Developer Responsibilities: Market Integrity and Application Code Risks

Chainlink Data Feeds provide access to highly secure, reliable, and decentralized real-world data published onchain. The assets priced by Chainlink Data Feeds are subject to market conditions beyond the ability of Chainlink node operators to control, as such developers are responsible for ensuring that the operation and performance of Chainlink Data Feeds match expectations.

When integrating Chainlink Data Feeds, developers must understand that the performance of feeds is subject to risks associated with both market integrity and application code.

- Market Integrity Risksare those associated with external market conditions impacting price behavior and data quality in unanticipated ways. Developers are solely responsible for monitoring and mitigating any potential market integrity risks.
- Application Code Risksare those associated with the quality, reliability, and dependencies of the code on which an application operates. Developers are solely responsible for monitoring and mitigating any potential application code risks.

Pleaserefer to this guide for additional informationabout market integrity risks and how developers can protect their applications.

Developer Responsibilities

Developers are responsible for maintaining the security and user experience of their applications. They must also securely manage all interactions between their applications and third-party services.

In particular, developers implementing Chainlink Data Feeds in their code and applications are responsible for their application's market integrity and code risks that may cause unanticipated pricing data behavior. These are described below in more detail.

Market Integrity Risks

Market conditions can impact the pricing behavior of assets in ways beyond the ability of Chainlink node operators to predict or control.

Market integrity risk factors can include but are not limited tomarket manipulation such as Spoofing, Ramping, Bear Raids, Cross-Market Manipulation, Washtrading, and Frontrunning. All assets are susceptible tomarket risk , but in particular, assets with high market risk, such as those with low liquidity, are the most vulnerable to market manipulation. Developers are solely responsible for accounting for such risk factors when integrating Chainlink Data Feeds into their applications. Developers should understand the market risks around the assets they intend their application to support before integrating associated Chainlink Data Feeds and inform their end users about applicable market risks.

Developers should reference the following additional information when implementing Chainlink Data Feeds:

- Data Feed Categories to evaluate market integrity risks associated with specific Chainlink Data Feeds Developers intend to integrate.
- Evaluating Data Source Risks to evaluate risk mitigation techniques associated with Chainlink Data Feeds broadly.

Application Code Risks

Developers implementing Chainlink Data Feeds are solely responsible for instituting the requisiterisk mitigation processes including, but not limited to, data quality checks, circuit breakers, and appropriate contingency logic for their use case.

- Code quality and reliability:Developers must execute code using Chainlink Data Feeds only if the code meets the quality and reliability requirements for their use case and application.
- Code and application audits:Developers are responsible for auditing their code and applications before deploying to production. Developers must determine the quality of any audits and ensure that they meet the requirements for their application.
- Code dependencies and imports:Developers are responsible for ensuring the quality, reliability, and security of any dependencies or imported packages that they use with Chainlink Data Feeds, and review and audit these dependencies and packages.