coinbase

To:
Bermuda Monetary Authority
BMA House
43 Victoria Street
Hamilton HM12
policy@bma.bm

30 September 2025

Re: The Responsible Use of Artificial Intelligence in Bermuda's Financial Services Sector

Coinbase Global, Inc. (together with Coinbase Bermuda Limited, Coinbase Bermuda Services Limited, and its other subsidiaries, "**Coinbase**") appreciates the opportunity to respond to *The Responsible Use of Artificial Intelligence in Bermuda's Financial Services Sector* (**Consultation**) published by the Bermuda Monetary Authority (**BMA**).

Coinbase is the most trusted service provider of crypto trading, custody, and infrastructure in the world. Founded in 2012 and publicly listed on the NASDAQ, we offer a secure and user-friendly interface for millions of verified retail and institutional investors globally. Coinbase is committed to building an open financial system and reimagining the future of finance through new technologies and innovative products.

There is a significant opportunity to improve the financial services sector by embracing the responsible use of Artificial Intelligence (**AI**). AI-based systems can more effectively ensure orderly markets and investor protection by preventing fraud and deterring market manipulation and other abuses. This technology can also enable regulated entities to better meet their own regulatory obligations, while simultaneously helping financial services regulators fulfil their missions.

Coinbase appreciates the BMA's engagement with this issue which we expect to only become more important in financial services. We look forward to continuing to work with you as this technology develops.

Sincerely,

Tom Duff Gordon,
VP, International Policy
Coinbase Global, Inc.

Jeffrey Baron,
COO, Coinbase Bermuda

Introduction

Coinbase applauds the BMA's release of the Discussion Paper because it demonstrates concretely that the BMA appreciates the impact that Artificial Intelligence (AI) technology will have—and is already having—on financial markets and the financial services industry. Indeed, Coinbase believes that machine learning (ML)[1] methods will be an important tool for growth, innovation, and consumer protection in the financial services sector. We use ML methods underlying Generative AI (GenAI)[2] products and processes for a number of purposes, including supervision of market activities in Coinbase, Inc. (CBI), developer productivity, and compliance. Coinbase Bermuda Limited, as the operator of the Coinbase International Exchange, leverages these advanced AI and ML tools to enhance its own compliance, market integrity, and customer protection programs in Bermuda.

Greater adoption of AI-enabled technologies like those that we and other market participants are adopting will not only enable regulated entities to better meet their own regulatory obligations but will also help financial services regulators fulfill their missions. We believe that regulators and self-regulatory organizations that use AI-based systems responsibly for purposes of fraud prevention, compliance and deterrence of market manipulation as well as other potential abuses will more effectively ensure orderly markets and investor protection than those that do not. As a consequence, these entities will enjoy higher integrity and offer greater safety for investors and consumers.

To that end, regulators should avoid adopting expansive rules that risk stifling innovation and investment in this nascent technology. Laws that create complex or potentially unclear rules for the use of AI may inhibit innovation by favoring a small set of large firms with the resources necessary to successfully navigate them. This would serve to entrench incumbent entities while limiting contributions from more innovative newcomers. The promise of AI in this area cannot be realized in an overly-prescriptive regulatory environment that limits the ability of entities to embrace future developments. Therefore, we agree with the approach of the BMA's proposed five-dimensional Risk Assessment Framework, which aligns with a sound, risk-based approach.

To be sure, the use of AI systems and tools is already present in the financial services sector. GenAI and ML, which are both captured in the definition of AI used by the Discussion Paper,[3] are being used and tested by Coinbase in certain carefully

---

[1] Machine learning defines a related but distinct area of computer science that focuses on the development and use of algorithms that enable computers to learn from and make predictions or decisions based on data without being explicitly programmed for each task.
[2] Generative AI is a type of artificial intelligence that can create new content, such as text, images, music, or code.
[3] *See* Discussion Paper at 29 (defining machine learning as "[a] subset of AI where systems improve their performance on tasks through experience without being explicitly programmed."). We use AI throughout this response as a general term to refer to both ML and GenAI.

governed ways to improve processes within the company and to increase efficiency, with promising results.

It is important to note that the relationship between AI and financial services, particularly services using blockchain technology, is a reciprocal and mutually beneficial one. Innovations in one can be used to advance the other. We discuss below the ways in which AI is helping the financial services sector improve, but we also wish to note that innovation in blockchain-based financial services can improve the quality and utility of AI. Last year, Coinbase witnessed the first AI-to-AI blockchain-based transaction on our blockchain, Base.[4] This transformative technology will empower AI tools to send and receive crypto assets by accessing onchain wallets, allowing them to complete transactions independently and provide much greater utility for users overall.

Applications in Financial Services

Market Surveillance and Integrity

One of the most prevalent uses of ML systems at Coinbase is for market surveillance programs, which ensure compliance with exchange trading rules. As we have expressed in other consultation responses, these systems can be designed to detect manipulative trading activities, such as "spoofing" or "layering," by observing trade message patterns that indicate such schemes.[5] These ML surveillance models can learn over time (through programmatic evolution as well as input from surveillance team analysts) which data patterns should trigger a regulatory alert to the market operator consistent with its surveillance and investigatory policies and procedures.

CBI is already using ML models to assist trade surveillance to reduce the escalation of false positives. The ML models deployed for CBI assign a probability score that is generated using fixed inputs. The Surveillance team sets the automation logic to close all alerts below a probability threshold score and to escalate for human review those above the Surveillance defined score. Guided by the Surveillance staff's probability score threshold setting, the ML model will auto-close a majority of false positives and allow analysts to focus on more high-probability manipulative activity.

These same methods are also now on track to be used by our derivatives exchange as part of our self regulatory obligations, to assist in fine tuning alert parameters and

---

[4] Brian Armstrong, *AIs are now paying other AIs with crypto*, (August 30, 2024) Brian Armstrong on X: "AIs are now paying other AIs with crypto" / X.

[5] Coinbase, *Re: Request for Comment on the Use of Artificial Intelligence in CFTC-Regulated Markets*, (April 24, 2024), *available at* https://assets.ctfassets.net/c5bd0wqjc7v0/4Hodz91tFl3ggSTBBBLR8r/641c68aeff2d28c46e618206506d3a3d/CFTC_Response.pdf; Coinbase, *Re: Request for Information on Uses, Opportunities, efficiand Risks of Artificial Intelligence in the Financial Services Sector* (Aug. 12, 2024), *available at* https://assets.ctfassets.net/o10es7wu5gm1/6uO6LHCnY5Rm7fYeiM3R6P/f99c7948d2445605917348e10e9b7422/2024-08-12-UST_RFI_on_Artificial_Intelligence.pdf; Coinbase, *Re: Targeted Consultation on Artificial Intelligence in the Financial Sector* (Sept. 13, 2024); *available at* https://assets.ctfassets.net/o10es7wu5gm1/2QLLSUiJojObmscA4iXmDf/a4ad814660814fda06560996d7eb7c5a/2024.08.19.EC_Consultation_on_AI_in_Financial_Services.pdf.

analyzing market data and participant activity. AI-enabled technologies stand to provide a new perspective into how the derivatives exchange's markets and participants operate, as well as potentially identifying and highlighting new disruptive practices.

CBI and our derivatives exchange have observed substantial efficiency gains in running their respective trade surveillance programs with these tools. These techniques enable 24/7/365 monitoring across all of Coinbase's trading platforms in a way that manual tracking alone cannot match. Unlike traditional market surveillance, which is often done forensically after the fact, these tools help to provide our Trade Surveillance teams with real-time insights that can be actioned and, often, mitigated quickly.

Particularly, as an ML model is trained to reduce false-positive alerts, the number of regulatory alerts processed and requiring review can be reduced over time. Similarly, the number of alerts that require further escalation and review also can be reduced. Designed and programmed responsibly, with the appropriate level of human intervention and other redundancies (including a robust quality control review program and model validation procedures), ML models can assist with the scaling of trade surveillance programs while at the same time improving their efficacy.

Improving the Customer Experience

Coinbase entities are also either using ML models or exploring the use of GenAI systems to improve the overall customer experience. GenAI and ML models hold great promise in improving the customer onboarding process, including in particular the preliminary steps in verifying customer identification, such as address verification.

Customer Onboarding

Verifying customer identity is a fundamental precursor to setting up a CBI account. CBI's customer identification program has policies and procedures that enable the company to confirm the identity of potential customers seeking to onboard. These same policies govern the use of third-party vendors that assist with customer identification.

The onboarding process involves asking for personal information, as required by applicable regulations. That work generates a risk score for the customer. Based on that score, the customer may also be required to undergo "Enhanced Due Diligence" (EDD), where Coinbase may request additional information, such as information about the customer's source of funds, to determine if the customer should have access to the Coinbase platform. The ID-verification process also involves the use of software that confirms the veracity of submitted documentation and its association with the onboarding customer through a variety of different methods. It is often during this onboarding stage where instances of first-party fraud attempts arise, which is where a person knowingly attempts to misrepresent their identity or give false information for financial or material gain.

Increasingly, AI-enabled technologies can assist with the ID-verification process and mitigate first-party fraud. CBI has leveraged third-party ML models to further automate the onboarding process and reduce the risks of human error that might enable fraudulent behavior. These models can be programmed to identify or flag any anomalous data for additional review, or to take some other automated action designed to address these types of risks detected during the onboarding process.

While there remain risks related to proper third-party vendor management related to an AI program, which are addressed below, an AI model for ID verification has the potential to reduce risks otherwise presented by human error during the administration of a customer identification procedure and the broader anti-money laundering program, all other considerations remaining equal.

Post-Onboarding Risks

Once an onboarding customer's identification is verified, there remain other risks related to fraud potentially presented during and after the onboarding process. CBI has observed that certain data on the CBI platform serve as indicia of those risks, which include second-party and third-party fraud.[6] Other common data inputs related to fraud include (i) when a customer buys an asset and immediately sends it to another account or wallet address, or (ii) any unusual transactional activity in a specific wallet address, including anomalous transaction sizes.

AI-enabled technologies can be developed to consume and process this type of information and discern or identify patterns indicative of second- or third-party fraud. The AI models can alert risk managers to conduct additional review and, over time, can learn to automate a response such as categorizing a particular account or accounts as "at risk," imposing a delay on the account's ability to transmit a transfer, or freezing asset transfers into or out of the account. Deployed in this manner, AI-enabled technologies can significantly improve the efficiency of reviewing account and transactional information.

Enhancing Customer Experience

Finally, Coinbase is using ML to enhance the customer experience, such as by providing more personalized notifications. ML models can help provide more curated information to customers when they visit the Coinbase website or app, and can enhance customer service by crafting customized responses to inquiries. Coinbase continues to explore ways in which to use AI-enabled technologies to improve customer experience.

Developer Productivity

[6] Second-party fraud is when a person knowingly gives their identity or personal information to another person, enabling that second person to perform some act to the first person's benefit. Third-party fraud is when a person uses another's identity or personal details without their consent or knowledge in order to gain access to credit or products, commonly referred to as "identity theft."

We are also leveraging AI to enhance developer productivity and streamline workflows. By integrating AI-driven tools, we aim to automate repetitive tasks, improve code quality, and facilitate faster debugging processes. These tools not only allow our developers to focus on more complex and innovative projects but also accelerate the overall development cycle, ensuring that we can deliver high-quality products to our users more efficiently.

Additionally, our AI initiatives include the implementation of intelligent code suggestions and real-time collaboration features, which empower developers to work more effectively both individually and as part of a team. We are committed to creating a more productive and collaborative environment for our developers, ultimately supporting and driving innovation.

Risk Assessment and Materiality Framework

We agree with the approach of the BMA's proposed five-dimensional Risk Assessment Framework, which aligns with a sound, risk-based approach. But we emphasize that the framework could be enhanced by explicitly recognizing the unique risk-mitigating and compliance-enabling qualities of public blockchain data. The transparent, immutable and publicly auditable nature of blockchain transactions provide an exceptional dataset for training AI models and conducting risk assessments—an approach we call "Know Your Transaction" (KYT). This richer data source fundamentally improves the integrity and reliability of AI risk models in a way unavailable to traditional finance.

Coinbase integrates AI risk management within its broader risk management system by implementing specific controls and safeguards, including:

- Employee Training: Providing training on ethical AI use and best practices.
- Quality Assurance Testing: Conducting quality assurance testing for all AI use cases prior to launch to ensure fairness and mitigate unintended bias or discrimination.
- "Human in the Loop": Implementing human oversight to review inputs and outputs, preventing automated decision-making without human intervention for significant decisions, thereby ensuring fairness and accountability.
- Monitoring and Testing: Continuously monitoring and testing large language solutions and their outputs to detect "model drift," identify biases, ensure model integrity, benchmark performance, and validate attribution methods. This involves periodic sampling of outputs and evaluation by human annotators.
- Transparency and Disclosure: Maintaining transparency in privacy policy and disclosures when users interact with chatbots.
- Data Controls: Implementing data minimization and access controls to limit data input into models, and utilizing a zero retention architecture to minimize unauthorized dissemination or training on user data.
- Centralized Risk Framework: Embedding a unique AI risk and control framework within Security & Privacy shared services functions to promote consistent

documentation, tracking, and treatment of identified risks through centralized registers and management.

- Third-Party Vendor Management: Rigorous due diligence, compliance assessment, data protection, and monitoring of third-party AI solutions, including technical understanding of the tools and transparency into their design and functioning.

Coinbase strongly supports the BMA's emphasis on an outcomes-based framework over prescriptive technical requirements, which we believe is the correct approach for any rapidly-evolving technology. Responsible AI governance can be demonstrated through outcomes that show both market integrity and consumer benefit. For example, AI should contribute to reducing fraud and manipulative practices, while also improving compliance processes and making them more efficient. It should enhance the overall customer experience by streamlining onboarding and resolving issues more effectively, and it should strengthen operational resilience by maintaining performance even under stress. Equally important, responsible governance requires strong protections around the quality, integrity, and security of data, ensuring that AI systems operate on reliable foundations.

From a regulatory perspective, we encourage any expectations to provide clarity without being overly rigid, allowing space for innovation while maintaining safeguards. A principles-based approach offers high-level objectives rather than detailed technical mandates, making it adaptable to new developments. Close collaboration between regulators, financial institutions, and technology experts will be key to keeping oversight relevant and effective. Finally, a commitment to regular review and updates ensures that regulatory frameworks evolve alongside advances in AI.

Finally, as a global company, we believe cross-border regulatory cooperation and harmonization are critical. Fragmented or conflicting jurisdictional rules would severely limit the effectiveness of AI models, which perform better when trained on larger, more diverse datasets. A rule requiring a model to be trained and used only on data from one country would ultimately harm consumers by weakening fraud and manipulation detection. Our approach to AI governance is consistent globally, focusing on robust risk management that protects all clients, whether institutional or retail.

Third-Party AI Risk Management

In addition to developing its own AI models, Coinbase sometimes partners with third-party vendors that use ML models in limited ways to deliver their products. In selecting these partners, Coinbase has not sought particular AI expertise or models, but rather the best product solutions, which might happen to leverage AI within the product-solution scope.

Coinbase has followed best practices related to the risk management of such vendors, including engaging in appropriate due diligence of potential partners before the relationships begin. This review involves assessing whether a potential vendor could

satisfy Coinbase's own policies and procedures where necessary, comply with applicable regulations, protect any data required to be shared with the vendor, and effectively allow monitoring of the vendor once it begins providing the product or service.

Although the principles of third-party risk management remain the same for vendors leveraging AI or ML tools, they do present some novel circumstances for managing third-party risks. In the realm of information and regulatory systems, a vendor's products tend to be powered by rules-based, algorithmic software where the processing of certain types of data will lead to predictable results. By and large, anomalies in output will be the result of anomalies in the data (unless, of course, there is a processing malfunction). With AI systems, data inputs feed into evolving decision-making paradigms—changes in data can lead to changes in the methods of processing itself.

Thus, due diligence and ongoing management of a vendor using AI require a level of understanding of the AI or ML tool itself. Achieving this understanding would involve a rigorous assessment to confirm that the correct data inputs are being ingested and turned into appropriate decision-making paradigms by the AI system. This, of course, requires adequate transparency into the design and functioning of these tools, which must be present at all stages of the vendor relationship.

Assessing whether a vendor using AI would enable Coinbase to meet any and all of its own relevant regulatory obligations requires an even deeper level of scrutiny and governance. Depending on the specific purpose of the vendor product, features of this review might include rigorous review of contractual terms; business leader accountability of and sign off for the vendor relationship; an independent evaluation of the vendor's infrastructure, controls, risks, and effectiveness of their controls (i.e., a SOC report); a review of any licensure and insurance for the vendor; and cybersecurity assessments.

In sum, an adequate level of technical understanding of these systems by the end user, combined with relatively greater transparency into the systems themselves provided by the vendor, should be the hallmarks of appropriate risk management of these relationships. This transparency should also include the vendor providing necessary access to data and information when necessary to review and deconstruct operational incidents. One necessary control that should be in place to achieve this goal is including a regular audit of the vendor and its AI systems as a feature of the vendor contract.