies since 2013. If you need assistance with compliance or fintech regulations, [click here](#).

EU Crypto Regulation Explained

An Essential Guide (2025)



What Is EU Crypto Regulation?

 innreg.com

EU crypto regulation refers to the **set of legal and supervisory frameworks** governing the operation of crypto-asset businesses across the European Union.

It includes the **Markets in Crypto-Assets Regulation** (MiCA), the revised **Transfer of Funds Regulation** (TFR), anti-money laundering directives, and several related laws that affect operational resilience and payment services.

These rules **standardize how crypto businesses register, disclose information, manage risks, and interact with customers** across all 27 member states. They apply to both EU-based firms and non-EU companies offering crypto services within the region.

Why EU Crypto Regulation Matters for Fintech and Crypto Startups

MiCA and related regulations apply to any business offering crypto-related services to users in the EU. That includes embedded finance platforms, neobanks, cross-border payment providers, and hybrid models that combine crypto with securities, loyalty programs, or real-world assets.

As such, global fintechs and crypto firms need to build a compliance infrastructure that scales with their businesses, incorporating **EU crypto regulation** as part of their **compliance strategy**.

Some firms manage compliance in-house, while others rely on outside specialists who already understand how to operationalize EU regulatory expectations within fast-moving fintech environments.

Integrating regulatory compliance into product and engineering early is no longer optional. InnReg partners with fintech innovators to help them align their business models with EU crypto rules. [Click here](#) to learn more.

Key Frameworks Under EU Crypto Regulation

EU crypto regulation is not a single law. It is a coordinated framework comprising several interlocking rules, some crypto-specific, others broader in scope but relevant.

Each regulation covers a different area: **market conduct, consumer protection, AML, operational resilience, payments, and tax reporting**. Together, they create a regulatory perimeter that crypto and fintech businesses can't afford to overlook.

The sections below provide a high-level overview of the major frameworks shaping the EU crypto compliance environment as of 2025:



MiCA (Markets in Crypto-Assets Regulation)

MiCA is the foundation of EU crypto regulation. It creates a unified legal framework for crypto-asset service providers (CASPs) and token issuers across all 27 EU member states.

For fintech companies operating in or targeting the EU, MiCA is likely the first, and most important, regulation to address.



Who **MiCA** applies to:

-  **Crypto exchanges and trading platforms**
-  **Custodial wallet providers**
-  **Token issuers (excluding securities)**
-  **Stablecoin projects**
-  **Crypto advisors and brokers**

It does not cover NFTs (unless they're fractionalized or fungible), **DeFi protocols** with no identifiable intermediary, or tokenized traditional financial instruments (which fall under **MiFID II** and other frameworks).

What MiCA Means for Crypto Businesses

MiCA introduces **operational, disclosure, and risk management requirements** that apply to most crypto-asset service providers (CASPs) and token issuers in the EU.

Whether a firm is launching a new product or scaling an existing one, its obligations include:

- **Licensing and Registration Requirements:** CASPs must apply for authorization through a National Competent Authority (NCA). Approval requires a compliant business model, capital adequacy, internal governance, and clear AML controls.
- **White Paper and Disclosure Rules:** Issuers must publish a MiCA-compliant white paper before offering or listing tokens. The document must disclose risks, token features, and project details. Marketing materials must match the white paper.
- **Governance, Risk, and Consumer Protection:** Firms need documented governance structures, fit-and-proper leadership, and user protection processes. This includes transparent pricing, client asset safeguards, and a formal complaint-handling process.
- **Market Abuse and Insider Trading Provisions:** MiCA prohibits insider trading, price manipulation, and false market signals. CASPs must monitor for abuse and report suspicious activity, following similar standards to those in traditional financial markets.
- **Stablecoin Rules and Reserve Requirements:** Issuers of **stablecoins** (ARTs and EMTs) must maintain full reserves, offer redemption rights, and meet liquidity and reporting obligations. Larger tokens are subject to additional supervision by the European Banking Authority (EBA).

MiCA introduces new regulatory thresholds that fintech teams must account for from the outset. For fintech teams, this means evaluating product structure early. A crypto-powered feature, such as embedded custody or **token issuance**, could trigger licensing requirements.

The EU Crypto Travel Rule (Transfer of Funds Regulation)

The **EU Crypto Travel Rule** extends traditional **anti-money laundering (AML) requirements** to crypto transfers. Under the revised Transfer of Funds Regulation (TFR), crypto-asset service providers (CASPs) must collect and transmit identifying information for both the sender and the recipient of any crypto transaction, regardless of amount.

Since the rule took effect on December 30, 2024, any business facilitating crypto transfers, whether directly or through white-label arrangements, must assess its current infrastructure to meet regulatory obligations.

Key **compliance requirements** of TFR include:

- **Data Requirements for Crypto Transfers:** CASPs must collect and transmit key identifying information for both parties in any crypto transaction. Required fields include the originator's name, wallet address, and ID number, as well as the beneficiary's name and their wallet address.
- **Dealing with Unhosted Wallets:** Transfers involving unhosted wallets are allowed. However, for amounts exceeding €1,000, CASPs must verify ownership of the wallet, typically through authentication methods such as message signing.
- **Implementation Timeline and Compliance Tools:** The rule is in effect, and CASPs are expected to meet real-time data-sharing obligations immediately. Many use Travel Rule vendors or integrated compliance solutions to handle transmission, recordkeeping, and wallet screening.

For fintechs and crypto firms with fast-moving development cycles, it's essential to assess early how transactional features map to Travel Rule triggers. Building compliance into architecture from the start is often more efficient than retrofitting controls later under regulatory pressure.

Speak to our experts about defining and managing **your regulatory compliance path**

[Contact Us](#)

AMLD5 and AMLD6

Before MiCA and the Travel Rule, crypto businesses in the EU were already subject to anti-money laundering obligations under **AMLD5** and **AMLD6**. These directives drew certain crypto activities into the regulatory perimeter, and they remain in effect.

AMLD5, effective since 2020, was the EU's first step in regulating crypto. It required two categories of crypto businesses to register with national authorities and implement full AML programs:

1. Fiat-to-crypto exchanges
2. Custodial wallet providers

These firms must conduct customer due diligence (**CDD**), monitor transactions, and report suspicious activity, similar to traditional financial institutions.

AMLD6 expanded enforcement by:

- Defining a harmonized list of predicate offenses
- Extending criminal liability to senior management
- Increasing penalties for non-compliance

It also improved cooperation across EU jurisdictions, making cross-border investigations easier.

If you are operating a regulated crypto business under AMLD5, you're already expected to have:

- A KYC process with risk-based tiers
- Internal AML policies and training
- A designated MLRO (money laundering reporting officer)
- Reporting capabilities for STRs/SARs

Note that **MiCA** and the updated **Travel Rule** are built on this foundation. They **do not replace AMLD** obligations but add to them.

DORA (Digital Operational Resilience Act)

The **Digital Operational Resilience Act (DORA)** is the EU's framework for managing IT and cybersecurity risks across the financial sector. As of **January 2025**, it **applies** to crypto firms licensed under **MiCA**.

DORA mandates that regulated entities:

- Identify and assess ICT risks
- Implement business continuity and disaster recovery strategies
- Test systems regularly, including penetration and scenario testing
- Monitor third-party service providers, especially cloud and data vendors

DORA also **introduces** obligations around **incident reporting**. Major IT incidents must be reported to regulators promptly, along with the root cause and remediation plans.

Compliance with DORA requires structured documentation, internal controls, and repeatable testing, as ad hoc processes do not meet the standard.

As such, fintech firms should treat DORA as a core component of their compliance function. Some outsource this work to compliance teams with experience in both crypto infrastructure and EU regulatory frameworks.

See also:

- [Florida Money Transmitter License: Checklist and Requirements](#)
- [Series 27 License: Responsibilities, Exam, and Compliance](#)
- [Investment Advisor Regulation: SEC and State Rules for RIAs](#)

E-Money and Payment Rules

MiCA simplifies crypto regulation, but it **does not replace e-money or payments law**. If a product falls into either category, a firm must assess whether dual licensing or structural changes are required.

Under MiCA, fiat-referenced stablecoins are categorized as **E-Money Tokens (EMTs)**. If a token is pegged 1:1 to a currency, such as the euro, it may need to be licensed not only under MiCA but also as an Electronic Money Institution (**EMI**).

Dual licensing is required when:

- Users can redeem tokens at face value
- The token is used broadly for payments
- The project functions like a stored-value system

Furthermore, if a platform facilitates payment initiation, fund transfers, or account access, **PSD2** might also apply.

Examples include:

- Platforms enabling crypto-to-fiat payouts
- Wallets with fiat on-ramps or off-ramps
- Services that move user funds between accounts

In these cases, the underlying rails and user experience may resemble those of regulated payment services, triggering PSD2 obligations, such as strong customer authentication (SCA), conduct rules, and reporting requirements.

Designing around dual licensing or payments triggers? [Learn more](#) about tokenized securities →



Need help with blockchain compliance?

Fill out the form below and our experts will get back to you.

First Name *

John

Last Name *

Doe

yourname@company.com

Company Name

Your Company

Message *

Enter your message

By submitting this form, you consent to be added to our mailing list and to receive marketing communications from us. You can unsubscribe at any time by following the link in our emails or contacting us directly.

SPEAK TO AN EXPERT

Taxation and Reporting (CARF and Beyond)

Tax compliance is not technically part of **MiCA**, but it's closely adjacent and increasingly complex to separate from regulatory planning. As crypto matures, tax transparency is becoming a core expectation across the EU.

The **Crypto-Asset Reporting Framework (CARF)** is an **OECD** initiative adopted by the EU in 2023. It requires crypto-asset service providers (CASPs) to **report user holdings and transactions** to national tax authorities, similar to how banks report under the **Common Reporting Standard (CRS)**.

CARF is designed to encompass:

- Capital gains from crypto trading
- Income from staking, lending, or token rewards
- Cross-border transfers and undeclared holdings

The framework applies to individuals and entities and is designed to prevent tax evasion through the use of offshore wallets or platforms.

CASPs operating in the EU, or serving EU customers, need to:

- Collect tax-relevant user data
- Report trades, transfers, and crypto-based income
- Identify customer residency and legal status

This introduces new compliance layers, including **customer classification**, **transaction labeling**, and coordination with national authorities. Technical implementation will likely be standardized across member states, but timelines and formats may vary.

Who Regulates Crypto in the EU?

Crypto regulation is a **multi-layered system** that combines national oversight with EU-level supervision. Understanding the regulatory landscape is essential for fintech and crypto companies to avoid gaps in licensing, compliance, and reporting.

The most important regulatory bodies include:

National Competent Authorities (NCAs)

Each EU member state has a financial regulator, its **National Competent Authority (NCAs)**, that is responsible for licensing and supervising crypto firms under MiCA.

Examples of NCAs include **BaFin in Germany**, **AMF in France**, **CNMV in Spain**, and **CONSOB in Italy**.

Applicants must submit their MiCA license application to the relevant NCA in their chosen Member State. Once authorized, the NCA serves as the primary supervisory authority, overseeing ongoing obligations, including audits, regulatory disclosures, and incident reporting.

ESMA, EBA, ECB, and AMLA

At the EU level, several authorities play distinct roles:

- **ESMA (European Securities and Markets Authority):** Develops technical standards, coordinates supervision across NCAs, and maintains public registers (including blacklists of non-compliant firms).
- **EBA (European Banking Authority):** Focuses on stablecoin issuers and prudential standards. Oversees asset reserves, liquidity frameworks, and governance of “significant” tokens.
- **ECB (European Central Bank):** Monitors financial stability. Can intervene if stablecoins pose a threat to monetary policy or payment systems.
- **AMLA (Anti-Money Laundering Authority):** Launching in 2026, AMLA will directly supervise the largest cross-border crypto firms for AML/CFT compliance.

Although firms primarily interact with their designated NCA, they should anticipate involvement from EU-level authorities, particularly during the licensing process or when operating across multiple Member States.

Financial Intelligence Units (FIUs)

Financial Intelligence Units (FIUs) are national agencies responsible for receiving and analyzing reports of suspicious financial activity. Under AMLD5 and AMLD6, crypto-asset service providers (CASPs) registered or licensed in the EU are required to report such activity directly to the FIU in their home jurisdiction.

Each EU member state operates its own FIU. While the specific structure may vary, their role is consistent: to support anti-money laundering and counter-terrorist financing enforcement by identifying potential financial crime.

Crypto firms authorized under MiCA are expected to integrate this reporting into their broader AML programs. The relationship with FIUs is continuous, and reporting obligations apply not just at onboarding or during large transactions, but throughout the entire customer lifecycle.

We help fintech innovators like you
succeed in regulated markets

Get a Free Consultation

Which Businesses Fall Under EU Crypto Regulation?

EU crypto regulation is activity-based, not company-type-based. That means whether a firm qualifies as a “crypto business” depends on what it does, not how it labels itself. Many fintech companies may fall under MiCA and related frameworks, even if crypto is not their core offering.

Regulated activities include custody, trading, issuance, and exchange of crypto-assets, as well as advisory and execution services. If a business provides one or more of these services in the EU, it is likely within scope. Non-EU firms targeting EU users also fall within the scope of MiCA, regardless of their headquarters.

The most common affected business types include:

Crypto Exchanges, Custodians, Wallet Providers

These are the most obvious in-scope businesses under MiCA. Centralized exchanges must register as CASPs and comply with rules on licensing, transparency, and market conduct.

Custodial wallet providers, those holding private keys on behalf of users, also fall under the same obligations.

Both categories are subject to AMLD5, the EU Travel Rule, and MiCA's requirements around client asset protection, operational resilience, and disclosure. Most will need to maintain internal controls comparable to those of traditional financial institutions.

Token Issuers, Stablecoin Projects, and NFT Platforms

Anyone issuing crypto-assets or tokens to the public in the EU **must** prepare and **publish a white paper** in line with MiCA.

Stablecoin issuers face additional scrutiny, including reserve management, redemption rights, and liquidity thresholds.

NFT platforms are generally excluded unless the NFTs are fractionalized or structured in a way that resembles financial instruments. If that's the case, the issuer may fall under MiCA or even securities law, depending on the specifics.

DeFi Protocols and Cross-Border Players

Fully **decentralized protocols** with no identifiable operator are currently **outside the scope** of MiCA. However, most projects are not fully decentralized in practice. If a company builds, maintains, or markets a DeFi interface, that activity may bring it within regulatory reach.

For firms operating from outside the EU, engaging EU users triggers cross-border compliance obligations, as MiCA has an extraterritorial effect.

Marketing crypto services in the EU or onboarding EU users without local registration could lead to enforcement.

See also:

- [Understanding FINRA Sanction Guidelines: What You Must Know](#)
- [What Is FINRA CRD? Guide to the Central Registration Depository](#)
- [Florida Money Transmitter License: Checklist and Requirements](#)

Who's Exempt (for now)

As of 2025, certain actors and activities fall outside MiCA, including:

- Central banks and public institutions
- NFTs (when truly unique, non-fungible, and not part of a large series)
- Crypto-assets that qualify as financial instruments under MiFID II
- Protocols without a central operator or control structure

However, it is essential to note that exemptions are narrowly defined, and the list may be subject to change over time.

Regulators are already exploring future rules for **DeFi**, **NFTs**, and **algorithmic stablecoins**. As such, businesses in these evolving segments should monitor policy shifts and prepare for possible new obligations.

Understanding the regulatory perimeter early is critical. Some models clearly require licensing. Others sit in gray areas. In both cases, compliance obligations may arise well before launch, particularly for firms onboarding EU users, marketing within the EU, or developing infrastructure linked to crypto transactions.

Get help for your
fintech startup



Talk To Compliance Experts

Timeline: EU Crypto Regulation in Effect (2024–2026)

EU crypto regulation is already active, but not all parts take effect at once.

These are the EU crypto regulation key milestones:

- **MiCA:** Titles III and IV (covering stablecoins) took effect on June 30, 2024. The remainder of MiCA, governing CASP licensing, disclosures, and conduct, came into force on December 30, 2024.
- **Transfer of Funds Regulation (Travel Rule):** The Travel Rule became enforceable on December 30, 2024, with no transitional grace period.
- **DORA (Digital Operational Resilience Act):** Applies from January 17, 2025, to all financial entities regulated under EU law, including crypto firms licensed under MiCA.
- **CARF (Crypto-Asset Reporting Framework):** Implementation timelines vary by Member State, but most are targeting adoption by 2026, following EU-level ratification in 2023.

While the **Travel Rule** has no grace period, **MiCA** allowed transitional arrangements at the national level. Some Member States have published specific paths for temporary authorization. Others expect full compliance from the outset.

Operating without proper authorization past these deadlines can lead to enforcement, including fines, shutdown orders, and blacklisting across the EU.

Crypto and fintech businesses should treat these timelines as hard cutoffs for internal planning, given the risk of regulatory action. In practice, that means submitting licensing applications early, building internal compliance functions, and

integrating controls with product and engineering roadmaps well in advance.

Common Compliance Challenges for Crypto Startups

With EU crypto rules in force, firms must adopt a forward-looking approach to regulatory planning, rather than relying on reactive adaptations.

These are the most frequent challenges businesses face:

- **Licensing Complexity:** Firms must determine how their business model aligns with one or more regulated activities. This requires legal analysis, internal documentation, and coordination with the relevant National Competent Authority. Operating in multiple Member States adds another layer of complexity.
- **AML/KYC Program Gaps:** Many early-stage crypto firms underestimate the operational burden of AML compliance. Basic onboarding tools fall short of EU expectations. Regulated entities must implement risk-based due diligence, transaction monitoring, and a straightforward escalation process for identifying and addressing suspicious activity. Without these elements, approval may be delayed or denied outright.
- **Product-Market Fit vs. Regulatory Fit:** Some features that drive growth (e.g., embedded wallets, token issuance, or payment-like functionality) also trigger regulatory scrutiny. Businesses often discover too late that product architecture requires licensing, reporting, or dual oversight. Identifying these dependencies early helps avoid costly redesigns or market restrictions.
- **Tech Debt and Compliance Infrastructure:** Manual processes and isolated tools rarely scale. Regulators expect auditable systems with documented roles, access controls, and regular testing. Retrofitting compliance infrastructure after launch is often more disruptive and expensive than building it into operations from the start.

As EU crypto regulations mature, firms that treat regulatory planning as a parallel track to product development are better positioned to scale, secure partnerships, and withstand scrutiny.

Misconceptions Founders Have About EU Crypto Regulation

Despite the growing clarity surrounding **EU crypto regulation**, some common misconceptions persist. These assumptions can lead to misaligned strategies, delayed approvals, or unintentional violations.



Common misconceptions about **EU Crypto Regulation**:

“We’re not in the EU, so it doesn’t apply.”

“DeFi and NFTs are out of scope.”

“We’ll get compliant later.”

(And more)

“We’re not in the EU, so it doesn’t apply.”

MiCA and other EU crypto frameworks apply **based on activity, not location**. If a firm targets EU users, whether through marketing, onboarding, or product access, it is likely subject to EU jurisdiction. Geofencing and disclaimers are often insufficient if the business model involves cross-border interactions.

“DeFi and NFTs are out of scope.”

True decentralization may fall outside the scope of MiCA for now, but **most DeFi** projects **involve** identifiable **intermediaries**, such as teams managing interfaces, liquidity, or upgrades. Similarly, NFT projects can trigger regulation if assets are fractionalized, bundled, or resemble financial instruments. Relying on current exclusions without legal review is risky.

“We’ll get compliant later.”

Waiting until launch or scale to address regulation is a common but costly mistake. Licensing timelines, technical integration, and internal controls often take months to implement. By the time the need becomes urgent, retrofitting compliance may already be delaying partnerships, banking access, or user onboarding.

Other false assumptions:

Founders sometimes believe that white-label platforms shift responsibility to vendors, that small user bases exempt them from scrutiny, or that early-stage status grants flexibility. None of these assumptions hold under current EU rules. Regulatory exposure exists from the moment a product is accessible to EU users.

Looking Ahead: What’s Next for EU Crypto Regulation?

EU crypto regulation will not remain static. Policymakers have already signaled future expansions to address emerging technologies and close perceived gaps in the current regulatory perimeter.

The following areas are already under discussion and may shape the next phase of EU crypto regulation:

- **Regulation of DeFi, NFTs, and AI-Driven Platforms:** DeFi activity with identifiable developers, user interfaces, or governance mechanisms may eventually fall under bespoke rules or modified MiCA provisions. NFT platforms that fractionalize assets or offer financial returns may also face classification as financial instruments. The growing use of AI in trading, lending, and compliance functions could prompt new supervisory expectations, particularly around transparency and model risk.
- **Possible Changes in MiCA Scope:** European regulators are actively assessing whether these areas warrant additional oversight. Projects with ambiguous or hybrid models may soon be subject to review.
- **Role of the Digital Euro:** The European Central Bank's Digital Euro initiative is likely to impact the regulation of private-sector stablecoins and wallets. If adopted, it could introduce additional technical and operational requirements for any fintech interacting with the central bank's digital currency infrastructure. That includes payment routing, settlement, identity verification, and fraud monitoring protocols.

As **EU crypto regulations** continue to evolve, firms must treat compliance as an integrated function, rather than an afterthought. That means embedding regulatory thinking into product development, engineering, and go-to-market strategies from the outset. Delays in compliance can have real consequences, including disruptions to operations, market credibility, or financing.

Whether refining a business model, entering the EU market, or reworking product architecture, involving regulatory experts early is a practical advantage. Staying ahead of EU crypto regulation is not just about meeting the rules; it is about building a business that can grow within them.

How Can InnReg Help?

InnReg is a global regulatory compliance and operations consulting team serving financial services companies since 2013.

We are especially effective at launching and scaling fintechs with innovative compliance strategies and delivering cost-effective managed services, assisted by proprietary regtech solutions.

If you need help with blockchain compliance, reach out to our regulatory experts today:

First Name *

John

Last Name *

Doe

Email *

yourname@company.com

Company Name

Your Company

Message *

Enter your message

By submitting this form, you consent to be added to our mailing list and to receive marketing communications from us. You can unsubscribe at any time by following the link in our emails or contacting us directly.

Regulatory Verticals

Broker-Dealers
RIAs
ATS
MSBs
Money Transmitters
Currency Exchanges
Check Cashers
Lenders
Consumer Lenders
Mortgage Lenders
Commercial Lenders
Money Brokers
Credit Builders
Payment Services
PI
EMI
Portals
Digital Banking
Crypto
Forex Brokers
Banks

Functions

Policies and Procedures
Regulatory Exams
Regulatory Strategy
Bank Partnerships
Licensing
Staffing
Supervision
Surveillance
Advertising
Communications
Recordkeeping
Onboarding
AML
Cybersecurity
Vendors
Training
Filings

Roles

CCO
CEO
AMLCO
FinOp
Series 4
Series 7
Series 24
Series 53
Series 79
PFO
POO
Research Principal
Securities Trader Principal
Government Securities Principal

Regulators

FINRA
SEC
FTC
CFTC
NFA
FinCEN
OFAC
MSRB
SIPC
OCC
FDIC
CFPB
FCA
ESMA
MAS
HKMA
ASIC
FINMA
BaFin

Frameworks

FINRA Rules
SEC Rules
Exchange Act of 1934
BASEL III
GDPR
BSA
Reg BI
USA Patriot Act
UDAAP
FCRA
ECOA
FATF
PSD2

AIFMD
MiCA
TILA
EFTA
FDCPA
GLBA

Subscribe for Compliance Insights

First Name

John

Last Name

Doe

Email

yourname@company.com

SIGN UP

Related Articles

Understanding FINRA Sanction Guidelines: What You Must Know

Broker-Dealers RIA's ATS

Sep 29, 2025 · 19 min read

What Is FINRA CRD? Guide to the Central Registration Depository

Broker-Dealers

Sep 28, 2025 · 10 min read

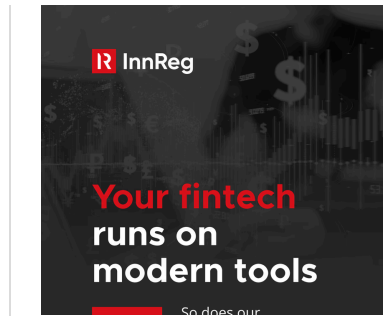
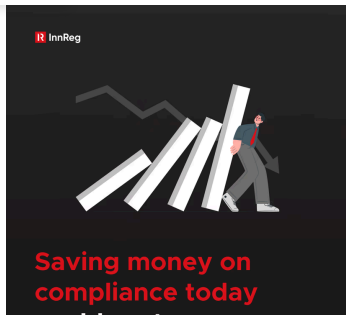
Florida Money Transmitter License: Checklist and Requirements

MSBs Money Transmitters

Sep 26, 2025 · 18 min read

Featured LinkedIn Posts

COOKIE SETTINGS



WHO WE SERVE

By Vertical

Broker-Dealers
Registered Investment Advisors (RIA)
Alternative Trading Systems (ATS)
Money Services Businesses (MSBs)
Lenders
Payment Services
Crowdfunding Portals
Digital Banking
Crypto and Blockchain
Forex Brokers
Banks

LICENSING SERVICES

By Vertical

Broker-Dealer Registration
Investment Advisor Registration
MSB Registration
Money Transmitter License
Currency Exchange License
Check Casher License
Lender License
Payment License
Crowdfunding Portal Registration
Crypto License
Forex Broker License

COMPLIANCE SERVICES

Compliance Consulting Operations

Regulatory and Product Strategy
Suspicious Activity Monitoring
Registrations and Licensing
Crossing Funding and Transfer Supervision
Compliance Workflow
Trading Supervision
Partnerships Support
Electronic Books and Records Management
Policies and Procedures Development
KYC & AML Programs
Electronic Communications Reviews
Cybersecurity Program Development
Advertising and Marketing Reviews
Regulatory Exams and Audit
Risk Management Program
Gap Analysis and Risk Assessments
Client Onboarding

By Role

Outsourced Chief Compliance Officer (CCO)
Outsourced Financial Operations Principal (FINOP)
Outsourced Supervisory Principals

RESOURCES

Learn

Blog
Case Studies
Regulatory Updates
FINRA Rules

Downloads

Ebooks
Spreadsheets

ABOUT INNREG

Company

Who We Are
Why InnReg
Careers
Referral Program
Contact Us

Legal

Privacy Policy
Terms of Use



© 2025 InnReg LLC

305-908-1160



9100 S Dadeland Blvd
Suite 1500
Miami, Florida 33156

COOKIE SETTINGS

The content provided on this website is for informational purposes only and does not constitute legal, investment, tax, or other professional advice. InnReg LLC is not a law firm, tax advisor, or regulated financial institution. Viewing this site or contacting InnReg does not create a client relationship. Results described in case studies or testimonials may not be typical and do not guarantee future outcomes. Tools, spreadsheets, or guides available on this site are provided for illustrative purposes only and should not be relied upon without professional guidance. Any links to third-party websites are provided for convenience and do not constitute endorsement or responsibility for their content. The information on this site may not be applicable in all jurisdictions. While we strive to provide accurate content, we make no representations as to its completeness or timeliness. Some visual assets on this site are sourced from Freepik.