CMIC
Crypto Market
Integrity Coalition

INTEGRITY ABOVE PROFIT

THE CRYPTO MARKET CONSUMER BILL OF RIGHTS

About the Crypto Market Integrity Coalition (CMIC): CMIC is an association of responsible digital assets companies that have committed to continually improve market integrity, combat market abuse and manipulation, and engage with regulators. Co-founded by Solidus Labs and 17 industry leaders in 2022, CMIC has grown to 55 members who have each pledged to advance market integrity standards and address gaps in current regulation. CMIC has developed and adopted a comprehensive market integrity code of conduct, launched CMIC Academy and resource library, and has built out a policy agenda focused on things like shared market surveillance, AML modernization, countering fraud, and other priorities.

TABLE OF CONTENT

Glossary of Terms

Please refer to the above link for a continually updated glossary of terms associated with the crypto market.

INTRODUCTION

The crypto market is developing so rapidly that the number and diversity of those who deliver and receive services has grown exponentially in the last decade. Boston Consulting Group predicts that a billion people will use digital assets by 2030[1]. This is a staggering rate of scale since 2009 when Bitcoin was first introduced.

The United States created a Consumer Bill of Rights in 1962 – 186 years after the Declaration of Independence. With the hyper scale of adoption and a nearly borderless system, the crypto market cannot wait this long to provide a unified set of assurances to its consumers.

In late 2023, CMIC members engaged in conversations and workshops to help develop several workstreams – all feeding important contributions to increase market integrity. One such workstream focused on consumer redress. A group of CMIC members in this workstream collaborated on the development of this document.

PURPOSE

The purpose of this document is to help crypto market leaders and government policymakers globally with the development of thoughtful and actionable consumer protection measures. Furthermore, service providers who demonstrate close alignment with the tenets of this document can conceivably earn and maintain a better reputation in a market which, like any other, depends on high integrity of, and continual trust among, all its participants.

PROBLEM STATEMENT

Crypto market consumers today are saddled with unjustified risk of damage to their financial health, reputation, and lifestyle expectations because of poorly designed, sparsely regulated, and wildly inconsistent measures for the protection of their rights. In cases of cryptocurrency theft, the recovery is typically convoluted, very expensive, lengthy, and has a relatively low probability of success.

[1] https://cointelegraph.com/news/crypto-to-reach-1-billion-users-in-2030-bcg-report

SOLUTION STATEMENT

Every crypto market service provider and regulator should have robust controls (both proactive and reactive) for the protection of consumer rights, and provide clear, simple, efficient ways of exercising such rights. Every consumer should be made aware of the risks and rights around the services they are receiving from any service provider throughout the duration of the relationship. Risks and rights awareness information should be designed and delivered in such a way that it would be understandable, memorable, and actionable throughout the duration of the relationship.

VISION

Consumers in the crypto market will have a very clear understanding of the risks and rights associated with every service they receive for the duration of the service delivery. They will be able to minimize their exposure to risks and exercise their rights with optimal effectiveness and efficiency while being fully supported by service providers and regulators. These steps will help build integrity and trust in the crypto market.

TARGET AUDIENCE

This document has been prepared for consideration and adoption by all service providers and regulators in the crypto market.

NECESSITY OF MULTI-JURISDICTIONAL APPLICATION

Blockchains, cryptocurrencies, non-fungible tokens, smart contracts, and many other digital platforms and products are not subject to geographic or political boundaries. They all rely on access to the worldwide web. Although the crypto market does include certain physical products like hardware wallets and cold storage, market regulation must follow the global nature of the market behavior. Therefore, consumer rights in the crypto market are country-agnostic and necessitate global adoption.

KEY DEFINITIONS

- **Crypto Market**: Any network where participants agree and capitalize on the value of cryptographically created entities such as blockchains, currency tokens, smart contracts, tokenized real-world assets (RWA), and many others for a variety of services.
- **Service**: Any assistance, support, and transactions that a service provider offers to consumers. This includes the provision of tasks and fulfillment of contractual obligations to meet the needs and expectations of consumers.
- **Service Provider**: Any formally registered organization which delivers any service to consumers.
- **Consumer**: Any individual or a formally registered organization which receives any service from a service provider.

SCOPE

This document addresses any service, service provider, and consumer operating in the crypto market.

RELEVANT SCENARIOS

SCENARIO 1

A cryptocurrency exchange customer notices some irregularities on their account. They attempt to contact customer service. To do so, they can send an email to a general email address and wait for a reply or initiate a chat with an AI bot as a filter for escalation of issues. The delay in getting a satisfactory resolution is significant.

SCENARIO 2

A crypto market service provider unexpectedly announces a freeze on customer funds' withdrawals. While some reasons and assurances are offered in the announcement, multiple customers begin to demand release of their funds. The only outlet for these customers is the

service provider itself and, potentially, law enforcement. Regardless, the process of funds' retrieval is lengthy, convoluted, and potentially expensive.

SCENARIO 3

A blockchain infrastructure development firm is supporting a financial institution as it rolls out an app and wallet-based cryptocurrency asset management platform. Customers are able to move some of their fiat holdings into various crypto tokens and execute individual trades or have such funds managed by professional investment managers. Suddenly, the app/wallet software experiences a glitch and there are irregularities with credits to and transfers out of individual customer accounts on the platform. The financial institution contacts the infrastructure development firm for assistance and forensic analysis of the backend they developed. However, the infrastructure development firm, realizing that there could be a financial risk, significantly downgrades their cooperation. The financial institution realizes that the only way of getting replies from their partner is through litigation and court-ordered release of pertinent information. Significant legal costs and a lengthy process are expected.

ASSUMPTIONS / CAVEATS

- This document will require at least semi-annual or issue-specific updates because of the crypto market's dynamic nature and changes in consumer behavior.
- Success of this document's implementation will depend on multiple factors and tools. For example, adoption by service providers and regulators in various jurisdictions as well as availability of a universally accessible industry collaboration and consumer rights portal.
- Successful adoption of this bill of rights depends on crypto market service providers having sufficiently competent talent to effectively implement consumer protection measures described in this document.

RIGHT TO TRANSPARENCY

An important factor of each service provider's integrity is the transparency with consumers about ways in which their products and services are delivered and what steps each consumer could take to seek recourse. Below are the foundational tenets.

DISCLOSURE OF FEES AND CHARGES

Consumers will receive a full written disclosure about fees and charges in plain language. Such disclosures will be designed to help maximize consumers' awareness and understanding, including ways of obtaining prompt and clear responses to any inquiries.

CLEAR COMMUNICATION OF RISKS

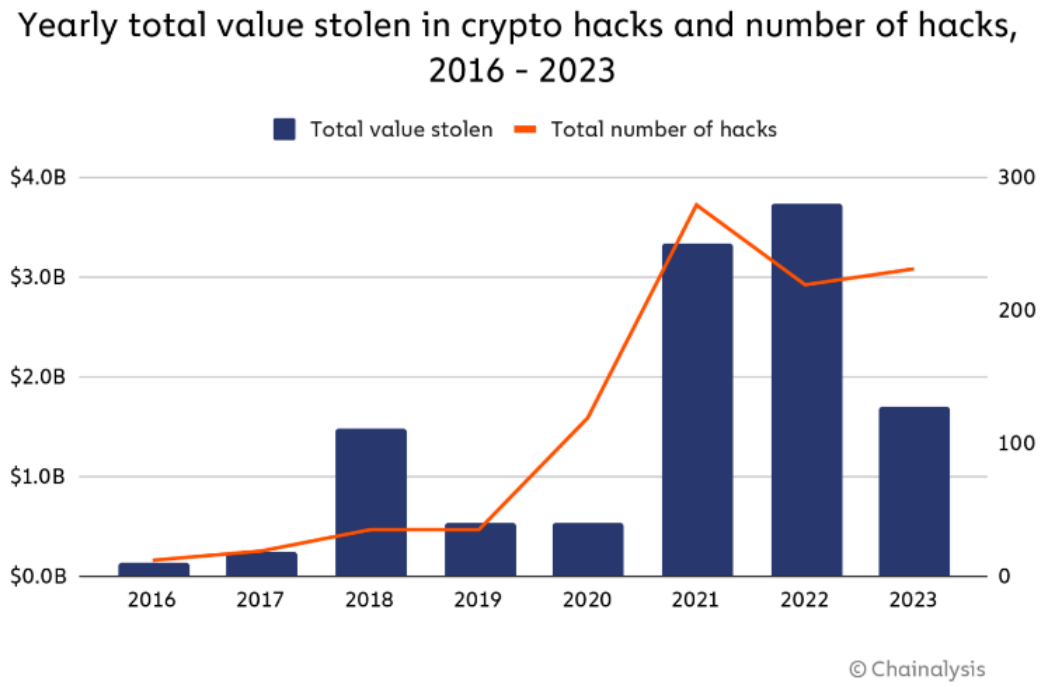
Consumers will receive a full written disclosure in plain language about risks of engaging with the service provider. Such disclosures will be designed to help maximize consumers' awareness and understanding, including ways of obtaining prompt and clear responses to any inquiries.

EXPLANATION OF TECHNOLOGY

Consumers will receive a full written disclosure in plain language about technology which helps deliver each of the services. Such disclosures will be designed to help maximize consumers' awareness and understanding, including ways of obtaining prompt and clear responses to any inquiries.

RIGHT TO SECURITY

Security, otherwise known as protection of assets, is another foundational aspect of the relationship between consumers and service providers in the crypto market. Every consumer expects service providers to handle assets entrusted to them, as well as the back-end infrastructure supporting mission-critical operations, in the most secure way possible. Furthermore, consumers expect every service they receive to be free of any malicious elements which could cause them financial and reputational harm. As the crypto market continues to mature, the security risks evolve. For example, a report for 2023 by Chainalysis notes a substantial decrease in the total value of funds stolen through cryptocurrency hacking incidents, but also warns of an increase in the total number of such incidents. One telling graphic from their report is below.



What remains unclear is whether the decrease in the value of stolen assets is due to better security measures or because more incidents go unreported. Whatever the root causes may be, consumers' expectation of effective security from service providers is ever present.

Addressed below are the key categories pertaining to consumers' security expectations.

DATA PROTECTION

At its fundamental level, data is computer code which shapes the majority of products and services in the crypto market. As numerous other industries and markets experience data breaches, the crypto market is not immune. Therefore, service providers in the crypto market must adopt global best practices and standards for the protection of data, including all digital assets in service providers' environments which pertain to consumers.

FRAUD PREVENTION AND RESOLUTION MEASURES

While prevention of fraud is the primary expectation of consumers, service providers must have robust controls for the entire fraud cycle – from detecting its early signs to offering a speedy resolution and improving controls after fraud has been committed. Consumers should expect prompt, attentive, and transparent communication during the entire fraud

cycle. The Association of Certified Fraud Examiners (ACFE) is the global leader in best practices and standards for fraud detection and management. Service providers must align closely with ACFE for collaboration and adoption of best practices and standards.

Source: https://www.lawyer-monthly.com/2022/11/moving-the-needle-on-fraud/

SECURE STORAGE SOLUTIONS

Crypto assets managed by service providers are stored in two ways:

- in environments which are – or can quickly be – directly connected to computer networks;
- on physical data storage devices which are completely disconnected from computer networks.

No matter the choice of storage, service providers must ensure that protection measures for stored assets meet global best industry practices and standards. Consumers should receive a clear explanation about security measures implemented to protect their stored assets.

RIGHT TO PRIVACY

Recognizing that service providers have different know-your-customer (KYC) requirements and processes depending on the nature of the product or service, the relationship with every

consumer entails expectations of privacy. Specifically, consumers expect that their personal information and the nature of their relationship with every service provider will not be shared with third parties without their prior authorization unless requested by a regulator, law enforcement, or a court. Outside of these exceptions, service providers must demonstrate their alignment with consumer expectations both through communication and design of privacy control measures.

PERSONAL DATA PROTECTION

Service providers will apply the same measures to the protection of personal data as discussed in the "Right to Security" section above.

ANONYMOUS TRANSACTIONS

While full anonymity for customer transactions is not possible because of the need for potential disclosure to authorities, service providers must anonymize consumer transactions on their platforms in the most optimal and secure way by using codification, encryption, and other methods. The same tools should be offered to consumers who receive services through mobile or desktop applications so that each consumer could control their own privacy settings.

RIGHT TO FAIR PRACTICES

NO DISCRIMINATION

Consumers are entitled to equal treatment without discrimination based on race, gender, age, religion, nationality, or any other characteristic. Service providers must ensure their services and interactions are inclusive, fostering a fair and respectful environment for all.

EQUITABLE ACCESS TO SERVICES

Every consumer should have fair and equal access to services. This means service providers need to remove barriers that might prevent consumers from obtaining services, ensuring accessibility to all, including those with disabilities, those from marginalized communities, and those from different geographies.

FAIR CONTRACT TERMS

Consumers have the right to contracts that are clear, transparent, and fair. Terms and conditions should be written in plain language, avoiding unfair terms or hidden clauses that could exploit or disadvantage consumers. This ensures trust and accountability between service providers and their customers.

RIGHT TO REDRESS

DISPUTE RESOLUTION MECHANISMS

Ensuring effective dispute resolution mechanisms is essential for protecting consumer rights and fostering trust. Service providers must adhere to the following principles:

Accessible Complaint Channels: Consumers should have easy access to channels through which they can lodge complaints. This includes hotlines and online portals ensuring consumers can raise issues without barriers.

Transparent Process: The dispute resolution process must be clear and transparent. Consumers should be informed about the steps involved, expected timelines, and the criteria used for decision-making.

Mediation / Arbitration / Litigation: Third parties, such as consumer protection agencies or accredited mediation / arbitration specialists, must be available to address disputes impartially. This helps ensure fairness and objectivity in resolving conflicts.

In addition to mediation and arbitration, consumers must have the right to seek legal recourse if their rights have been violated. This includes access to courts, legal representation, and fair hearings to resolve disputes and enforce consumer rights.

All disputes must be resolved within a reasonable timeframe to ensure that consumers do not suffer prolonged uncertainty or inconvenience. Clear timelines should be established and adhered to by the service providers.

Protection from Retaliation: Consumers seeking recourse must be protected from retaliation or adverse consequences from service providers or other entities involved in the dispute. This ensures that consumers can exercise their rights without fear of reprisal.

Consumer Education: Educating consumers about their rights and the dispute resolution process empowers them to effectively address issues. Information must be readily available

through various channels, including websites, digital forums, and consumer outreach programs.

REFUND AND COMPENSATION POLICIES

Each service provider must adhere to the following principles:

Right to Refund: Consumers are entitled to a refund if the products or services they purchase fail to meet the promised standards or are found to be defective. Service providers must clearly communicate the promised standards and criteria for faulty products or services prior to consumers acquiring them. This ensures that consumers are not unfairly disadvantaged by faulty or misrepresented products or services.

Fairness and Transparency: Refund and compensation policies must be clearly communicated and easily accessible. Terms should be straightforward, specifying conditions for eligibility, timeframes, and the process for requesting a refund or compensation.

Reasonable Timeframes: Consumers should be able to request refunds or compensation within a reasonable period after the purchase. This timeframe should be clearly stated and allow adequate time for consumers to identify any issues with the product or service.

No Penalties for Legitimate Claims: Service providers must not impose unreasonable penalties or fees on consumers who request refunds or compensation for legitimate reasons. This ensures that consumers can seek redress without facing unfair financial burdens.

Proactive Resolution: In cases where a product or service issue arises, service providers should proactively offer solutions, including refunds or compensation, without placing undue burden on consumers to initiate the process.

Equal Treatment: All consumers, regardless of their background or circumstances, should have equal access to refund and compensation policies. This prevents discriminatory practices and ensures fairness in the resolution process.

CASE STUDIES AND PRECEDENTS

This collection of links to industry resources is not exhaustive and will be continually updated.

- Avoiding unfair business practices: A Guide for Business and Legal Practitioners
- 2023 in Review: Australian Competition and Consumer Commission
- Submission to the Treasury on the Licensing and Custody Requirements for Crypto Asset Secondary Service Providers (CASSPrs)
- Consumer contacts us to complain after a cryptocurrency investment scam Fraud and scams

RIGHT TO EDUCATION

ACCESS TO EDUCATIONAL RESOURCES & CONTINUOUS CONSUMER EDUCATION PROGRAMS[2]

The low literacy rates require immediate policy actions, such as creating awareness for financial literacy, compulsory integration of financial education in schools' curricula, encouraging employer-provided financial education programmes, etc. The development of financial literacy programmes can be greatly aided by universities. Financial literacy programmes should be designed with clear objectives for targeted audiences, such as youth, women, elderly and professionals. The journey toward financial literacy does not end with the mastery of concepts and principles. It must evolve to encompass digital, sustainable, and ethical finance, shaping a future that is equitable, prosperous, and environmentally conscious. As technology continues to evolve and global markets become more intricate, the need for financial literacy will only grow, and it is our collective responsibility to ensure that future generations are equipped with the knowledge and skills to navigate this complex landscape.

RIGHT TO CONTROL

OWNERSHIP AND CONTROL OF ASSETS

Consumers shall have complete ownership and control over their digital assets, encompassing not only cryptocurrencies but also any digital representations of value or

[2] Crypto Market Integrity Coalition Academy (free)

ownership rights, including tokens, virtual property, and digital collectibles. Service providers must facilitate secure and timely access, transfer, and management of these assets according to the consumer's instructions, ensuring that consumers can exercise full control over their digital property. This includes enabling compatibility with various self-custody solutions and providing clear information about the risks and benefits associated with different asset storage mechanisms.

CONSENT FOR USE OF PERSONAL DATA

Service providers must obtain explicit and informed consent from consumers before collecting, using, or sharing their personal data. Consumers should have granular control over their data and privacy settings, including the option to revoke consent, request data deletion, or restrict the use of their data for specific purposes. Service providers should prioritize data minimization principles, collecting only the data necessary for the provision of services and ensuring robust security measures to protect consumer data from unauthorized access or breaches.

RESPONSIBILITIES OF SERVICE PROVIDERS

ENSURING COMPLIANCE

Service providers must not only comply with all applicable laws and regulations related to consumer protection, data privacy, and financial services but also proactively adapt to the evolving regulatory landscape. This includes staying abreast of emerging legislation, regulatory guidance, and industry best practices to ensure ongoing compliance and maintain a secure and transparent environment for consumers.

ETHICAL BUSINESS PRACTICES

Service providers must conduct their business in an ethical and transparent manner, prioritizing consumer interests and fostering trust. This includes avoiding deceptive or unfair practices, providing clear and accurate information about products and services, and maintaining open communication channels with consumers. Service providers should actively promote ethical standards within the industry and contribute to the development of a responsible and sustainable crypto ecosystem.

ACCOUNTABILITY AND TRANSPARENCY

Service providers should be accountable for their actions and transparent in their operations, providing clear and accessible information about their products, services, fees, and security measures. They should also establish clear channels for consumer feedback and complaint resolution, ensuring that consumer concerns are addressed promptly and effectively. Service providers should proactively disclose any conflicts of interest and maintain comprehensive records of their operations to ensure accountability and transparency.

REGULATORY FRAMEWORK

As digital assets continue to grow steadily becoming an integral part of the global financial system, regulatory bodies worldwide are intensifying their focus on consumer protection to address the unique challenges posed by this rapidly evolving sector. The regulatory landscape is increasingly nuanced, reflecting a growing understanding of the risks associated with digital assets and the need for robust consumer safeguards.

APPLICABLE LAWS AND REGULATIONS

Globally, regulatory frameworks are adapting to ensure consumer protection in the crypto sector. The European Union's MiCA Regulation stands out for its comprehensive approach, integrating strong consumer protection measures into its legal framework. MiCA introduces a broad set of anti-market abuse provisions, including those targeting the AML/CFT compliance, sanctions, fraud prevention, insider trading and various forms of price manipulation. The regulations are also focusing on the Maximum Extractable Value (MEV) strategies prevalent in DeFi environments. These rules aim to curtail market manipulation by ensuring that manipulative practices, which can undermine market integrity, are subject to strict oversight. The MiCA framework also introduced robust reporting requirements and cross-border cooperation between national regulatory authorities.

In the United States, the debate for legislative initiatives is still ongoing, with a number of Bills being introduced in Congress. Up to the end of 2024, the regulatory authorities are extensively exercising regulation by enforcement, imposing fines and taking market participants to courts. SEC applied the Howey Test to determine if a digital asset is a security, thereby subjecting it to securities regulations that protect investors from fraud. The CFTC regulates digital assets as commodities under the Commodity Exchange Act, with a focus on

preventing manipulation and fraud. The IRS treats digital assets as taxable assets, overseeing compliance and investigating financial crimes linked to digital assets. Legislators on State level are providing some clarity for the digital assets community with New York, California, Texas and Wyoming leading the course. The post-elections sentiments in the US are very positive and both the legislators and regulators are keen on introducing clear "rules of the game" for the digital assets market to thrive and ensure consumer protection.

The UK has defined the legal status of digital assets and is currently working on developing its regulatory framework to prevent market abuse and fraud in crypto assets market.

Hong Kong and Singapore regulations are extensively focusing on AML/CFT and market abuse prevention addressing payment service providers and other types of VASPs. Similarly, Japan's Payment Services Act ensures that crypto transactions are conducted with full transparency and fairness.

In India, the Crypto Awareness Campaign spearheaded by the Investor Education and Protection Fund (IEPF) and the Consumer Protection (E-Commerce) Rules, 2020 emphasize the need for transparency and consumer education, particularly as they pertain to crypto exchanges and DeFi services. South Korea has enacted the Virtual Asset User Protection Act, which mandates stringent disclosure requirements and consumer safeguards against fraudulent practices.

Role of Regulatory Bodies

Regulatory bodies are pivotal in enforcing these frameworks and ensuring market integrity, protecting consumers from fraud, market manipulation, and other abusive practices.

There are national regulators in every country, with some dedicated digital assets regulatory agency's (such as VARA in Dubai and self-regulatory agency in Japan) that address market abuse and protect investors.

In Europe, the European Securities and Markets Authority (ESMA) alongside with the National Competent Authorities (NCAs) oversee the enforcement of MiCA, with particular emphasis on preventing market abuse and ensuring that decentralized finance platforms adhere to anti-manipulation rules. The Financial Conduct Authority (FCA) and His Majesty's Treasury (HMT) in the UK is also working to expand market abuse regulations to cover crypto assets, aiming to align regulatory practices with traditional financial markets.

There are multiple entities in the US that investigate and enforce against market abuse in the digital assets space both on Federal and state levels. On Federal level the following authorities are overseeing the digital assets market participants:

- Financial Crimes Enforcement Network (FinCEN): Under the Department of the Treasury, FinCEN enforces the Bank Secrecy Act (BSA) and oversees money services businesses (MSBs) like cryptocurrency exchanges to ensure compliance with anti-money laundering (AML) regulations. FinCEN has issued specific guidance on the treatment of cryptocurrency as money transmission services.
- Securities and Exchange Commission (SEC): Oversees securities-related transactions involving cryptocurrency, especially regarding ICOs (Initial Coin Offerings), unlicensed trading and fraudulent schemes that impact investors.
- Commodity Futures Trading Commission (CFTC): Regulates digital commodities and derivatives, such as futures and swaps, ensuring market integrity.
- Internal Revenue Service (IRS): Focuses on ensuring compliance with tax regulations related to digital assets, including the reporting of capital gains and preventing tax evasion.
- Office of Foreign Assets Control (OFAC): Administers and enforces economic and trade sanctions, targeting the use of digital assets to evade sanctions, especially by rogue states.

In summary, as the crypto market continues to expand, the convergence of regulatory efforts worldwide reflects a unified focus on protecting consumers and maintaining market stability. This evolving regulatory landscape not only addresses current risks but also anticipates future challenges, setting a precedent for how global financial systems can adapt to the digital age.

INTERNATIONAL STANDARDS AND COOPERATION

Given the global nature of digital assets, regulators cooperate with each other and with the law enforcement to track illicit digital assets activity across borders. Notably, the IOSCO, BIS and FATF issued numerous reports and guidelines to define approaches in crypto markets regulations and address issues that pose threats to market fairness and integrity. FBI, Interpol and Europol have established dedicated units to fight financial crime and protect investors, recovering stolen funds and ensuring the pursuit of justice.

ENFORCEMENT AND COMPLIANCE

MONITORING AND REPORTING

Market surveillance is rapidly becoming a required component of an effective digital asset compliance program in the face of increased market demand and regulatory guidance, requirements, investigations, and enforcement activity. In recent years, state and federal regulators in the United States and globally have issued clear warnings about the risk of market manipulation in digital asset markets, and increased enforcement activity against digital asset platforms and participants. The failure of a digital asset marketplace to establish a comprehensive market surveillance and risk monitoring can accordingly create substantial enterprise risk and impede the further development and adoption of digital assets.

In comparison to traditional financial markets, the digital asset market is exposed to unique risks and therefore requires a tailored monitoring approach. Below are some of such peculiarities[3]:

Native Onchain Threat Detection: monitoring of wallets, decentralized financial applications (DeFi apps), and smart contracts for scams, hacks, and exploits, utilizing proprietary detection mechanisms, open source feeds, and best of breed data sources. FRT may be used as tools for money laundering after exploits and scams are conducted onchain, and may even be directly involved in executing of such exploits and scams.

Unique DeFi - CeFi Monitoring: unlocking comprehensive ecosystem insights including order book + onchain activity, allowing for monitoring of offchain risks (e.g., unusual volume involving fiat-referenced tokens), to cross-chain manipulative strategies like liquidity pool price manipulation through flash loans followed by CEX arbitrage.

Risk-assessment of clients and tailored monitoring approaches: companies based on their risk profile, will require persistent or frequent, periodic monitoring. This includes both onchain and offchain monitoring to capture a comprehensive view of their activities, ensuring that potential risks are promptly identified and addressed. By customizing monitoring strategies digital assets platforms can maintain a more robust compliance framework and mitigate the likelihood of market abuse or other illicit activities.

[3] Solidus Labs 2023 Crypto Market Manipulation Report Series

Supply Reporting: transparent, and regular reporting of the full suite of supply and holder statistics will enable critical risk management modeling for counterparties, regulators, and even central banks as issuers grow in market cap and contribute to a more meaningful part of the overall economy.

When introducing regulations, the global regulatory authorities often require real-time monitoring and timely reporting of suspicious activities based on the suspicious report template provided by a particular regulator.

PENALTIES FOR NON-COMPLIANCE

Penalties for non-compliance in the digital assets market resemble those in traditional finance, emphasizing the need for strict adherence to regulatory requirements. Regulatory authorities may impose hefty fines on firms that violate compliance requirements, with penalties potentially reaching millions of dollars. Additionally, firms may face sanctions such as suspension or revocation of licenses, effectively crippling their operations. Reputational damage is also a significant risk, as breaches of compliance can undermine consumer trust and deter investors, paralleling the fallout seen in traditional financial institutions. Moreover, individuals within the firm, including executives, may face personal liability and even criminal charges for egregious violations or fraudulent activities. Overall, these penalties highlight the critical importance of robust compliance measures in the digital assets and in a manner similar to traditional financial markets to safeguard consumer interests and uphold market integrity.

CONSUMER PROTECTION AGENCIES

In the United States and globally, various agencies focus on protecting consumers from the fraud and scam associated with digital assets. These agencies aim to prevent fraud, ensure transparency, and help consumers navigate the complexities of digital assets markets.

In the U.S., the Federal Trade Commission (FTC) is a key player in safeguarding consumers in the digital asset space. The FTC primarily targets fraudulent schemes and deceptive practices related to digital assets. It actively monitors and takes action against crypto scams, ponzi schemes, and misleading advertising. Additionally, the FTC provides consumers with guidance on how to avoid falling victim to crypto fraud and provides a platform for reporting fraud or scam.

The Consumer Financial Protection Bureau (CFPB) also plays a significant role in protecting consumers within the financial sector, which includes digital asset-related products. The

CFPB focuses on transparency and fairness in services such as digital wallets and cryptocurrency payment platforms. It oversees consumer complaints and ensures companies offering digital assets follow consumer protection laws.

At the state level, consumer protection offices handle issues related to local crypto fraud and assist consumers in disputes with businesses.

Globally, consumer protection efforts are also increasing. In the European Union, consumer protection is being strengthened with the development of regulations like the Markets in Crypto-Assets (MiCA) framework, which focuses on protecting crypto consumers and ensuring fair practices across member states. The Financial Conduct Authority (FCA) in the United Kingdom ensures that consumers are not misled by crypto companies and that they have access to accurate information about digital asset products. In Australia, the Australian Competition and Consumer Commission (ACCC* addresses crypto-related fraud and scams, helping consumers stay informed and safe in the digital asset market. Similarly, Canada's Financial Consumer Agency (FCAC) provides oversight and resources to protect consumers in their dealings with digital assets.

Beyond individual nations, international cooperation on consumer protection is growing. The International Consumer Protection and Enforcement Network (ICPEN) and EGMONT Group allow for collaboration between countries to combat cross-border digital asset fraud and ensure consistent consumer protection standards. This collective effort helps consumers across the globe navigate the risks associated with digital assets while empowering them with the knowledge and resources needed to protect themselves from fraud and exploitation.

ACKNOWLEDGEMENT

This Consumer Bill of Rights is the result of a collaborative effort by the Consumer Redress Workstream, under the leadership of Ilya Umanskiy, Partner at Sphere State Group.

We gratefully acknowledge the contributions of the following CMIC members, whose dedication and expertise have been instrumental in bringing this project to fruition:

- **Ilya Umanskiy**, Partner, Sphere State Group
- **José Nunes**, COO, VAF Compliance
- **Jugnu Verma**, Head of Market and Trade Surveillance, BitMEX
- **Chen Arad**, Co-Founder and CXO, Solidus Labs
- **Amina Turgulova**, Senior Policy & Regulatory Affairs Advisor, Solidus Labs