CIRCLE

Navigating Blockchain Compliance

A Guide for Enterprises & Developers

Contents

Introduction

This whitepaper is intended as a support aide for Circle's partners across the blockchain services ecosystem. From builders in early stage startups to compliance professionals in large enterprises, we want to provide helpful guidance on navigating your blockchain compliance journey to build in a safe and trusted ecosystem.

This whitepaper highlights the potential of compliance as a key value add for your customers and outlines why Circle emphasizes trust and compliance in our own operations. Later sections provide high-level guidance on identifying your requirements and some of the key questions to understand the potential regulatory obligations of your business. We conclude with some of Circle's plans to empower builders to integrate compliance best practices into your services to help satisfy compliance requirements.

Background

Various forms of laws, rules and regulations have applied to financial products and services offerings for centuries. The same is true for stablecoins, wallets, custody and other utility use cases across the blockchain ecosystem.

Awareness of—and adherence to—applicable regulatory requirements is a critical step in navigating the often complex landscape required to offer innovative products and services. Failure to do so can have detrimental consequences to consumers, investors and the global financial services ecosystem, along with the companies that offer these services.

Throughout our 10+ year journey to create a more open financial system for everyone, Circle and the broader ecosystem have benefitted from our compliance-first approach. Our commitment to building long-lasting partnerships and developing bespoke compliance solutions to meet nuanced requirements along the way has helped Circle offer a broad range of safe and trusted products and services across many jurisdictions.

While this guide serves as a resource, it should not be considered legal advice. Please consult legal counsel when evaluating compliance requirements as they relate to your unique business model and the jurisdictions in which you operate.

PART 1

Compliance as a Value-Add

Adhering to the laws, rules, and regulations applicable to your business is more than a check-the-box exercise—it's an ongoing commitment.

Blockchain services face rigorous scrutiny from a broad range of stakeholders, including regulators, banking partners, payment service providers and customers, among others. Failing to meet the expectations of any of these stakeholders could limit the success of your launch or hurt your business's ability to operate. Prioritizing compliance and investing in the right compliance solutions minimizes these risks and serves as a valuable differentiator. It separates businesses that are committed to their customers and the long-term growth and success of their products and services from those that take shortcuts.

Consumers have grown very familiar with the various compliance steps required to open a bank or brokerage account, such as providing evidence of identity and agreeing to the terms of a privacy policy. In fact, they expect to navigate these steps when they engage with a new product or service. Rather than being a hindrance, failure to offer these onboarding checkpoints can lead to a loss of trust and potentially inhibit the customer acquisition process.

Investing in appropriate compliance solutions does more for your business than meeting baseline regulatory obligations. Your business's approach to compliance could make all the difference when it comes to customer acquisition and retention, the level of regulatory scrutiny you are subjected to and the overall success of your project.

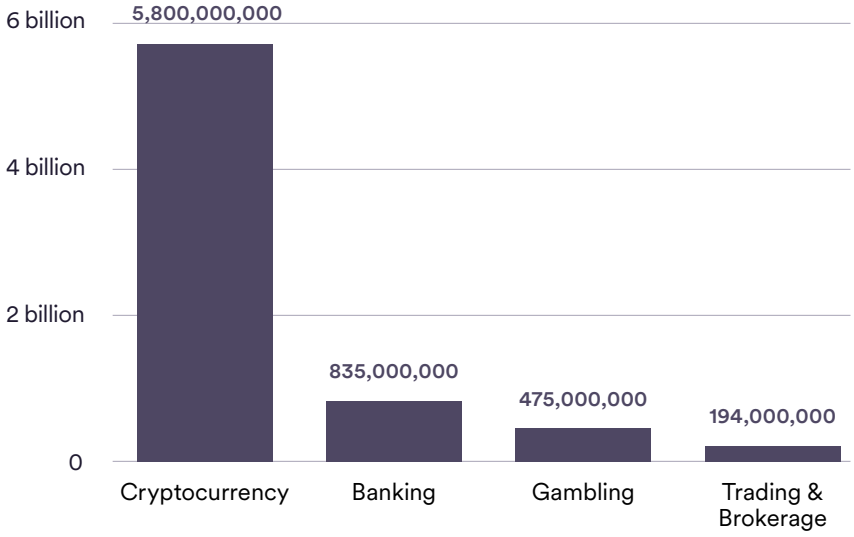
Particular areas of focus generally include:

Legal & Regulatory Compliance

Non-compliance with these regulations can result in disciplinary actions from regulators, which may include severe monetary fines, loss of licensure and other penalties that can impact a business's ability to operate. There are numerous laws,

rules, and regulations in the various jurisdictions designed to safeguard the integrity of the financial system by setting forth a series of compliance obligations that aim to prevent money laundering, terrorist financing, and protect consumers from unfair practices. While anti-money laundering and sanctions laws receive the most attention in the blockchain space, it's important to consider all areas of a compliance program, including prudential, consumer protection, anti-bribery and corruption, and payments regulatory compliance. A business's ability to meet these obligations are of particular interest to regulators since they promote market transparency, financial stability, and safeguard the interests of customers. Regulators routinely monitor the timely submission of the required regulatory reports, including but not limited to, periodic returns, audited financial statements, suspicious activity reports, notifications of material changes as well as breaches.

Industry Sectors with Top AML Fines Incurred 2023 (in USD)[1]



Protecting User Data

Privacy and data protection requirements generally apply in any scenario where personal data is processed, which is usually the case in the provision of financial services products and services. Non-compliance can likewise have a number of consequences, including significant financial penalties, legal action, and reputational damages. There are extensive privacy and financial regulatory frameworks that apply including the General Data Protection Regulation (GDPR), Gramm-Leach Bliley Act (GLBA), and a patchwork of privacy laws that have been passed both in the US and around the globe. These laws outline obligations on businesses and rights in favor of individuals, which include stringent data security requirements, rigid data processing and protection requirements, data subject rights and breach notification obligations.

1. Cameron, Sarah. "The Biggest AML Fines in 2023." ComplyAdvantage, 18 May 2024, complyadvantage.com/insights/aml-fines-2023/.

Privacy and data security regulations may apply to companies located outside the jurisdiction issuing the regulation offering protections to the individuals that reside in that jurisdiction. In addition these obligations can extend to the vendors or service providers even if these entities are not directly regulated by these laws.

Building Trust and Credibility

Complying with stringent and rigorous frameworks demonstrates a commitment to ethical business practices and customer protection. This helps assure customers that their financial transactions and personal information are secure and their rights as consumers are protected. These safeguards promote trust and credibility. This is essential in the blockchain services ecosystem, where decentralized technologies rely on community participation and collaboration.

Avoiding Reputational Damage

Reputational damage caused by non-compliance—whether it be regulatory enforcement actions, customer complaints, or media articles—can have a severe and long-lasting impact. Damaged credibility and trust can result in the loss of strategic partnerships, customers, and investors as well as future revenue, profit and growth. Devoting the time and resources to understand compliance requirements and meet the compliance obligations will help to avoid adverse reputational impact.

PART 2

Circle's Case for Building Trust with Compliance

Compliance is woven into every aspect of Circle's operations, and it is a bedrock component of building trust and growing our business.

Our compliance-first culture is critical to building global, frictionless value-exchange through compliant stablecoins, secure message protocols, and other open-source, compliant, and trusted blockchain-based solutions. Compliant solutions promote transparency and trust with regulators and other governing authorities, further solidifying Circle's reputation in this space and providing stability in the emerging regulatory landscape.

Strong Compliance and Risk Culture

Circle's senior management prioritizes and promotes our culture of compliance through ongoing involvement and support in compliance initiatives. Senior leader engagement fosters a strong compliance and risk-based culture which is embedded throughout the business, including product design, customer onboarding, and customer engagement. Circle employees understand their compliance responsibilities and uphold our values, beliefs, and behaviors.

Transparency and Stability

USDC reserve holdings are fully disclosed on a weekly basis, along with associated mint/burn flows and key externally facing policies. Additionally, a Big Four accounting firm provides monthly third-party assurance that the value of USDC reserves are greater than the amount of USDC in circulation. The reports are prepared according to attestation standards set out by the American Institute of Certified Public Accountants (AICPA). This industry-leading level of transparency is designed to instill confidence in customers we serve, as well as regulators and supervisory agencies.

Proven Track Record

Circle has built a reputation for being trustworthy and compliant. As the sole issuer of USDC, Circle is no stranger to regulation. Circle has obtained and maintains licenses as a money transmitter in 46 U.S. states and territories, along with key regulators Singapore and France—all of whom routinely examine or inspect us. We were the first New York Bitlicensee, and the first global stablecoin issuer to achieve compliance with the Markets in Crypto-Assets (MiCA) regulatory framework, one of the world's most comprehensive regulatory regimes for digital assets.[2] Circle's real-world experience operating in a highly regulated space, afforded us opportunities to engage directly with regulators and supervisory agencies and build a strong rapport. These relationships have been instrumental in developing Circle's core compliance infrastructure from the very beginning. Circle is constantly building and evolving best in class compliance technology to enable the growth of global products and services and satisfy regulatory bodies around the world.

Commitment to Security and Privacy

Circle prioritizes the security and privacy of our customers' data. We follow industry best practices and comply with data protection regulations where required. Leveraging the cybersecurity framework established by the National Institute of Standards and Technology (NIST), Circle's information security program is designed to identify ongoing risks, protect critical infrastructure, detect threats and attacks, respond to cybersecurity events, define recovery plans to mitigate the impact of events, and report events, where required. Circle is certified to the Payment Card Industry (PCI) standards; testing and review of detection capabilities are subject to routine audits. Circle issues Service Organization Controls (SOC 1 and SOC 2) Type 2 reports, which are audited annually by an independent audit firm. These reports provide assurance regarding the design and operational effectiveness of Circle's controls, ranging from minting and burning, to security privacy controls. Both SOC 1 and SOC 2 reports are prepared in accordance with the reporting standards established by the American Institute of Certified Public Accountants (AICPA).

2. For more detail regarding Circle's licenses, see: https://www.circle.com/en/legal/licenses.

PART 3

Guidance on Requirements Journey

As an emerging industry utilizing blockchain technology, operating in the blockchain space presents unique regulatory challenges and obligations, compounded by jurisdictional requirements that vary by country.

Less established, newer business/industry types (e.g., miners, decentralized autonomous organizations [DAOs], non-fungible tokens [NFTs], unhosted wallet providers, decentralized finance [DeFi], etc.) may have yet to be captured in an existing regulatory regime/framework, making their regulatory status less clear. While some jurisdictions have taken steps to impose regulatory requirements on businesses, others have not, and still others have attempted to leverage existing regulatory regimes, resulting in a global patchwork of regulation. There is little uniformity across jurisdictions that do regulate these activities, and the application of regulations is often highly dependent on the specifics of a company's business model.

Accordingly, it is strongly advised that any business wishing to operate in the blockchain ecosystem first seek its own independent legal guidance.

Some helpful questions to consider as you start to understand the potential regulatory obligations of your business include:

What jurisdictions and regulatory frameworks are relevant to you?

- Where is your business registered or domiciled?
- What jurisdiction(s) does the business currently operate in or plan to operate?
- Where are your customers going to be located?
- Does the jurisdiction have a regulatory framework in place for the products/services that your business supports?

What types of customers do you service?

- Consumers
- Financial institutions
- Business entities

What are their industry types?

- Asset managers, hedge funds
- Banks and credit unions
- Crypto automated teller machine operator
- Crypto exchanges
- Crypto investing and lending
- Crypto on-ramps/retail OTC trading
- Crypto wallets and custodians
- Peer-to-peer payments/money transmission
- Marketplaces/E-Commerce

How are your customers regulated?

What type of digital assets do you interact with?

- Cryptoassets
- Stablecoins
- Non-fungible tokens
- Central Bank Digital Currencies
- Security tokens
- Utility tokens

How do you interact with these digital assets?

- Exchange between digital assets and fiat currencies
- Exchange between one or more forms of digital assets
- Transfers of virtual assets
- Safekeeping and/or administration of digital assets

This is not an exhaustive list of considerations. There are multiple variations that could result in a wide array of legal, regulatory and compliance options to be factored into any future business offering.

PART 4

Satisfying compliance requirements

After identifying regulatory obligations and performing a gap assessment, the journey to build a compliance program with the infrastructure that covers the key compliance and risk domains tailored to your business model can begin.

Circle is committed to helping ecosystem partners around the world establish best-in-class compliance programs. This commitment is part of our vision to foster a safe and secure operational environment and contribute to a more prosperous global economy for everyone.

An outcome of our vision is the development of educational compliance content and technical solutions, empowering builders to integrate compliance best practices into their services. As a foundational step in this leadership initiative, Circle is launching Compliance Engine for Programmable Wallets. Compliance Engine enables businesses to protect their users and meet regulatory requirements with customizable, programmatically enforced compliance checks for their blockchain transactions. Visit www.circle.com to learn more about our compliance solutions, or contact our team here.

Services are provided by Circle Technology Services, LLC (“CTS”). Services do not include financial, investment, tax, legal, regulatory, accounting, business, or other advice. CTS is only a provider of software and related technology and is not engaged in any regulated money transmission activity in connection with the services it provides. For additional details, please click here to see the Circle Developer terms of service.