Risk Factors Comparison 2024-02-15 to 2023-02-21 Form: 10-K

Legend: **New Text** ~~Removed Text~~ Unchanged Text Moved Text Section

Investing in our Class A common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below, together with all of the other information in this Annual Report on Form 10- K, including the section titled " Management' s Discussion and Analysis of Financial Condition and Results of Operations " and the consolidated financial statements and related notes. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of or that we deem immaterial may also become important factors that adversely affect our business. If any of the following risks occur, our business, operating results, financial condition, and future prospects could be materially and adversely affected. Many risks affect more than one category, and the risks are not in order of significance or probability of occurrence because they have been grouped by categories. **The** ~~In that event, the~~ market price of our Class A common stock could decline, and you could lose part or all of your investment **due to any of these risks** . Risk Factors ~~Summary Consistent with the foregoing, our business is subject to a number of risks and uncertainties, including those risks discussed at length below. These risks include, among others, the following, which we consider our most material risks: • Our operating results have and will significantly fluctuate, including due to the highly volatile nature of crypto; • Our total revenue is substantially dependent on the prices of crypto assets and volume of transactions conducted on our platform. If such price or volume declines, our business, operating results, and financial condition would be adversely affected; • Our net revenue may be concentrated in a limited number of areas. Within transaction revenue and subscription and services revenue, a meaningful concentration is from transactions in Bitcoin and Ethereum and interest income in connection with USDC, respectively. If revenue from these areas declines and is not replaced by new demand for crypto assets or other products and services, our business, operating results, and financial condition could be adversely affected; • We have in the past, and may in the future, enter into partnerships, collaborations, joint ventures, or strategic alliances with third parties. If we are unsuccessful in establishing or maintaining strategic relationships with these third parties or if these third parties fail to deliver certain operational services, our business, operating results, and financial condition could be adversely affected; • Interest rate fluctuations could negatively impact us; • The future development and growth of crypto is subject to a variety of factors that are difficult to predict and evaluate. If crypto does not grow as we expect, our business, operating results, and financial condition could be adversely affected; • Cyberattacks and security breaches of our platform, or those impacting our customers or third parties, could adversely impact our brand and reputation and our business, operating results, and financial condition; • We are subject to an extensive, highly- evolving and uncertain regulatory landscape and any adverse changes to, or our failure to comply with, any laws and regulations could adversely affect our brand, reputation, business, operating results, and financial condition; • We operate in a highly competitive industry and we compete against unregulated or less regulated companies and companies with greater financial and other resources, and our business, operating results, and financial condition may be adversely affected if we are unable to respond to our competitors effectively; • We compete against a growing number of decentralized and noncustodial platforms and our business may be adversely affected if we fail to compete effectively against them; • As we continue to expand and localize our international activities, our obligations to comply with the laws, rules, regulations, and policies of a variety of jurisdictions will increase and we may be subject to inquiries, investigations, and enforcement actions by U. S. and non- U. S. regulators and governmental authorities, including those related to sanctions, export control, and anti-money laundering; • We are, and may continue to be, subject to material litigation, including individual and class action lawsuits, as well as investigations and enforcement actions by regulators and governmental authorities. These matters are often expensive and time consuming, and, if resolved adversely, could harm our business, financial condition, and operating results; • If we cannot keep pace with rapid industry changes to provide new and innovative products and services, the use of our products and services, and consequently our net revenue, could decline, which could adversely impact our business, operating results, and financial condition; • A particular crypto asset' s status as a " security " in any relevant jurisdiction is subject to a high degree of uncertainty and if we are unable to properly characterize a crypto asset, we may be subject to regulatory scrutiny, inquiries, investigations, fines, and other penalties, which may adversely affect our business, operating results, and financial condition; • We currently rely on third- party service providers for certain aspects of our operations, and any interruptions in services provided by these third parties may impair our ability to support our customers; • Loss of a critical banking or insurance relationship could adversely impact our business, operating results, and financial condition; • Any significant disruption in our products and services, in our information technology systems, or in any of the blockchain networks we support, could result in a loss of customers or funds and adversely impact our brand and reputation and our business, operating results, and financial condition; • Our failure to safeguard and manage our and our customers' fiat currencies and crypto assets could adversely impact our business, operating results, and financial condition; and • The theft, loss, or destruction of private keys required to access any crypto assets held in custody for our own account or for our customers may be irreversible. If we are unable to access our private keys or if we experience a hack or other data loss relating to our ability to access any crypto assets, it could cause regulatory scrutiny, reputational harm, and other losses.~~ The Most Material Risks Related to Our Business and Financial Position Our operating results have and will significantly fluctuate, including due to the highly volatile nature of crypto. Our operating results are dependent on crypto assets and the broader cryptoeconomy. Due to the highly volatile nature of the cryptoeconomy and the prices of crypto assets, which have experienced and continue to experience significant volatility, our operating results have, and will continue to, fluctuate significantly from quarter to quarter in accordance with market sentiments and movements in the broader cryptoeconomy. Our operating results will continue to fluctuate significantly as a result of a

variety of factors, many of which are unpredictable and in certain instances are outside of our control, including: • our dependence on offerings that are dependent on crypto asset trading activity, including trading volume and the prevailing trading prices for crypto assets, whose trading prices and volume can be highly volatile; • our ability to attract, maintain, and grow our customer base and engage our customers; • changes in the legislative or regulatory environment, or actions by U. S. or foreign governments or regulators, including fines, orders, or consent decrees; • regulatory changes **or scrutiny** that impact our ability to offer certain products or services; • our ability to continue to diversify and grow our subscription and services revenue; • our mix of revenue between transaction and subscription and services; • pricing for **or temporary suspensions of** our products and services; • investments we make in the development of products and services as well as technology offered to our developers, international expansion, and sales and marketing; • adding crypto assets to, or removing from **,** our platform; • our ability to establish and maintain partnerships, collaborations, joint ventures, or strategic alliances with third parties; • market conditions of, and overall sentiment towards, the cryptoeconomy; • macroeconomic conditions, including interest rates ~~and ,~~ inflation **and instability in the global banking system** ; • adverse legal proceedings or regulatory enforcement actions, judgments, settlements, or other legal proceeding and enforcement- related costs; • the development and introduction of existing and new products and services by us or our competitors; • our ability to control costs, including our operating expenses incurred to grow and expand our operations and to remain competitive; • system failure, outages or interruptions, including with respect to our crypto platform and third- party crypto networks; • our lack of control over decentralized or third- party blockchains and networks that may experience downtime, cyber- attacks, critical failures, errors, bugs, corrupted files, data losses, or other similar software failures, outages, breaches and losses; • breaches of security or privacy; • inaccessibility of our platform due to our or third- party actions; • our ability to attract and retain talent; and • our ability to compete with our competitors. As a result of these factors, it is difficult for us to forecast growth trends accurately and our business and future prospects are difficult to evaluate, particularly in the short term. In particular, our subscription and services revenue has grown over time **,** with ~~interest income~~ **stablecoin revenue** received in connection with USDC ~~is~~ becoming a more meaningful revenue contributor. Therefore, our operating results could fluctuate significantly as a result of changes in the demand for our subscription and service offerings, in the demand for USDC, **in** the balance of USDC on our platform, in interest rates, and to our ongoing relationships with third parties, such as the issuer of USDC. In view of the rapidly evolving nature of our business and the cryptoeconomy, period- to- period comparisons of our operating results may not be meaningful, and you should not rely upon them as an indication of future performance. Quarterly and annual expenses reflected in our financial statements may be significantly different from historical or projected rates. Our operating results in one or more future quarters may fall below the expectations of securities analysts and investors. As a result, the trading price of our Class A common stock may increase or decrease significantly. Our total revenue is substantially dependent on the prices of crypto assets and volume of transactions conducted on our platform. If such price or volume declines, our business, operating results, and financial condition would be adversely affected **and the price of our Class A common stock could decline** . We generate a large portion of our total revenue from transaction fees on our platform in connection with the purchase, sale, and trading of crypto assets by our customers. Transaction revenue is based on transaction fees that are either a flat fee or a percentage of the value of each transaction. For our consumer trading product, we also charge a spread to ensure that we are able to settle purchases and sales at the price we quote to customers. We also generate a large portion of total revenue from our subscription and services, and such revenue has grown over time, primarily due to ~~interest income~~ **stablecoin revenue** growth in connection with USDC. Declines in the volume of crypto asset transactions, the price of crypto assets, or market liquidity for crypto assets generally may result in lower total revenue to us. The price of crypto assets and associated demand for buying, selling, and trading crypto assets have historically been subject to significant volatility. For instance, in 2017, the value of certain crypto assets, including Bitcoin, experienced steep increases in value, and our customer base expanded worldwide. The increases in value of certain crypto assets, including Bitcoin, from 2016 to 2017, and then again in 2021, were followed by a steep decline in 2018 and again in 2022, which ~~has~~ adversely affected our net revenue and operating results. ~~If~~ **While the value of crypto assets, including Bitcoin, increased towards the end of 2023, if** the value of crypto assets and transaction volume do not **continue to** recover or ~~further~~ decline **in the future** , our ability to generate revenue may suffer and customer demand for our products and services may decline, which could adversely affect our business, operating results and financial condition **and cause the price of our Class A common stock to decline** . The price and trading volume of any crypto asset is subject to significant uncertainty and volatility, depending on a number of factors, including: • market conditions of, and overall sentiment towards, crypto assets and the cryptoeconomy, including, but not limited to, as a result of actions taken by or developments of other companies in the cryptoeconomy; • changes in liquidity, market- making volume, and trading activities; • trading activities on other crypto platforms worldwide, many of which may be unregulated, and may include manipulative activities; • investment and trading activities of highly active consumer and institutional users, speculators, miners, and investors; • the speed and rate at which crypto is able to gain adoption as a medium of exchange, utility, store of value, consumptive asset, security instrument, or other financial assets worldwide, if at all; • decreased user and investor confidence in crypto assets and crypto platforms; • negative publicity and events relating to the cryptoeconomy; • unpredictable social media coverage or " trending " of, or other rumors and market speculation regarding **,** crypto assets; • the ability for crypto assets to meet user and investor demands; • the functionality and utility of crypto assets and their associated ecosystems and networks, including crypto assets designed for use in various applications; • consumer preferences and perceived value of crypto assets and crypto asset markets; • increased competition from other payment services or other crypto assets that exhibit better speed, security, scalability, or other characteristics; • **adverse legal proceedings or regulatory enforcement actions, judgments, or settlements impacting cryptoeconomy participants; •** regulatory or legislative changes **, scrutiny** and updates affecting the cryptoeconomy; • the characterization of crypto assets under the laws of various jurisdictions around the world; • the adoption of unfavorable taxation policies on crypto asset investments by governmental entities; • the maintenance, troubleshooting, and development of the blockchain networks underlying crypto assets, including by miners, validators, and developers worldwide; •

the ability for crypto networks to attract and retain miners or validators to secure and confirm transactions accurately and efficiently; • legal and regulatory changes affecting the operations of miners and validators of blockchain networks, including limitations and prohibitions on mining activities, or new legislative or regulatory requirements as a result of growing environmental concerns around the use of energy in ~~bitcoin~~ **Bitcoin** and other proof- of- work mining activities; • ongoing technological viability and security of crypto assets and their associated smart contracts, applications and networks, including vulnerabilities against hacks and scalability; • fees and speed associated with processing crypto asset transactions, including on the underlying blockchain networks and on crypto platforms; • financial strength of market participants; • the availability and cost of funding and capital; • the liquidity and credit risk of other crypto platforms; • interruptions **or temporary suspensions or other compulsory restrictions** in **products or** ~~service~~ **services** from or failures of major crypto platforms; • availability of an active derivatives market for various crypto assets; • availability of banking and payment services to support crypto- related projects; • **instability in the global banking system and the** level of interest rates and inflation; • monetary policies of governments, trade restrictions, and fiat currency devaluations; and • national and international economic and political conditions. There is no assurance that any supported crypto asset will maintain its value or that there will be meaningful levels of trading activities. In the event that the price of crypto assets or the demand for trading crypto assets decline, our business, operating results, and financial condition would be adversely affected **and the price of our Class A common stock could decline** . Our net revenue may be concentrated in a limited number of areas. Within transaction revenue and subscription and services revenue, a meaningful concentration is from transactions in Bitcoin and Ethereum and ~~interest income~~ **stablecoin revenue** in connection with USDC, respectively. If revenue from these areas declines and is not replaced by new demand for crypto assets or other products and services, our business, operating results, and financial condition could be adversely affected. While we support a diverse portfolio of crypto assets for trading, staking and custody, our net revenue is concentrated in a limited number of areas, such as transactions in Bitcoin and Ethereum for transaction revenue and ~~interest income~~ **stablecoin revenue** in connection with USDC for subscription and services revenue. **Since** ~~For the year ended December 31,~~ 2022, we **have** derived a more meaningful amount of our net revenue from ~~interest income~~ **subscription and services revenue** , primarily **due to stablecoin revenue** in connection with USDC, than we have historically. For the years ended December 31, **2023 and** 2022 ~~and 2021~~ , we derived a meaningful amount of our net revenue from transaction fees generated in connection with the purchase, sale, and trading of Bitcoin and Ethereum; these trading pairs drove approximately **54 % and** 55 ~~% and 45~~ % of total Trading Volume on our platform during these periods, respectively. ~~Moreover, during~~ **During** 2022, the value of Bitcoin and Ethereum declined steeply **. While the value of Bitcoin** and **Ethereum moderately recovered in 2023,** if the value of Bitcoin and Ethereum do not **continue to** recover or ~~further~~ decline **in the future** , our business and operating results could be adversely affected. As such, in addition to the factors impacting the broader cryptoeconomy described in this section, our revenue may be adversely affected if the markets for Bitcoin and Ethereum deteriorate or if their prices decline, including as a result of the following factors: • the reduction in mining rewards of Bitcoin, including block reward halving events, which are events that occur after a specific period of time and reduces the block reward earned by miners; • public sentiment related to the actual or perceived environmental impact of Bitcoin, Ethereum, and related activities, including environmental concerns raised by private individuals and governmental actors related to the energy resources consumed in the Bitcoin mining process; • ~~the launch of Ethereum 2. 0, including~~ the migration of Ethereum to a proof- of- stake model; • disruptions, hacks, splits in the underlying networks also known as " forks ", attacks by malicious actors who control a significant portion of the networks' hash rate such as double spend or 51 % attacks, or other similar incidents affecting the Bitcoin or Ethereum blockchain networks; • hard " forks " resulting in the creation of and divergence into multiple separate networks, such as Bitcoin Cash and Ethereum Classic; • informal governance led by Bitcoin and Ethereum' s core developers that lead to revisions to the underlying source code or inactions that prevent network scaling, and which evolve over time largely based on self- determined participation, which may result in new changes or updates that affect their speed, security, usability, or value; • the ability for Bitcoin and Ethereum blockchain networks to resolve significant scaling challenges and increase the volume and speed of transactions; • the ability to attract and retain developers and customers to use Bitcoin and Ethereum for payment, store of value, unit of accounting, and other intended uses and the absence of another supported crypto asset to attract and retain developers and customers for the same; • transaction congestion and fees associated with processing transactions on the Bitcoin and Ethereum networks and the absence of another supported crypto asset to replace these transactions; • the identification of Satoshi Nakamoto, the pseudonymous person or persons who developed Bitcoin, or the transfer of Satoshi' s Bitcoins; • negative perception of Bitcoin or Ethereum; • development in mathematics, technology, including in digital computing, algebraic geometry, and quantum computing that could result in the cryptography being used by Bitcoin and Ethereum becoming insecure or ineffective; • regulatory ~~or~~ **,** legislative **or other compulsory or informal** restrictions or limitations on Bitcoin or Ethereum lending, mining or staking activities; • liquidity and credit risk issues experienced by other crypto platforms and other participants of the cryptoeconomy; and • laws and regulations affecting the Bitcoin and Ethereum networks or access to these networks, including a determination that either Bitcoin or Ethereum constitutes a security or other regulated financial instrument under the laws of any jurisdiction. Moreover, our subscription and services revenue has grown over time, including ~~interest income~~ **stablecoin revenue** received in connection with USDC. Such revenue depends on a variety of factors, including demand for our subscription and services offerings, demand for USDC, the balance of USDC on our platform, interest rates, and ongoing relationships with third parties, such as the issuer of USDC. If such factors are negatively impacted, our business, operating results and financial condition could be adversely affected. We have in the past, and may in the future, enter into partnerships, collaborations, joint ventures, or strategic alliances with third parties. If we are unsuccessful in establishing or maintaining strategic relationships with these third parties or if these third parties fail to deliver certain operational services, our business, operating results, and financial condition could be adversely affected. We have in the past, and may in the future, enter into partnerships, collaborations, joint ventures, or strategic alliances with third parties in connection with the development,

operation and enhancements to our platform and products and the provision of our services. For example, the issuer of USDC provides us with creation and redemption services for USDC, including the operational capabilities required for our USDC customer- facing services. If the issuer of USDC fails to provide certain operational services, our ability to maintain our current level of offerings and customer experience for USDC could be harmed **and interest or confidence in USDC could be impacted** . Identifying strategic relationships with third parties, and negotiating and documenting relationships with them may be time- consuming and complex and may distract management. Moreover, we may be delayed, or not be successful, in achieving the objectives that we ~~anticipated~~ **anticipate** as a result of such strategic **relationships. In evaluating counterparties in connection with partnerships, collaborations, joint ventures or strategic alliances, we consider a wide range of economic, legal and regulatory criteria depending on the nature of such** relationship **, including the counterparties' reputation, operating results and financial condition, operational ability to satisfy our and our customers' needs in a timely manner, efficiency and reliability of systems, certifications costs to us or to our customers, and licensure and compliance status. Despite this evaluation, third parties may still not meet our or our customers' needs which may adversely affect our ability to deliver products and services to customers, may adversely impact our business, operating results, and financial condition** . Counterparties to any strategic relationship may have economic or business interests or goals that are, or that may become, inconsistent with our business interests or goals, and may subject us to additional risks to the extent such third party becomes the subject of negative publicity, faces its own litigation or regulatory challenges, or faces other adverse circumstances. Conflicts may arise with our strategic partners, such as the interpretation of significant terms under any agreement, which may result in litigation or arbitration which would increase our expenses and divert the attention of our management. If we are unsuccessful in establishing or maintaining strategic relationships with third parties, our ability to compete in the marketplace or to grow our revenue could be impaired and our business, operating results, and financial condition could be adversely affected. Interest rate fluctuations could negatively impact us. The level of prevailing short- term interest rates affects our profitability because we derive a large portion of our revenue from interest earned from funds deposited with us by our customers which we hold on their behalf in custodial accounts at banks and from **stablecoin revenue, which is derived from** interest ~~income~~ earned **on** ~~in connection with~~ USDC **reserve balances** . Higher interest rates increase the amount of interest income **and stablecoin revenue** earned from these activities. When short- term interest rates decline, our revenue derived from interest correspondingly declines, which negatively impacts our profitability. Further, because **stablecoin revenue** ~~interest income, particularly~~ from USDC ~~,~~ has become an increased portion of our subscription and services revenue, if interest rates were to significantly decline from levels reached in ~~2022~~ **the current interest rate environment** , our net revenue could decline. Conversely, when interest rates increase, investors may choose to shift their asset allocations, which could negatively impact our stock price or the cryptoeconomy more generally. The future development and growth of crypto is subject to a variety of factors that are difficult to predict and evaluate. If crypto does not grow as we expect, our business, operating results, and financial condition could be adversely affected. Crypto assets built on blockchain technology were only introduced in 2008 and remain in the early stages of development. In addition, different crypto assets are designed for different purposes. Bitcoin, for instance, was designed to serve as a peer- to- peer electronic cash system, while Ethereum was designed to be a smart contract and decentralized application platform. Many other crypto networks- ranging from cloud computing to tokenized securities networks- have only recently been established. The further growth and development of any crypto assets and their underlying networks and other cryptographic and algorithmic protocols governing the creation, transfer, and usage of crypto assets represent a new and evolving paradigm that is subject to a variety of factors that are difficult to evaluate, including: • many crypto networks have limited operating histories, have not been validated in production, and are still in the process of developing and making significant decisions that will affect the design, supply, issuance, functionality, and governance of their respective crypto assets and underlying blockchain networks, any of which could adversely affect their respective crypto assets; • many crypto networks are in the process of implementing software upgrades and other changes to their protocols, which could introduce bugs, security risks, or adversely affect the respective crypto networks; • several large networks, including Bitcoin and Ethereum, are developing new features to address fundamental speed, scalability, and energy usage issues. If these issues are not successfully addressed, or are unable to receive widespread adoption, it could adversely affect the underlying crypto assets; • security issues, bugs, and software errors have been identified with many crypto assets and their underlying blockchain networks, some of which have been exploited by malicious actors. There are also inherent security weaknesses in some crypto assets, such as when creators of certain crypto networks use procedures that could allow hackers to counterfeit tokens. Any weaknesses identified with a crypto asset could adversely affect its price, security, liquidity, and adoption. If a malicious actor or botnet (a volunteer or hacked collection of computers controlled by networked software coordinating the actions of the computers) obtains a majority of the compute or staking power on a crypto network, as has happened in the past, it may be able to manipulate transactions, which could cause financial losses to holders, damage the network' s reputation and security, and adversely affect its value; • the development of new technologies for mining, such as improved application- specific integrated circuits (commonly referred to as ASICs), or changes in industry patterns, such as the consolidation of mining power in a small number of large mining farms, could reduce the security of blockchain networks, lead to increased liquid supply of crypto assets, and reduce a crypto' s price and attractiveness; • if rewards and transaction fees for miners or validators on any particular crypto network are not sufficiently high to attract and retain miners, a crypto network' s security and speed may be adversely affected, increasing the likelihood of a malicious attack; • many crypto assets have concentrated ownership or an " admin key ", allowing a small group of holders to have significant unilateral control and influence over key decisions related to their crypto networks, such as governance decisions and protocol changes, as well as the market price of such crypto assets; • the governance of many decentralized blockchain networks is by voluntary consensus and open competition, and many developers are not directly compensated for their contributions. As a result, there may be a lack of consensus or clarity on the governance of any particular crypto network, a lack of incentives for developers to maintain or develop the network, and other unforeseen

issues, any of which could result in unexpected or undesirable errors, bugs, or changes, or stymie such network' s utility and ability to respond to challenges and grow; and • many crypto networks are in the early stages of developing partnerships and collaborations, all of which may not succeed and adversely affect the usability and adoption of the respective crypto assets. Various other technical issues have also been uncovered from time to time that resulted in disabled functionalities, exposure of certain users' personal information, theft of users' assets, and other negative consequences, and which required resolution with the attention and efforts of their global miner, user, and development communities. If any such risks or other risks materialize, and in particular if they are not resolved, the development and growth of crypto may be significantly affected and, as a result, our business, operating results, and financial condition could be adversely affected. Cyberattacks and security breaches of our platform, or those impacting our customers or third parties, could adversely impact our brand and reputation and our business, operating results, and financial condition. Our business involves the collection, storage, processing, and transmission of confidential information, customer, employee, service provider, and other personal data, as well as information required to access customer assets. We have built our reputation on the premise that our platform offers customers a secure way to purchase, store, and transact in crypto assets. As a result, any actual or perceived security breach of us or our third- party partners may: • harm our reputation and brand; • result in our systems or services being unavailable and interrupt our operations; • result in improper disclosure of data and violations of applicable privacy and data protection laws; • result in significant regulatory scrutiny, investigations, fines, penalties, and other legal, regulatory, and financial exposure; • cause us to incur significant remediation costs; • lead to theft or irretrievable loss of our or our customers' fiat currencies or crypto assets; • reduce customer confidence in, or decreased use of, our products and services; • divert the attention of management from the operation of our business; • result in significant compensation or contractual penalties from us to our customers or third parties as a result of losses to them or claims by them; and • adversely affect our business and operating results. **For example, in 2021, third parties independently obtained login credentials and personal information for at least 6, 000 customers and used those credentials to exploit a vulnerability that previously existed in the account recovery process. Coinbase reimbursed impacted customers approximately $ 25. 1 million.** Further, any actual or perceived breach or cybersecurity attack directed at other financial institutions or crypto companies, whether or not we are directly impacted, could lead to a general loss of customer confidence in the cryptoeconomy or in the use of technology to conduct financial transactions, which could negatively impact us, including the market perception of the effectiveness of our security measures and technology infrastructure. An increasing number of organizations, including large merchants, businesses, technology companies, and financial institutions, as well as government institutions, have disclosed breaches of their information security systems, some of which have involved sophisticated and highly targeted attacks, including on their websites, mobile applications, and infrastructure. Attacks upon systems across a variety of industries, including the crypto industry, are increasing in their frequency, persistence, and sophistication, and, in many cases, are being conducted by sophisticated, well- funded, and organized groups and individuals, including state actors. The techniques used to obtain unauthorized, improper, or illegal access to systems and information (including customers' personal data and crypto assets), disable or degrade services, or sabotage systems are constantly evolving, may be difficult to detect quickly, and often are not recognized or detected until after they have been launched against a target. These attacks may occur on our systems or those of our third- party service providers or partners. Certain types of cyberattacks could harm us even if our systems are left undisturbed. For example, attacks may be designed to deceive employees and service providers into releasing control of our systems to a hacker, while others may aim to introduce computer viruses or malware into our systems with a view to stealing confidential or proprietary data. Additionally, certain threats are designed to remain dormant or undetectable until launched against a target and we may not be able to implement adequate preventative measures. Although we have developed systems and processes designed to protect the data we manage, prevent data loss and other security breaches, effectively respond to known and potential risks, and expect to continue to expend significant resources to bolster these protections, there can be no assurance that these security measures will provide absolute security or prevent breaches or attacks. We have experienced from time to time, and may experience in the future, breaches of our security measures due to human error, malfeasance, insider threats, system errors or vulnerabilities, or other irregularities. Unauthorized parties have attempted, and we expect that they will continue to attempt, to gain access to our systems and facilities, as well as those of our customers, partners, and third- party service providers, through various means, including hacking, social engineering, phishing, and attempting to fraudulently induce individuals (including employees, service providers, and our customers) into disclosing usernames, passwords, payment card information, or other sensitive information, which may in turn be used to access our information technology systems and customers' crypto assets. Threats can come from a variety of sources, including criminal hackers, hacktivists, state- sponsored intrusions, industrial espionage, and insiders. Certain threat actors may be supported by significant financial and technological resources, making them even more sophisticated and difficult to detect. We may also acquire other companies that expose us to unexpected security risks or increase costs to improve the security posture of the acquired company. Further, there has been an increase in such threat actor activities as a result of the ~~coronavirus or COVID- 19, pandemic~~ **increased prevalence of hybrid and remote working arrangements in recent years** . As a result, our costs and the resources we devote to protecting against these advanced threats and their consequences may continue to increase over time. Although we maintain insurance coverage, it may be insufficient to protect us against all losses and costs stemming from security breaches, cyberattacks, and other types of unlawful activity, or any resulting disruptions **or data theft and loss** from such events. Outages and disruptions of our platform, including any caused by cyberattacks, may harm our reputation and our business, operating results, and financial condition. We are subject to an extensive, highly- evolving and uncertain regulatory landscape and any adverse changes to, or our failure to comply with, any laws and regulations could adversely affect our brand, reputation, business, operating results, and financial condition. Our business is subject to extensive laws, rules, regulations, policies, orders, determinations, directives, treaties, and legal and regulatory interpretations and guidance in the markets in which we operate, including those governing financial services and banking, federal government contractors, trust companies,

securities, derivative transactions and markets, broker- dealers and alternative trading systems (“ ATS ”), commodities, credit, crypto asset custody, exchange, and transfer, cross- border and domestic money and crypto asset transmission, ~~consumer and~~ commercial lending, usury, foreign currency exchange, privacy, data governance, data protection, cybersecurity, fraud detection, payment services (including payment processing and settlement services), consumer protection, escheatment, antitrust and competition, bankruptcy, tax, anti- bribery, economic and trade sanctions, anti- money laundering, and counter- terrorist financing. Many of these legal and regulatory regimes were adopted prior to the advent of the internet, mobile technologies, crypto assets, **generative artificial intelligence (“ AI ”)** and related technologies. As a result, some applicable laws and regulations do not contemplate or address unique issues associated with the cryptoeconomy, are subject to significant uncertainty, and vary widely across U. S. federal, state, and local and international jurisdictions. These legal and regulatory regimes, including the laws, rules, and regulations thereunder, evolve frequently and may be modified, interpreted, and applied in an inconsistent manner from one jurisdiction to another, and may conflict with one another. Moreover, the complexity and evolving nature of our business and the significant uncertainty surrounding the regulation of the cryptoeconomy requires us to exercise our judgment as to whether certain laws, rules, and regulations apply to us, and it is possible that governmental bodies and regulators may disagree with our conclusions. To the extent we have not complied with such laws, rules, and regulations, we could be subject to significant fines, revocation of licenses, limitations on **or temporary or permanent suspensions of** our products and services, reputational harm, and other regulatory consequences, each of which may be significant and could adversely affect our business, operating results, and financial condition. Additionally, various governmental and regulatory bodies, including legislative and executive bodies, in the United States and in other countries may adopt new laws and regulations, the direction and timing of which may be influenced by changes in the governing administrations and major events in the cryptoeconomy. For example, following the failure of several prominent crypto trading venues and lending platforms, such as FTX, Celsius Networks, Voyager and Three Arrows Capital in 2022 (the “ 2022 Events ”), the U. S. Congress expressed the need for both greater federal oversight of the cryptoeconomy and comprehensive cryptocurrency legislation. ~~In~~ **Presently, and in** the ~~near~~ future, various governmental and regulatory bodies, including in the United States, may introduce new policies, laws, and regulations relating to crypto assets and the cryptoeconomy generally, and crypto asset platforms in particular. ~~The~~ **Other companies’** failures of risk management and other control functions ~~at other companies~~ that played a role in the 2022 Events could accelerate an existing regulatory trend toward stricter oversight of crypto asset platforms and the cryptoeconomy. Furthermore, new interpretations of existing laws and regulations may be issued by such bodies or the judiciary, which may adversely impact the development of the cryptoeconomy as a whole and our legal and regulatory status in particular by changing how we operate our business, how our products and services are regulated, and what products or services we and our competitors can offer, requiring changes to our compliance and risk mitigation measures, imposing new licensing requirements, or imposing a total ban on certain crypto asset transactions, as has occurred in certain jurisdictions in the past. For example, **in April 2023, the SEC reopened a comment period for amendments to Rule 3b- 16 under the Securities Exchange Act of 1934, as amended (the “ Exchange Act ”), that could subject several cryptoeconomy participants and systems to registration or other operational compliance requirements under the Exchange Act. If the SEC’ s proposed amendment is adopted in its current form, we, along with other cryptoeconomy participants, could face significant additional uncertainty and risk of increased operational costs. In September 2023, the New York Department of Financial Services (“ NYDFS ”) proposed new guidance regarding the policies and procedures required for virtual currency business entities licensed in New York, such as Coinbase, Inc. This guidance and other applicable state law guidance regarding virtual currency business activity could result in changes to our business in such states as well as the risk of increased operational costs and the risk of enforcement actions. If we are unable to comply with any new requirements, our ability to offer our products and services in their current form may be adversely affected. Additionally,** under recommendations from the Financial Crimes Enforcement Network (“ FinCEN ”), and the Financial Action Task Force (“ FATF ”), the United States and several foreign jurisdictions have or are likely to impose the Funds Travel Rule and the Funds Transfer Rule (commonly referred to collectively as the Travel Rule) on financial service providers in the cryptoeconomy. We may face substantial costs to operationalize and comply with the Travel Rule and may be further subject to administrative sanctions for technical violations or customer attrition if the user experience suffers as a result. In ~~December~~ **October** ~~2020~~ **2023** , FinCEN released a proposed rule that ~~burden for our business in Europe and~~ ,as a result of the fragmented approach to the implementation of its provisions,resulted in distinct and divergent national licensing and registration regimes for us in different E.U.member states.Further E.U.- level legislation imposing additional regulatory requirements in relation to crypto- related activities is also expected in the near term,such as with the ~~effectiveness~~ **enactment** of the Markets in Crypto- Assets Regulation (“ MiCA ”).Among other provisions,MiCA **is expected to** ~~introduces~~ **introduce** a comprehensive authorization and compliance regime for crypto asset service providers and a disclosure regime for the issuers of certain crypto assets,which is expected to impact our operations in the European Union.For example,the requirements of privacy and data protection laws in the European Union,United States,and elsewhere are typically founded on the premise of centralized,data- controller- based data processing,and require fulfilling,among other things,individual rights to access or delete one’ s data.This creates unique compliance challenges given the nature of blockchain’ s peer- to- peer network architecture,lack of centralized control,immutability,and perpetual data storage.Because we have offered and will continue to offer a variety of innovative products and services to our customers,many of our offerings are subject to significant regulatory uncertainty and we from time to time face regulatory inquiries regarding our current and planned products.For instance,we are a **founding member of the Centre Consortium and a** reseller of USDC,a stablecoin redeemable on a one- to- one basis for U.S.dollars.The regulatory treatment of fiat- backed stablecoins is highly uncertain and has drawn significant attention from legislative and regulatory bodies around the world.The issuance and resale of such stablecoins may implicate a variety of banking,deposit,money transmission,prepaid access and stored value,anti- money laundering,commodities,securities,sanctions,and other laws and

regulations in the United States and in other jurisdictions.Moreover,in October 2021,the President' s Working Group on Financial ~~Markets,the Federal~~ would **subject stablecoin issuers and** ~~require us to collect personal information from the owners of self- custodied wallets~~ **wallet providers** ~~that transfer cryptocurrencies~~ to **increased** ~~or receive cryptocurrencies from us, and report certain transactions to the~~ federal ~~government~~ **oversight** . There are substantial uncertainties on how these requirements would apply in practice, and we may face substantial **compliance** costs to operationalize and comply with these rules. Moreover, **our products and services incorporate digital engagement, including recommendations, incentives, notifications, educational content and relevant news. Legislators and regulators in jurisdictions in which we operate have solicited comment from the public or proposed or adopted laws or regulations relating to the use of gamification, predictive analytics or other digital engagement features or practices in various products and services, including potential conflicts of interest that may arise as a result of such practices. If such laws or regulations are adopted in jurisdictions in which we operate and deemed to apply to the products and services** we offer ~~and may in~~ **, we could be required to change** the **way we market** ~~future offer products and services whose functionality or~~ **our offerings** ~~value depends in part on our management of token transaction smart contracts, liquid staking, asset tracking, or other applications that provide novel forms of customer engagement~~ and ~~interaction delivered via blockchain protocols. We may also offer products and services whose functionality or value depends on our ability to develop, integrate, or otherwise~~ interact with ~~such applications~~ **existing and prospective customers or modify certain features contained** within ~~the bounds of~~ our ~~legal and compliance obligations. The legal and regulatory landscape for such~~ products ~~, including the law governing the rights~~ and **services, any of** ~~obligations between and among smart contract developers and users and the extent to~~ which ~~such relationships entail regulated activity is uncertain and rapidly evolving. Our interaction with those applications, and the interaction of other blockchain users with any smart contracts or assets we may generate or control,~~ could **adversely impact** ~~present legal, operational, reputational, and regulatory risks for~~ our business **, operating** ~~. We may be further subject to administrative sanctions for technical violations or customer attrition if the user experience suffers as a result~~ **results** ~~. As another example, the recent extension of anti- money laundering requirements to certain crypto- related activities by the European Union' s Fifth Money Laundering Directive has increased the regulatory compliance burden for our business in Europe~~ and , as a result of the fragmented..... President' s Working Group on Financial **financial condition** ~~Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, issued a joint report that recommended legislation that would subject stablecoin issuers and wallet providers to increased federal oversight. There are substantial uncertainties on how these requirements would apply in practice, and we may face substantial compliance costs to operationalize and comply with these rules~~ . Certain products and services offered by us that we believe are not subject to regulatory oversight, or are only subject to certain regulatory regimes, such as Coinbase Wallet, a standalone mobile application that allows customers to manage their own private keys and store their crypto assets directly on their mobile devices, may cause us to be deemed to be engaged in a form of regulated activity for which licensure is required or cause us to become subject to new and additional forms of regulatory oversight. We also offer various staking, rewards, and lending products, all of which are subject to significant regulatory uncertainty, and could implicate a variety of laws and regulations worldwide. For example, there is regulatory uncertainty regarding the status of our staking, lending, rewards, and other yield- generating activities under the U. S. federal and state securities laws. While we have implemented policies and procedures, including geofencing for certain products and services, designed to help monitor for and ensure compliance with existing and new laws and regulations, there can be no assurance that we and our employees, contractors, and agents will not violate or otherwise fail to comply with such laws and regulations. To the extent that we or our employees, contractors, or agents are deemed or alleged to have violated or failed to comply with any laws or regulations, including related interpretations, orders, determinations, directives, or guidance, we or they could be subject to a litany of civil, criminal, and administrative fines, penalties, orders and actions, including being required to suspend or terminate the offering of certain products and services. Moreover, to the extent our customers nevertheless access our platform, products or services outside of jurisdictions where we have obtained required governmental licenses and authorization, we could similarly be subject to a variety of civil, criminal, and administrative fines, penalties, orders and actions as a result of such activity. Due to our business activities, we are subject to ongoing examinations, oversight, and reviews and currently are, and expect in the future, to be subject to investigations and inquiries, by U. S. federal and state regulators and foreign financial service regulators, many of which have broad discretion to audit and examine our business. We are periodically subject to audits and examinations by these regulatory authorities. As a result of findings from these audits and examinations, regulators have, are, and may in the future require us to take certain actions, including amending, updating, or revising our compliance measures from time to time, limiting the kinds of customers that we provide services to, changing, terminating, or delaying our licenses and the introduction of our existing or new product and services, and undertaking further external audit or being subject to further regulatory scrutiny, including investigations and inquiries. We have received, and may in the future receive, examination reports citing violations of rules and regulations, inadequacies in existing compliance programs, and requiring us to enhance certain practices with respect to our compliance program, including due diligence, monitoring, training, reporting, and recordkeeping. Implementing appropriate measures to properly remediate these examination findings may require us to incur significant costs, and if we fail to properly remediate any of these examination findings, we could face civil litigation, significant fines, damage awards, forced removal of certain employees including members of our executive team, barring of certain employees from participating in our business in whole or in part, revocation of existing licenses, limitations on existing and new products and services, reputational harm, negative impact to our existing relationships with regulators, exposure to criminal liability, or other regulatory consequences. ~~For example, in January 2023, we settled a New York Department of Financial Services (" NYDFS ") compliance investigation for a monetary penalty of $ 50 million and a separate commitment to make $ 50 million in compliance program investments by the end of 2024.~~ Further, we believe increasingly strict legal and regulatory requirements and additional regulatory investigations and enforcement, any of which could occur or intensify, may continue to result in changes to our

business, as well as increased costs, and supervision and examination for ourselves, our agents, and service providers **. For example, in June 2023, the SEC filed a complaint in the U. S. District Court for the Southern District of New York against us and Coinbase, Inc. alleging that (i) Coinbase, Inc. has acted as an unregistered securities exchange, broker, and clearing agency in violation of Sections 5, 15 (a) and 17A (b) of the Exchange Act and that, through its staking program, Coinbase, Inc. has offered and sold securities without registering its offers and sales in violation of Sections 5 (a) and 5 (c) of the Securities Act of 1933, as amended (the " Securities Act "), and (ii) we are liable for the alleged violations as an alleged control person of Coinbase, Inc. (the " June 2023 SEC Complaint ")** . Moreover, new laws, regulations, or interpretations may result in additional litigation, regulatory investigations, and enforcement or other actions, including preventing or delaying us from offering certain products or services offered by our competitors or could impact how we offer such products and services. Adverse changes to, or our failure to comply with, any laws and regulations have had, and may continue to have, an adverse effect on our reputation and brand and our business, operating results, and financial condition. We operate in a highly competitive industry and we compete against unregulated or less regulated companies and companies with greater financial and other resources, and our business, operating results, and financial condition may be adversely affected if we are unable to respond to our competitors effectively. The cryptoeconomy is highly innovative, rapidly evolving, and characterized by healthy competition, experimentation, changing customer needs, frequent introductions of new products and services, and subject to uncertain and evolving industry and regulatory requirements. We expect competition to further intensify in the future as existing and new competitors introduce new products or enhance existing products. We compete against a number of companies operating both within the United States and abroad, and both those that focus on traditional financial services and those that focus on crypto- based services. Our main competition falls into the following categories: • traditional financial technology and brokerage firms that have entered the crypto asset market in recent years and offer overlapping features targeted at our customers; • companies focused on the crypto asset market, some of whom adhere to local regulations and directly compete with our platform, and ~~many~~ **others** who choose to operate outside of local rules and regulations or in jurisdictions with less stringent local rules and regulations and are potentially able to more quickly adapt to trends, support a greater number of crypto assets, and develop new crypto- based products and services due to a different standard of regulatory scrutiny; • crypto- focused companies and traditional financial incumbents that offer point or siloed solutions specifically targeted at institutional customers; and • stablecoins, other than USDC, and fiat currencies globally. Historically, a major source of competition has been from companies, in particular those located outside the United States, who **at times** are **and may in the future be** subject to significantly less stringent regulatory and compliance requirements in their local jurisdictions. Their business models rely on being unregulated or only regulated in a small number of lower compliance jurisdictions, whilst also offering their products in highly regulated jurisdictions, including the United States, without necessarily complying with the relevant regulatory requirements in such jurisdictions. **Given the uneven** ~~To date, due to limited~~ enforcement by United States and foreign regulators, many of these competitors have been able to operate from offshore while offering large numbers of products and services to consumers, including in the United States, Europe, and other highly regulated jurisdictions, without complying with the relevant licensing and other requirements in these jurisdictions, and ~~seemingly~~ **historically** without penalty. Due to our regulated status in several jurisdictions and our commitment to legal and regulatory compliance, we have not been able to offer many popular products and services, including products and services that our unregulated or less regulated competitors are able to offer to a group that includes many of our customers, which may adversely impact our business, financial condition, and results of operations. We also have expended significant managerial, operational, and compliance costs to meet the legal and regulatory requirements applicable to us in the United States and other jurisdictions in which we operate, and expect to continue to incur significant costs to comply with these requirements, which these unregulated or less regulated competitors have not had to incur. Additionally, due to the broad nature of our products and services, we also compete with, and expect additional competition from, digital and mobile payment companies and other traditional financial services companies. Many innovative start- up companies and larger companies have made, and continue to make, significant investments in research and development, and we expect these companies to continue to develop similar or superior products and technologies that compete with our products. Further, more traditional financial and non- financial services businesses may choose to offer crypto-based services in the future as the industry gains adoption. Our current and potential competitors may establish cooperative relationships among themselves or with third parties that may further enhance their resources. Our existing competitors have, and our potential competitors are expected to have, various competitive advantages over us, such as: • the ability to trade crypto assets and offer products and services that we do not support or offer on our platform (due to constraints from regulatory authorities, our banking partners, and other factors) such as tokens that constitute securities or derivative instruments under U. S. or foreign laws; • greater name recognition, longer operating histories, larger customer bases, and larger market shares; • larger sales and marketing budgets and organizations; • more established marketing, banking, and compliance relationships; • greater customer support resources; • greater resources to make acquisitions; • lower labor, compliance, risk mitigation, and research and development costs; • larger and more mature intellectual property portfolios; • greater number of applicable licenses or similar authorizations; • established core business models outside of the trading of crypto assets, allowing them to operate on lesser margins or at a loss; • operations in certain jurisdictions with lower compliance costs and greater flexibility to explore new product offerings; and • substantially greater financial, technical, and other resources. If we are unable to compete successfully, or if competing successfully requires us to take costly actions in response to the actions of our competitors, our business, operating results, and financial condition could be adversely affected. We compete against a growing number of decentralized and noncustodial platforms and our business may be adversely affected if we fail to compete effectively against them. We also compete against an increasing number of decentralized and noncustodial platforms. On these platforms, users can interact directly with a market- making smart contract or ~~on- chain~~ **onchain** trading mechanism to exchange one type of crypto asset for another without any centralized intermediary. These platforms are typically not as easy to use as our platform, and some lack the

speed and liquidity of centralized platforms, but various innovative models and incentives have been designed to bridge the gap. In addition, such platforms have low startup and entry costs as market entrants often remain unregulated and have minimal operating and regulatory costs. A significant number of decentralized platforms have recently been developed and released, including on Ethereum, Tron, Polkadot, and Solana, and many such platforms have experienced significant growth and adoption. For instance, we have seen increased interest in certain decentralized platforms with transaction volumes rivaling our own platform on multiple occasions, and expect interest in decentralized and noncustodial platforms to grow further as the industry develops. If the demand for decentralized platforms grows and we are unable to compete with these decentralized and noncustodial platforms, our business may be adversely affected. As we continue to expand and localize our international activities, our obligations to comply with the laws, rules, regulations, and policies of a variety of jurisdictions will increase and we may be subject to inquiries, investigations, and enforcement actions by U. S. and non- U. S. regulators and governmental authorities, including those related to sanctions, export control, and anti- money laundering. As we expand and localize our international activities, we have become increasingly obligated to comply with the laws, rules, regulations, policies, and legal interpretations of both the jurisdictions in which we operate and those into which we offer services on a cross- border basis. For instance, financial regulators outside the United States have increased their scrutiny of crypto asset exchanges over time, such as by requiring crypto asset exchanges operating in their local jurisdictions to be regulated and licensed under local laws. Moreover, laws regulating financial services, the internet, mobile technologies, crypto, and related technologies outside of the United States are highly evolving, extensive and often impose different, more specific, or even conflicting obligations on us, as well as broader liability. In addition, we are required to comply with laws and regulations related to economic sanctions and export controls enforced by **the U. S. Department of the Treasury' s Office of Foreign Assets Control (" OFAC "), the** U. S. Department of Commerce' s Bureau of Industry and Security, and U. S. anti- money laundering and counter- terrorist financing laws and regulations, enforced by FinCEN and certain state financial services regulators. U. S. sanctions and export control laws and regulations generally restrict dealings by persons subject to U. S. jurisdiction with certain jurisdictions that are the target of comprehensive embargoes, currently the Crimea Region, the Donetsk People ~~'~~**'** s Republic ~~(DNR)~~, and the Luhansk People ~~'~~**'** s Republic ~~(LNR)~~ of Ukraine, Cuba, Iran, North Korea, and Syria, as well as with persons, entities, and governments identified on certain prohibited party lists. Moreover, as a result of the Russian invasion of Ukraine, the United States, the E. U., the United Kingdom, and other jurisdictions have imposed wide- ranging sanctions on Russia and Belarus and persons and entities associated with Russia and Belarus. There can be no certainty regarding whether such governments or other governments will impose additional sanctions, or other economic or military measures against Russia or Belarus. We have continued to engage in activity in Russia and Belarus and with customers associated with these countries. At the same time, we have implemented additional processes and procedures to **comply** ~~further compliance~~ with these new sanctions. However, our activity in Russia and Belarus and with these customers associated with these countries subjects us to further exposure to sanctions as they are released. We have an OFAC compliance program in place that includes monitoring of IP addresses to identify prohibited jurisdictions and of blockchain addresses that have either been identified by OFAC as prohibited or that otherwise are believed by us to be associated with prohibited persons or jurisdictions. Nonetheless, there can be no guarantee that our compliance program will prevent transactions with particular persons or addresses or prevent every potential violation of OFAC sanctions. From time to time, we have submitted voluntary disclosures to OFAC or responded to administrative subpoenas from OFAC. Certain of these voluntary self- disclosures are currently under review by OFAC. To date, none of those proceedings has resulted in a monetary penalty or finding of violation. Any present or future government inquiries relating to sanctions could result in negative consequences for us, including costs related to government investigations, financial penalties, and harm to our reputation. The impact on us related to such matters could be substantial. Although we have implemented controls, and are working to implement additional controls and screening tools designed to prevent sanctions violations, there is no guarantee that we will not inadvertently provide access to our products and services to sanctioned parties or jurisdictions in the future. Regulators worldwide frequently study each other' s approaches to the regulation of the cryptoeconomy. Consequently, developments in any jurisdiction may influence other jurisdictions. New developments in one jurisdiction may be extended to additional services and other jurisdictions. As a result, the risks created by any new law or regulation in one jurisdiction are magnified by the potential that they may be replicated, affecting our business in another place or involving another service. Conversely, if regulations diverge worldwide, we may face difficulty adjusting our products, services, and other aspects of our business with the same effect. These risks are heightened as we face increased competitive pressure from other similarly situated businesses that engage in regulatory arbitrage to avoid the compliance costs associated with regulatory changes. The complexity of U. S. federal and state and international regulatory and enforcement regimes, coupled with the global scope of our operations and the evolving global regulatory environment, could result in a single event prompting a large number of overlapping investigations and legal and regulatory proceedings by multiple government authorities in different jurisdictions. Any of the foregoing could, individually or in the aggregate, harm our reputation, damage our brand and business, and adversely affect our operating results and financial condition. Due to the uncertain application of existing laws and regulations, it may be that, despite our regulatory and legal analysis concluding that certain products and services are currently unregulated, such products or services may indeed be subject to financial regulation, licensing, or authorization obligations that we have not obtained or with which we have not complied. As a result, we are at a heightened risk of enforcement action, litigation, regulatory, and legal scrutiny which could lead to sanctions, cease and desist orders, or other penalties and censures which could significantly and adversely affect our continued operations and financial condition. We are, and may continue to be, subject to material litigation, including individual and class action lawsuits, as well as investigations and enforcement actions by regulators and governmental authorities. These matters are often expensive and time consuming, and, if resolved adversely, could harm our business, financial condition, and operating results. We have been, currently are, and may from time to time become subject to claims, arbitrations, individual and class action lawsuits with respect to a variety of matters, including employment, consumer

protection, advertising, and securities. In addition, we have been, currently are, and may from time to time become subject to, government and regulatory investigations, inquiries, actions or requests, other proceedings and enforcement actions alleging violations of laws, rules, and regulations, both foreign and domestic. For example, in January 2023, we settled ~~an~~ **a** NYDFS compliance investigation for a monetary penalty of $ 50 **. 0** million and a separate commitment to make $ 50 **. 0** million in compliance program investments by the end of 2024. **In June 2023, the SEC filed the June 2023 SEC Complaint, in connection with which the SEC is seeking, among other relief, injunctive relief, disgorgement, and civil money penalties, and we and Coinbase, Inc. subsequently filed an answer to the June 2023 SEC Complaint. In August 2023, we and Coinbase, Inc. also filed a motion for judgment on the pleadings. In October 2023, the SEC filed its response and we and Coinbase, Inc. filed our reply. Oral argument took place on January 17, 2024. The impact of the litigation relating to the June 2023 SEC Complaint, including the costs, timing, results and other potential consequences thereof, are unknown at this time. An adverse resolution of the June 2023 SEC Complaint could have a material impact on our business, operating results and financial condition.** Additionally, we are currently subject to securities class actions and shareholder derivative actions. **Furthermore, in June 2023, we and Coinbase, Inc. were issued notices, show- cause orders, and cease- and- desist letters, and became the subject of various legal actions initiated by U. S. state securities regulators in the states of Alabama, California, Illinois, Kentucky, Maryland, New Jersey, South Carolina, Vermont, Washington and Wisconsin alleging violations of state securities laws with respect to staking services provided by Coinbase, Inc. (the " State Staking Actions "). In July 2023, we and Coinbase, Inc. entered into agreements with state securities regulators in California, New Jersey, South Carolina and Wisconsin, pursuant to which customers in those states will no longer be able to stake new funds, in each case pending final adjudication of the matters. In October 2023, we and Coinbase, Inc. entered into a similar agreement with the Maryland state securities regulator.** For a description of certain such litigation, regulatory investigations, and other proceedings, ~~please~~ see Note ~~21~~ **22** . Commitments and Contingencies, ~~in~~ **of** the Notes to our consolidated financial statements included in Part II, Item 8 of this Annual Report on Form 10- K. The scope, determination, and impact of claims, lawsuits, government and regulatory investigations, enforcement actions, disputes, and proceedings to which we are subject cannot be predicted with certainty, and may result in: • substantial payments to satisfy judgments, fines, or penalties; • substantial outside counsel, advisor, and consultant fees and costs; • substantial administrative costs, including arbitration fees; • additional compliance and licensure requirements; • loss or non- renewal of existing licenses or authorizations, or prohibition from or delays in obtaining additional licenses or authorizations, required for our business; • loss of productivity and high demands on employee time; • criminal sanctions or consent decrees; • termination of certain employees, including members of our executive team; • barring of certain employees from participating in our business in whole or in part; • orders that restrict our business or prevent us from offering certain products or services; • changes to our business model and practices; • delays to planned transactions, product launches or improvements; and • damage to our brand and reputation. Because of our large customer base, actions against us may claim large monetary damages, even if the alleged per- customer harm is small or non- existent. From time to time, we receive letters alleging claims on behalf of our users. Due to our large customer base, the ongoing defense and resolution or settlement of these alleged claims could be material and we may incur significant expenses associated with arbitrating or litigating the claims. Moreover, to the extent ~~the current~~ **that a** deterioration of the crypto asset market ~~continues~~ **occurs** for a prolonged period, large platforms like us may become subject to or the target of increased litigation and additional government and regulatory scrutiny. Regardless of the outcome, any such matters can have an adverse impact, which may be material, on our business, operating results, or financial condition because of legal costs, diversion of management resources, reputational damage, and other factors. If we cannot keep pace with rapid industry changes to provide new and innovative products and services, the use of our products and services, and consequently our net revenue, could decline, which could adversely impact our business, operating results, and financial condition. Our industry has been characterized by many rapid, significant, and disruptive products and services in recent years. These include decentralized applications, DeFi, yield farming, non- fungible tokens (" NFTs "), play- to- earn games, lending, staking, token wrapping, governance tokens, innovative programs to attract customers such as transaction fee mining programs, initiatives to attract traders such as trading competitions, airdrops and giveaways, staking reward programs, **" layer 2 " blockchain networks,** and novel cryptocurrency fundraising and distribution schemes, such as " initial exchange offerings. " We expect new services and technologies to continue to emerge and evolve, which may be superior to, or render obsolete, the products and services that we currently provide **. For example, disruptive technologies such as generative AI may fundamentally alter the use of our products or services in unpredictable ways** . We cannot predict the effects of new services and technologies on our business. However, our ability to grow our customer base and net revenue will depend heavily on our ability to innovate and create successful new products and services, both independently and in conjunction with third- party developers. In particular, developing and incorporating new products and services into our business may require substantial expenditures, take considerable time, and ultimately may not be successful. Any new products or services could fail to attract customers, generate revenue, or perform or integrate well with third- party applications and platforms. In addition, our ability to adapt and compete with new products and services may be inhibited by regulatory requirements and general uncertainty in the law, constraints by our banking partners and payment processors, third- party intellectual property rights, or other factors. Moreover, we must continue to enhance our technical infrastructure and other technology offerings to remain competitive and maintain a platform that has the required functionality, performance, capacity, security, and speed to attract and retain customers, including large, institutional, high- frequency and high- volume traders. As a result, we expect to incur significant costs and expenses to develop and upgrade our technical infrastructure to meet the evolving needs of the industry. Our success will depend on our ability to develop and incorporate new offerings and adapt to technological changes and evolving industry practices. If we are unable to do so in a timely or cost- effective manner, our business and our ability to successfully compete, to retain existing customers, and to attract new customers may be adversely affected. A particular crypto asset **, product or service** ' s status as a " security "

in any relevant jurisdiction is subject to a high degree of uncertainty and if we are unable to properly characterize a crypto asset or product offering, we may be subject to regulatory scrutiny, inquiries, investigations, fines, and other penalties, which may adversely affect our business, operating results, and financial condition. The ~~Securities and Exchange Commission (the " SEC ")~~ and its staff have taken the position that ~~certain~~ **a range of** crypto assets **, products and services** fall within the definition of a " security " under the U. S. federal securities laws **. Despite the SEC being the principal federal securities law regulator in the United States, whether or not an asset, product or service is a security or constitutes a securities offering under federal securities laws is ultimately determined by a federal court** . The legal test for determining whether any given crypto asset **, product or service** is a security ~~is~~ **was set forth in the 1946 Supreme Court case SEC v. W. J. Howey Co. and requires** a highly complex, fact- driven analysis **. Accordingly, whether any given crypto asset, product or service would be ultimately deemed to be a security is uncertain and difficult to predict notwithstanding the conclusions of the SEC or any conclusions we may draw based on our risk- based assessment regarding the likelihood** that ~~evolves over time~~ **a particular crypto asset** , ~~and the outcome is difficult to predict~~ **product or service could be deemed a " security " or " securities offering " under applicable laws** . The SEC generally does not provide advance guidance or confirmation on **its assessment of** the status of any particular crypto asset **, product or service** as a security. Furthermore, the SEC' s views in this area have evolved over time **,** and **, at times, have appeared contradictory** ~~it is difficult to predict the direction or timing of any continuing evolution~~ . It is also possible that a change in the governing administration or the appointment of new SEC commissioners could substantially impact the ~~views of~~ **approach to enforcement by** the SEC and its staff. ~~For example, Chair Gary Gensler has repeatedly remarked on the need for further regulatory oversight on crypto assets, crypto trading, and lending platforms by the SEC. Public statements made in the past by senior officials at the SEC have indicated that the SEC does not intend to take the position that Bitcoin or Ethereum are securities (in their current form). In May 2022, the Chair of the U. S. Commodity Futures Trading Commission (the " CFTC "), Rostin Behnam, stated that Bitcoin and Ethereum are commodities. However, in June 2022, Mr. Gensler suggested that Bitcoin is a commodity but did not opine on the status of other crypto assets. In September 2022, Mr. Gensler suggested that he~~ **The** ~~believes a vast majority of cryptocurrencies are securities. Such statements by officials at the CFTC and SEC are not official policy statements by these agencies and reflect only the speakers' views, which are not binding on any agency or court and cannot be generalized to any other crypto asset. In addition, in July 2022, the SEC separately filed securities fraud charges against a former employee related to misuse of confidential Coinbase information. These SEC charges allege that nine crypto assets involved in this matter are securities under federal securities laws, seven of which are, or were, listed on our platform: AMP, RLY, DDX, XYO, RGT, LCX, POWR. Despite the SEC being the principal federal securities law regulator in the United States, whether or not an asset is a security under federal securities laws is ultimately determined by a federal court. No court ruling has yet been made in connection with these seven crypto assets. With respect to these and other crypto assets, there is currently no certainty under the applicable legal test that such assets are not securities, notwithstanding the conclusions we may draw based on our risk- based assessment regarding the likelihood that a particular crypto asset could be deemed a " security " under applicable laws. Similarly, though the~~ SEC' s Strategic Hub for Innovation and Financial Technology published a framework for analyzing whether any given crypto asset is a security in April 2019 **. The SEC has also recently brought enforcement actions and entered into settlements with numerous cryptoeconomy participants alleging that certain digital assets are securities** , ~~this~~ **including the June 2023 Complaint. These statements,** framework ~~is also~~ **and enforcement actions are** not ~~a rule~~ **rules** ~~,~~ **or** ~~regulation~~ **regulations** ~~or statement~~ of the SEC and ~~is~~ **are** not binding on the SEC **. There is currently no certainty under the SEC' s application of the applicable legal test as to whether particular crypto assets, products or services are not securities. Moreover, the SEC and the Commodities Futures Trading Commission (the " CFTC ") and their senior officials have, at times, taken conflicting positions in speeches and enforcement actions as to whether a particular crypto asset is a security or commodity** . Several foreign jurisdictions have taken a broad- based approach to classifying crypto assets **, products and services** as " securities, " while other foreign jurisdictions, such as Switzerland, Malta, and Singapore, have adopted a narrower approach. As a result, certain crypto assets **, products or services** may be deemed to be a " security " under the laws of some jurisdictions but not others. Various foreign jurisdictions may, in the future, adopt additional laws, regulations, or directives that affect the characterization of crypto assets **, products or services** as " securities. " The classification of a crypto asset **, product or service** as a security under applicable law has wide- ranging implications for the regulatory obligations that flow from the offer, sale, trading, and clearing **, as applicable,** of such assets **, products or services** . For example, a crypto asset **, product or service** that is a security in the United States may generally only be offered or sold in the United States pursuant to a registration statement filed with the SEC or in an offering that qualifies for an exemption from registration. Persons that effect transactions in crypto assets **, products or services** that are securities in the United States may be subject to registration with the SEC as a " broker " or " dealer. " Platforms that bring together purchasers and sellers to trade crypto assets that are securities in the United States are generally subject to registration as national securities exchanges, or must qualify for an exemption, such as by being operated by a registered broker- dealer as an ATS in compliance with rules for ATSs. Persons facilitating clearing and settlement of securities may be subject to registration with the SEC as a clearing agency. Foreign jurisdictions may have similar licensing, registration, and qualification requirements. We have policies and procedures to analyze whether each crypto asset that we seek to facilitate trading **of** on Coinbase Spot Market **, as well as our products and services,** could be deemed to be a " security " under applicable laws. Our policies and procedures do not constitute a legal standard, but rather represent our company- developed model, which we use to make a risk- based assessment regarding the likelihood that a particular crypto asset **, product or service** could be deemed a " security " under applicable laws. ~~Regardless of our conclusions, we could be subject to legal or regulatory action in the event the SEC, a state or foreign regulatory authority, or a court were to determine that a supported crypto asset currently offered, sold, or traded on our platform is a " security " under applicable laws. As discussed above, the SEC brought an enforcement action in July 2022 against a third party that alleges that seven crypto assets that are, or~~

~~were, trading on our platform are securities. Such enforcement action may increase the risk that the SEC decides to bring an enforcement action against us for facilitating trading in these crypto assets on the basis that our platform is not registered as a national securities exchange or ATS.~~ Because Coinbase Spot Market, Coinbase Prime and Coinbase app are not registered or licensed with the SEC or foreign authorities as a broker- dealer, national securities exchange, or ATS (or foreign equivalents), we only permit trading of those crypto assets **, and offer products and services,** for which we determine there are reasonably strong arguments to conclude that the crypto asset **, product or service** is not a security. We believe that our process reflects a comprehensive and thoughtful analysis and is reasonably designed to facilitate consistent application of available legal guidance ~~to~~ **on** crypto assets **, products and services and** to facilitate informed risk- based business judgment. In addition, as we shared in our petition for SEC rulemaking, we remain open to registering or relying on an exemption to facilitate and offer the sale of crypto asset securities. We recognize that the application of securities laws to the specific facts and circumstances of crypto assets **, products and services** may be complex and subject to change, and that a listing determination does not guarantee any conclusion under the U. S. federal securities laws. **Regardless of our conclusions, we have been, and could in the future be, subject to legal** ~~For~~ **or** ~~example,~~ **regulatory action** in ~~December 2020~~ **the event the SEC or a state or foreign regulatory authority were to assert** , ~~we announced~~ **or a court were to determine,** that ~~we had made~~ a ~~decision to suspend all XRP trading pairs~~ **supported crypto asset, product or service offered, sold, or traded** on our platform **or a product or service that we offer is a** ~~in light of the SEC' s lawsuit filed against Ripple Labs, Inc. (~~ " ~~Ripple~~ **security** " **under applicable** ~~) and two of its executives, alleging that they have engaged in an unregistered, ongoing securities offering through the sale of XRP. The SEC' s litigation with Ripple is still pending resolution. Further, the SEC may file similar lawsuits against issuers of other crypto assets, which may cause us to reevaluate our support for such assets, and, potentially, decide to suspend listing such assets or assets with similar characteristics on our platform or suspend support for products related to such assets. Additionally, as discussed above, in July 2022, the SEC filed securities fraud charges against one of our former employees and, as part of that complaint, alleged that seven of the digital assets that are, or were, listed on our platform and traded by the former employee are securities. We expect our risk assessment policies and procedures to continuously evolve to take into account case law~~ **laws** ~~, facts, and developments in technology~~ . There can be no ~~assurances~~ **assurance** that we will properly characterize over time any given crypto asset ~~or~~ **,** product **or service** offering as a security or non- security ~~for purposes of determining whether Coinbase Spot Market will support trading of the crypto asset or product offering of the program~~ , or that the SEC, foreign regulatory authority, or a court **having final determinative authority on the topic** , if the question was presented to it, would agree with our assessment. ~~For example~~ **We expect our risk assessment policies and procedures to continuously evolve to take into account case law** , **legislative developments, facts, and developments** in ~~February~~ **technology. In June** 2023, the SEC ~~entered into~~ **filed the June 2023 SEC Complaint. We and Coinbase, Inc. subsequently filed an answer to the June 2023 SEC Complaint in June 2023. In August 2023, we and Coinbase, Inc. also filed** a ~~settlement agreement with Kraken after alleging~~ **motion for judgment on the pleadings. In October 2023, the SEC filed** its **response** ~~staking- as- a- service program constituted an~~ **and** ~~offering~~ **we** and ~~sale of securities. Pursuant to the settlement agreement, Kraken committed to cease offering or selling securities through its crypto asset staking services or staking programs in the United States.~~ Coinbase ~~also has a staking program~~ , **Inc. filed** ~~which meaningfully differs from Kraken' s and does not constitute an offering or~~ **our reply** ~~sale of securities~~ . ~~Specifically~~ **Oral argument took place on January 17** , **2024. Additionally** ~~while Kraken itself determined the rewards customers of its staking program received~~ , **in June 2023, we and** Coinbase ~~pays rewards as set by the protocol~~ , **Inc** ~~minus our disclosed, flat- rate commission~~ . **became** ~~However,~~ the **subject of** ~~SEC may not agree with our assessment. Additionally, in February 2023,~~ the **State Staking** ~~SEC issued a Wells notice to the Paxos Trust Company, LLC (" Paxos "), which Paxos claims pertains to a potential SEC action~~ **Actions** ~~alleging BUSD, a stablecoin that we currently list for trading on our platform, is a security. As a result, it is unclear if the SEC would take a similar view or action with respect to other crypto assets. Further, the SEC may disagree with our prior assessments concerning XRP and the seven digital assets flagged in July 2022 and believe these crypto assets are securities~~ . If an applicable regulatory authority or a court, in either case having final determinative authority on the topic, were to determine that a supported crypto asset **, product or service** currently offered, sold, or traded on our platform is a security, we would not be able to offer such crypto asset for trading **, or product or service on our platform,** until we are able to do so in a compliant manner. A determination by the SEC, a state or foreign regulatory authority, or a court that an asset that we currently support for trading on our platform **, or product or service that we offer on our platform,** constitutes a security may result in **us** removing that crypto asset from **or ceasing to offer that product or service on** our platform, and may also result in us determining that it is advisable to remove assets from our platform **, or to cease offering products and services on our platform,** that have similar characteristics to the asset **, product or service** that was alleged or determined to be a security. Alternatively, we may determine not to remove a particular crypto asset from Coinbase Spot Market **or to continue to offer a product or service on our platform** even if the SEC or another regulator alleges that the crypto asset **, product or service** is a security, pending a final judicial determination as to that crypto asset **, product or service** ' s proper characterization, and the fact that we waited for a final judicial determination would generally not preclude penalties or sanctions against us for our having previously made our platform available for trading that crypto asset **or offering that product or service on our platform** without registering as a national securities exchange or ATS or registering tokens that we may issue, such as our cbETH token **or our staking services** , with the SEC. As such, we could be subject to judicial or administrative sanctions for failing to offer or sell the crypto asset **, product or service** in compliance with the registration requirements, or for acting as a broker, dealer, or national securities exchange without appropriate registration **, including in connection with the June 2023 SEC Complaint** . Such an action could result in injunctions, cease and desist orders, as well as civil monetary penalties, fines, and disgorgement, criminal liability, and reputational harm. Customers that traded such supported crypto asset on our platform and suffered trading losses could also seek to rescind a transaction that we facilitated on the basis that it was conducted in violation of applicable law, which could subject us to significant liability. We

may also be required to cease facilitating transactions in the supported crypto asset other than via our licensed subsidiaries, which could negatively impact our business, operating results, and financial condition. Additionally, the SEC has brought and may in the future bring enforcement actions against other cryptoeconomy participants and their product offerings **and services** that may cause us to modify or discontinue a product offering **or service** on our platform. If we were to modify or discontinue any product offering **or service** or remove any assets from trading on our platform for any reason, our decision may be unpopular with users, may reduce our ability to attract and retain customers (especially if similar ~~product~~ **products** ~~offerings~~ **, services** or such assets ~~remain~~ **continue to be offered or** traded on unregulated exchanges, which includes many of our competitors), and may adversely affect our business, operating results, and financial condition. Further, if Bitcoin, Ethereum, stablecoins or any other supported crypto asset is deemed to be a security under any U. S. federal, state, or foreign jurisdiction, or in a proceeding in a court of law or otherwise, it may have adverse consequences for such supported crypto asset. For instance, all transactions in such supported crypto asset would have to be registered with the SEC or other foreign authority, or conducted in accordance with an exemption from registration, which could severely limit its liquidity, usability and transactability. Moreover, the networks on which such supported crypto assets are utilized may be required to be regulated as securities intermediaries, and subject to applicable rules, which could effectively render the network impracticable for its existing purposes. Further, it could draw negative publicity and a decline in the general acceptance of the crypto asset. Also, it may make it difficult for such supported crypto asset to be traded, cleared, and custodied as compared to other crypto assets that are not considered to be securities. Specifically, even if transactions in a crypto asset were registered with the SEC or conducted in accordance with an exemption from registration, the current intermediary- based framework for securities trading, clearance and settlement is not consistent with the operations of the crypto asset market. For example, under current SEC guidance, crypto asset securities cannot be held on behalf of customers by broker- dealers that also support custody of traditional securities; and the SEC has not permitted public permissionless blockchain- based clearance and settlement systems for securities. We currently rely on third- party service providers for certain aspects of our operations, and any interruptions in services provided by these third parties may impair our ability to support our customers. We rely on third parties in connection with many aspects of our business, including payment processors, banks, and payment gateways to process transactions; cloud computing services and data centers that provide facilities, infrastructure **, smart contract development** , website functionality and access, components, and services, including databases and data center facilities and cloud computing; as well as third parties that provide outsourced customer service, compliance support and product development functions, which are critical to our operations. Because we rely on third parties to provide these services and to facilitate certain of our business activities, we face increased operational risks. We do not directly manage the operation of any of these third parties, including their data center facilities that we use. These third parties may be subject to financial, legal, regulatory, and labor issues, cybersecurity incidents, **data theft or loss,** break- ins, computer viruses **or vulnerabilities in their code** , denial- of- service attacks, sabotage, acts of vandalism **, loss, disruption, or instability of third- party banking relationships** , privacy breaches, service terminations, disruptions, interruptions, and other misconduct. They are also vulnerable to damage or interruption from human error, power loss, telecommunications failures, fires, floods, earthquakes, hurricanes, tornadoes, pandemics ~~(including the COVID- 19 pandemic)~~ and similar events. For example, on February 24, 2021, the U. S. Federal Reserve' s payments network experienced an outage, which had the potential to result in reduced functionality for certain of our products. In addition, these third parties may breach their agreements with us, disagree with our interpretation of contract terms or applicable laws and regulations, refuse to continue or renew these agreements on commercially reasonable terms or at all, fail or refuse to process transactions or provide other services adequately, take actions that degrade the functionality of our services, impose additional costs or requirements on us or our customers, or give preferential treatment to competitors. There can be no assurance that third parties that provide services to us or to our customers on our behalf will continue to do so on acceptable terms, or at all. If any third parties do not adequately or appropriately provide their services or perform their responsibilities to us or our customers on our behalf, such as if third- party service providers to close their data center facilities without adequate notice, are unable to restore operations and data, fail to perform as expected, or experience other unanticipated problems, we may be unable to procure alternatives in a timely and efficient manner and on acceptable terms, or at all, and we may be subject to business disruptions, losses or costs to remediate any of the deficiencies, customer dissatisfaction, reputational damage, legal or regulatory proceedings, or other adverse consequences which could harm our business. Loss of a critical banking or insurance relationship could adversely impact our business, operating results, and financial condition. We rely on bank ~~accounts~~ **relationships** to provide our platform and custodial services. In particular, customer cash holdings on our platform are held with one or more of our multiple banking partners. As a registered money services business with FinCEN under the Bank Secrecy Act, as amended by the USA PATRIOT Act of 2001, and its implementing regulations enforced by FinCEN, or collectively, the BSA, a licensed money transmitter in a number of U. S. states and territories, a licensee under NYDFS' s Virtual Currency Business Activity regime, commonly referred to as a BitLicense, a licensed electronic money institution under both the U. K. Financial Conduct Authority and the Central Bank of Ireland, and a limited purpose trust company chartered by the NYDFS, our banking partners view us as a higher risk customer for purposes of their anti- money laundering programs. We may face difficulty establishing or maintaining banking relationships due to **instability in the global banking system, increasing regulatory uncertainty and scrutiny, or** our banking partners' policies and some prior bank partners have terminated their relationship with us or have limited access to bank services. The loss of these banking partners or the imposition of operational restrictions by these banking partners and the inability for us to utilize other redundant financial institutions may result in a disruption of business activity as well as regulatory risks. In addition, as a result of the myriad of regulations, the risks of crypto assets generally, ~~or~~ the adverse reputational impact of the 2022 Events on our industry **, or in the event of an adverse outcome of the June 2023 SEC Complaint** , financial institutions in the United States and globally may decide to not provide, or be prohibited from providing, account, custody, or other financial services to us or the cryptoeconomy generally. Further, we have existing redundancies in U.

S. and global financial institutions that work with crypto companies with which we engage. However, if these financial institutions **are subject to bank resolution or failure, or** limit or end their cryptomarket activity, or if banking relationships become severely limited or unavailable to cryptomarket participants in a certain country, there could be temporary delays in or unavailability of services in such country that are critical to our **or our partners'** operations, developers or customers, a further limit on available vendors, reduced quality in services we, our **partners, our** developers or our customers are able to obtain, and a general disruption to the cryptoeconomy, potentially leading to reduced activity on our platform which may adversely impact our business, operating results, and financial condition **. For example, while our business and operations have not been materially affected by the closures of Silvergate Capital Corp. and Signature Bank and the cessation of their real- time fiat currency payment networks in March 2023, large cryptoeconomy participants, including us and our institutional customers, experienced a temporary inability to transfer fiat currencies outside of standard business hours** . We also rely on insurance carriers to insure customer losses resulting from a breach of our physical security, cyber security, or by employee or ~~service provider~~ **third party** theft **and hold surety bonds as required for compliance with certain of our licenses under applicable state laws** . Our ability to maintain crime, specie, and cyber insurance **, as well as surety bonds,** is subject to the insurance carriers' ongoing underwriting criteria and our inability to obtain and maintain appropriate insurance coverage could cause a substantial business disruption, adverse reputational impact, inability to compete with our competitors, and regulatory scrutiny. Any significant disruption in our products and services, in our information technology systems, or in any of the blockchain networks we support, could result in a loss of customers or funds and adversely impact our brand and reputation and our business, operating results, and financial condition. Our reputation and ability to attract and retain customers and grow our business depends on our ability to operate our service at high levels of reliability, scalability, and performance, including the ability to process and monitor, on a daily basis, a large number of transactions that occur at high volume and frequencies across multiple systems **. For example, in March 2023, there was a temporary disruption to USDC services for several days following the news of Silicon Valley Bank' s closure** . Our platform, the ability of our customers to trade, and our ability to operate at a high level, are dependent on our ability to access the blockchain networks underlying the supported crypto assets, for which access is dependent on our systems' ability to access the internet. Further, the successful and continued operations of such blockchain networks will depend on a network of computers, miners, or validators, and their continued operations, all of which may be impacted by service interruptions. Our systems, the systems of our third- party service providers and partners, and certain crypto asset and blockchain networks have experienced from time to time, and may experience in the future service interruptions or degradation because of hardware and software defects or malfunctions, distributed denial- of- service and other cyberattacks, insider threats, break- ins, sabotage, human error, vandalism, earthquakes, hurricanes, floods, fires, and other natural disasters, power losses, disruptions in telecommunications services, fraud, military or political conflicts, terrorist attacks, computer viruses or other malware, or other events. In addition, extraordinary Trading Volumes or site usage could cause our computer systems to operate at an unacceptably slow speed or even fail. Some of our systems, including systems of companies we have acquired, or the systems of our third- party service providers and partners are not fully redundant, and our or their disaster recovery planning may not be sufficient for all possible outcomes or events. If any of our systems, or those of our third-party service providers, are disrupted for any reason, our products and services may fail, resulting in unanticipated disruptions, slower response times and delays in our customers' trade execution and processing, failed settlement of trades, incomplete or inaccurate accounting, recording or processing of trades, unauthorized trades, loss of customer information, increased demand on limited customer support resources, customer claims, complaints with regulatory organizations, lawsuits, or enforcement actions. Further, when these disruptions occur, we have in the past, and may in the future, fulfill customer transactions using inventory to prevent adverse user impact and limit detrimental impact to our operating results. A prolonged interruption in the availability or reduction in the availability, speed, or functionality of our products and services could harm our business. Significant or persistent interruptions in our services could cause current or potential customers or partners to believe that our systems are unreliable, leading them to switch to our competitors or to avoid or reduce the use of our products and services, and could permanently harm our reputation and brands. Moreover, to the extent that any system failure or similar event results in damages to our customers or their business partners, these customers or partners could seek significant compensation or contractual penalties from us for their losses, and those claims, even if unsuccessful, would likely be time- consuming and costly for us to address. Problems with the reliability or security of our systems would harm our reputation ~~, and damage to our reputation~~ and the cost of remedying these problems could negatively affect our business, operating results, and financial condition. Because we are a regulated financial institution in certain jurisdictions, interruptions have resulted and in the future may result in regulatory scrutiny, and significant or persistent interruptions could lead to significant fines and penalties, and mandatory and costly changes to our business practices, and ultimately could cause us to lose existing licenses or banking relationships that we need to operate or prevent or delay us from obtaining additional licenses that may be required for our business. In addition, we are continually improving and upgrading our information systems and technologies. Implementation of new systems and technologies is complex, expensive, time- consuming, and may not be successful. If we fail to timely and successfully implement new information systems and technologies, or improvements or upgrades to existing information systems and technologies, or if such systems and technologies do not operate as intended, it could have an adverse impact on our business, internal controls (including internal controls over financial reporting), operating results, and financial condition. Our failure to safeguard and manage our and our customers' fiat currencies and crypto assets could adversely impact our business, operating results, and financial condition. **We** ~~As of December 31, 2022, we held~~ **hold cash** ~~a combined $ 80. 5 billion in custodial fiat currencies~~ and ~~cryptocurrencies~~ **safeguard crypto assets** on behalf of **our** customers **and hold fiat and crypto for corporate investment and operating purposes** . ~~Supported~~ **In addition, following the acquisition of Coinbase Asset Management, formerly One River Digital Asset Management (" CBAM "), we additionally safeguard, as defined by SAB 121, an immaterial amount of cryptocurrencies at third- party custodians for asset management products. Safeguarding**

customers' cash and crypto assets **is integral to the trust we build with our customers. We believe our policies, procedures, operational controls and controls over financial reporting, protect us from material risks surrounding the safeguarding of these assets and conflicts of interest. Our controls over financial reporting include among others, controls over the segregation of corporate crypto asset balances from customer crypto asset balances, controls over the processes of customer crypto asset deposits and customer crypto asset withdrawals and corporate and customer fiat balances. Our financial statements and disclosures, as a whole,** are ~~not insured~~ **available through periodic filings on a quarterly basis, and compliant with annual audit requirements of Article 3 of Regulation S- X. We hold cash at financial institutions in accounts designated as** ~~or~~ **for the benefit of** ~~guaranteed by any government or~~ **our customers** ~~government agency~~. We have also entered into partnerships or joint ventures with third parties, such as with the issuer of USDC, where we or our partners receive and hold customer funds. Our and our **financial** partners' abilities to manage and accurately **hold** ~~safeguard these~~ customer ~~assets~~ **cash** and **cash** ~~the crypto assets~~ we hold for our own investment and operating purposes requires a high level of internal controls. **We are limited in our ability to influence or manage the controls and processes of third party partners or vendors and may be dependent on our partners' and vendors' operations, liquidity and financial condition to manage these risks.** As **we maintain,** ~~our business continues to~~ grow and ~~we~~ expand our product and ~~service~~ **services** offerings ~~,~~ we **also** must ~~continue to~~ **scale and** strengthen our ~~associated~~ internal controls and **processes,** ~~ensure that our partners do the same. Our success~~ and **monitor** ~~the success of~~ our **third party** ~~offerings requires significant public confidence in our and our~~ partners' **and vendors'** ability to ~~properly manage~~ **similarly scale and strengthen. Failure to do so could adversely impact our business, operating results, and financial condition. This is important both to the actual controls and processes and the public perception of the same. Any inability by us to maintain our safeguarding procedures, perceived or otherwise, could harm our business, operating results, and financial condition. Accordingly, we take steps to ensure customer cash is always secure. Customer cash and crypto asset balances are maintained through our internal ledgering processes. Customer cash is maintained in segregated Company bank accounts that are held for the exclusive benefit of customers with our financial institution banking partners or in government money market funds. We safeguard crypto assets using proprietary technology and operational processes. Crypto assets are not insured or guaranteed by any government or government agency, however we have worked hard to safeguard our** customers' ~~balances and handle large transaction volumes and amounts of customer funds. In addition, we are dependent on our partners' operations, liquidity, and financial condition for the proper maintenance, use, and safekeeping of these customer assets. We believe our policies and procedures protect us from material risks surrounding the safeguarding of~~ crypto assets ~~, audited ledgering of customer funds~~ and ~~corporate~~ **our own crypto** assets ~~,~~ **for investment** and ~~conflicts of interest~~ **operational purposes with legal and operational protections**. **Any** ~~However, any~~ material failure by us or our partners to maintain the necessary controls, policies, procedures or to manage the crypto assets we hold for our own investment and operating purposes could **also** adversely impact our business, operating results, and financial condition. Further, any material failure by us or our partners to maintain the necessary controls or to manage customer crypto assets and funds appropriately and in compliance with applicable regulatory requirements could result in reputational harm, litigation, regulatory enforcement actions, significant financial losses, lead customers to discontinue or reduce their use of our and our partners' products, and result in significant penalties and fines and additional restrictions, which could adversely impact our business, operating results, and financial condition. Moreover, because custodially held crypto assets may be considered to be the property of a bankruptcy estate, in the event of a bankruptcy, the crypto assets we hold in custody on behalf of our customers could be subject to bankruptcy proceedings and such customers could be treated as our general unsecured creditors. This may result in customers finding our custodial services more risky and less attractive and any failure to increase our customer base, discontinuation or reduction in use of our platform and products by existing customers as a result could adversely impact our business, operating results, and financial condition. ~~Further~~ **Additionally** , ~~we~~ **following the acquisition of CBAM, some of our asset management products hold customer assets at third- party custodians with their own bankruptcy protection procedures. We** place great importance on safeguarding crypto assets we custody and keeping them bankruptcy remote from our general creditors, and in June 2022 we updated our Retail User Agreement to clarify the applicability of UCC Article 8 to custodied crypto assets ~~-~~ – the same legal protection that our institutional custody and prime broker clients also rely upon. UCC Article 8 provides that financial assets held by Coinbase are not property of Coinbase and not subject to the claims of its general creditors. In light of UCC Article 8, we believe that a court would not treat custodied crypto assets as part of our general estate; however, due to the novelty of crypto assets, courts have not yet considered this type of treatment for custodied crypto assets. We deposit, transfer, and custody customer cash and crypto assets in multiple jurisdictions. In each instance, we require bank- level security encryption to safeguard customers' assets for our wallet and storage systems, as well as our financial management systems related to such custodial functions. Our security technology is designed to prevent, detect, and mitigate inappropriate access to our systems, by internal or external threats. We believe we have developed and maintained administrative, technical, and physical safeguards designed to comply with applicable legal requirements and industry standards. However, it is nevertheless possible that hackers, employees or service providers acting contrary to our policies, or others could circumvent these safeguards to improperly access our systems or documents, or the systems or documents of our business partners, agents, or service providers, and improperly access, obtain, **or** misuse customer crypto assets and funds. The methods used to obtain unauthorized access, disable, or degrade service or sabotage systems are also constantly changing and evolving and may be difficult to anticipate or detect for long periods of time. Certain of our customer contracts do not limit our liability with respect to security breaches and other security- related matters and our insurance coverage for such impropriety is limited and may not cover the extent of loss nor the nature of such loss, in which case we may be liable for the full amount of losses suffered, which could be greater than all of our assets. Our ability to maintain insurance is also subject to the insurance carriers' ongoing underwriting criteria. Any loss of customer cash or crypto assets could result in a subsequent lapse in insurance coverage, which could cause

a substantial business disruption, adverse reputational impact, inability to compete with our competitors, and regulatory investigations, inquiries, or actions. Additionally, transactions undertaken through our websites or other electronic channels may create risks of fraud, hacking, unauthorized access or acquisition, and other deceptive practices. Any security incident resulting in a compromise of customer assets could result in substantial costs to us and require us to notify impacted individuals, and in some cases regulators, of a possible or actual incident, expose us to regulatory enforcement actions, including substantial fines, limit our ability to provide services, subject us to litigation, significant financial losses, damage our reputation, and adversely affect our business, operating results, financial condition, and cash flows. **The theft, loss, or destruction of private keys required to access any crypto assets held in custody for our own account or for our customers may be irreversible. If we are unable to access our private keys or if we experience a hack or other data loss relating to our ability to access any crypto assets, it could cause regulatory scrutiny, reputational harm, and other losses.** Crypto assets are generally controllable only by the possessor of the unique private key relating to the digital wallet in which the crypto assets are held. While blockchain protocols typically require public addresses to be published when used in a transaction, private keys must be safeguarded and kept private in order to prevent a third party from accessing the crypto assets held in such a wallet. To the extent that any of the private keys relating to our wallets containing crypto assets held for our own account or for our customers is lost, destroyed, or otherwise compromised or unavailable, and no backup of the private key is accessible, we will be unable to access the crypto assets held in the related wallet. Further, we cannot provide assurance that our ~~wallet~~ **wallets** will not be hacked or compromised. Crypto assets and blockchain technologies have been, and may in the future be, subject to security breaches, hacking, or other malicious activities. Any loss of private keys relating to, or hack or other compromise of, digital wallets used to store our customers' crypto assets could adversely affect our customers' ability to access or sell their crypto assets, require us to reimburse our customers for their losses, and subject us to significant financial losses in addition to losing customer trust in us and our products. As such, any loss of private keys due to a hack, employee or service provider misconduct or error, or other compromise by third parties could hurt our brand and reputation, result in significant losses, and adversely impact our business. The total value of crypto assets in our possession and control is significantly greater than the total value of insurance coverage that would compensate us in the event of theft or other loss of funds, which could cause our business, operating results, and financial condition to be adversely impacted in the event of such uninsured loss. Other Risks Related to Our Business and Financial Position If we fail to retain existing customers or add new customers, or if our customers decrease their level of engagement with our products, services and platform, our business, operating results, and financial condition may be significantly harmed. Our success depends on our ability to retain existing customers and attract new customers, including developers, to increase engagement with our products, services, and platform. To do so, we must continue to offer leading technologies and ensure that our products and services are secure, reliable, and engaging. We must also expand our products and services, and offer competitive prices in an increasingly crowded and price- sensitive market. There is no assurance that we will be able to continue to do so, that we will be able to retain our current customers or attract new customers, or keep our customers engaged. Any number of factors can negatively affect customer retention, growth, and engagement, including if: • customers increasingly engage with competing products and services, including products and services that we are unable to offer due to regulatory reasons; • we fail to introduce new and improved products and services, or if we introduce new products or services that are not favorably received; • we fail to support new and in- demand crypto assets or if we elect to support crypto assets with negative reputations; • there are changes in sentiment about the quality or usefulness of our products and services or concerns related to privacy, security, **fiat pegging** or other factors; • there are adverse changes in our products and services that are mandated by legislation, regulatory authorities, or litigation; • customers perceive the crypto assets on our platform to be bad investments, or experience significant losses in investments made on our platform; • technical or other problems prevent us from delivering our products and services with the speed, functionality, security, and reliability that our customers expect; • cybersecurity incidents, employee or service provider misconduct, or other unforeseen activities cause losses to us or our customers, including losses to assets held by us on behalf of our customers; • modifications to our pricing model or modifications by competitors to their pricing **models** ; • we fail to provide adequate customer service; • regulatory and governmental bodies in countries that we target for expansion express negative views towards crypto asset trading platforms and, more broadly, the cryptoeconomy; or • we or other companies **or high- profile figures** in our industry are the subject of adverse media reports or other negative publicity. From time to time, certain of these factors have negatively affected customer retention, growth, and engagement to varying degrees. If we are unable to maintain or increase our customer base and customer engagement, our revenue and financial results may be adversely affected. Any decrease in user retention, growth, or engagement could render our products and services less attractive to customers, which may have an adverse impact on our revenue, business, operating results, and financial condition. If our customer growth rate slows or declines, we will become increasingly dependent on our ability to maintain or increase levels of user engagement and monetization in order to drive growth of revenue. Our operating expenses may increase in the future and we may not be able to achieve profitability or ~~achieve~~ positive cash flow from operations on a consistent basis, which may cause our business, operating results, and financial condition to be adversely impacted. Our operating expenses may increase in the future as we continue to attract and retain talent, expand our sales and marketing efforts, develop additional products and services, expand our international business, **incur unforeseen regulatory or compliance expenses,** and in connection with certain expenses related to operating as a public company. While we consistently evaluate opportunities to **drive** ~~reduce our operating costs and optimize efficiencies~~ **efficiency** ~~, including, for example, through our workforce reductions in June 2022 and January 2023~~ , we cannot guarantee that these efforts will be successful or that we will not re- accelerate operating expenditures in the future ~~in order to capitalize on growth opportunities~~ . Our operations may prove more expensive than we currently anticipate, and we may not succeed in increasing our net revenue sufficiently to offset these higher expenses. Our revenue growth ~~and net revenue~~ may **be further impacted by** ~~continue to decline for a number of other reasons, including~~ reduced demand for our offerings, increased competition, adverse macroeconomic conditions, a

decrease in the growth or size of the cryptoeconomy, **regulatory uncertainty or scrutiny, or changes that impact** ~~or~~ **our ability to offer certain products or services,** any failure to capitalize on growth opportunities ~~. Any~~ **, or** failure **of new products and services we develop** to **gain traction in the market** ~~increase our revenue could prevent us from achieving profitability~~ . We cannot be certain that we will be able to achieve profitability or achieve positive operating cash flow on any quarterly or annual basis. If we are unable to effectively manage these risks and difficulties as we encounter them, our business, operating results, and financial condition may suffer. If we do not effectively scale our business, or are unable to maintain and improve our systems and processes, our operating results could be adversely affected. We have experienced a period of significant growth in recent years, both in terms of employee headcount and customer growth, followed by the scaling back of our business in response to changing economic conditions ~~throughout 2022~~ . As our business changes, it becomes increasingly complex. To effectively manage and capitalize on our growth periods, we need to manage headcount, capital and processes efficiently while making investments such as expanding our information technology and financial, operating, and administrative systems and controls. Growth and scaling back initiatives could strain our existing resources, and we could experience ongoing operating difficulties in managing our business as it expands across numerous jurisdictions, including difficulties in hiring, training, managing and retaining a remote and evolving employee base. If we do not adapt or scale to meet these evolving challenges, we may experience erosion to our brand, the quality of our products and services may suffer, and our company culture may be harmed. Moreover, the failure of our systems and processes could undermine our ability to provide accurate, timely, and reliable reports on our financial and operating results, including the financial statements provided herein, and could impact the effectiveness of our internal controls over financial reporting. In addition, our systems and processes may not prevent or detect all errors, omissions, or fraud. Any of the foregoing operational failures could lead to noncompliance with laws, loss of operating licenses or other authorizations, or loss of bank relationships that could substantially impair or even suspend company operations. Successful implementation of our growth strategy will also require significant expenditures before any substantial associated revenue is generated and we cannot guarantee that these increased investments will result in corresponding and offsetting revenue growth. Because we have a limited history operating our business at its current scale, it is difficult to evaluate our current business and future prospects, including our ability to plan for and model future growth. Our limited operating experience at this scale, combined with the rapidly evolving nature of the crypto asset market in which we operate, substantial uncertainty concerning how these markets may develop, and other economic factors beyond our control, reduces our ability to accurately forecast quarterly or annual revenue. Additionally, from time to time, we realign our resources and talent to implement stage- appropriate business strategies, including furloughs, layoffs and reductions in force. For example, in June 2022 and in January 2023, in response to rapidly changing economic conditions and in an effort to reduce our operational costs and improve our organizational efficiency, we reduced our workforce. If there are unforeseen expenses associated with such realignments in our business strategies, and we incur unanticipated charges or liabilities, then we may not be able to effectively realize the expected cost savings or other benefits of such actions. Failure to manage any growth or any scaling back of our operations could have an adverse effect on our business, operating results, and financial condition. Our strategy and focus on delivering high- quality, compliant, easy- to- use, and secure crypto- related financial services may not maximize short- term or medium- term financial results. We have taken, and expect to continue to take, actions that we believe are in the best interests of our customers and the long- term interests of our business, even if those actions do not necessarily maximize short- term or medium- term results. These include expending significant managerial, technical, and legal efforts on complying with laws and regulations that are applicable to our products and services and ensuring that our products are secure. We also focus on driving long- term engagement with our customers through innovation and developing new industry- leading products and technologies. These decisions may not be consistent with the short- term and medium- term expectations of our stockholders and may not produce the long- term benefits that we expect, which could have an adverse effect on our business, operating results, and financial condition. A significant amount of the Trading Volume on our platform is derived from a relatively small number of customers, and the loss of these customers, or a reduction in their Trading Volume, could have an adverse effect on our business, operating results, and financial condition. A relatively small number of institutional market makers and high-transaction volume consumer customers account for a significant amount of the Trading Volume on our platform and our net revenue. We expect significant Trading Volume and net revenue attributable to these customers for the foreseeable future. As a result, a loss of these customers, or a reduction in their Trading Volume, and our inability to replace these customers with other customers, could have an adverse effect on our business, operating results, and financial condition. Due to our limited operating history, it may be difficult to evaluate our business and future prospects, and we may not be able to achieve or maintain profitability in any given period. We began our operations in 2012 and since then our business model has continued to evolve. Our net revenue has significantly grown since our formation, but there is no assurance that ~~this~~ growth ~~rate~~ will continue in future periods and you should not rely on the **net** revenue growth of any given prior quarterly or annual period as an indication of our future performance. For example, while we generated $ 7. 4 billion ~~and $ 1. 1 billion~~ in total net revenue for the **year ended December 31, 2021, our total net revenue for the** years ended December 31, ~~2021~~ **2023** and ~~December 31, 2020, respectively, our total net revenue for the year ended December 31,~~ 2022 ~~was~~ **declined to $ 2. 9 billion and** $ 3. 1 billion, **respectively** ~~representing a decline of 57 % compared to the prior year~~ , primarily due to declining crypto prices, lower crypto asset volatility, and uncertainty in the cryptoeconomy following the 2022 Events. If our total net revenue were to further decline significantly for an extended period of time, our business, operating results and financial condition could be adversely affected. Our limited operating history and the volatile nature of our business make it difficult to evaluate our current business and our future prospects. We have encountered and will continue to encounter risks and difficulties as described in this section. If we do not manage these risks successfully, our business may be adversely impacted. If our **revenue** growth rate were to decline significantly or become negative, it could adversely affect our operating results and financial condition. If we are not able to achieve or maintain positive cash flow from operations, our business may be adversely impacted and we may require additional

financing, which may not be available on favorable terms or at all, or which would be dilutive to our stockholders. Because our long- term success depends, in part, on our ability to expand our sales to customers outside the United States, our business is susceptible to risks associated with international operations. We currently have subsidiaries in the United States and abroad. We plan to enter into or increase our presence in additional markets around the world. We have a limited operating history outside the United States, and our ability to manage our business and conduct our operations internationally requires considerable management attention and resources and is subject to particular challenges of supporting a growing business in an environment of diverse cultures, languages, customs, tax laws, legal systems, alternate dispute systems, and regulatory systems. As we continue to expand our business and customer base outside the United States, we will be increasingly susceptible to risks associated with international operations. These risks and challenges include: • difficulty establishing and managing international operations and the increased operations, travel, infrastructure, including establishment of local customer service operations **, local infrastructure to manage supported cryptocurrency or other financial instruments and corresponding books and records** , and legal and regulatory compliance costs associated with different jurisdictions; • the need to vary pricing and margins to effectively compete in international markets; • the need to adapt and localize our products and services for specific countries, including offering services and support in local languages; • compliance with multiple, potentially conflicting and changing governmental laws and regulations across different jurisdictions; • compliance with U. S. and foreign laws designed to combat money laundering and the financing of terrorist activities, as well as economic and trade sanctions; • **the need to comply with a greater set of law enforcement inquiries including those subject to mutual legal assistance treaties; • compliance with the extraterritorial reach of any U. S. regulatory rules, including those imposed by the CFTC, SEC, FinCEN or other U. S. based regulators; •** difficulties obtaining **and maintaining** required licensing from regulators in foreign jurisdictions; • competition with companies that have greater experience in the local markets, pre- existing relationships with customers in these markets or are subject to less regulatory requirements in local jurisdictions; • varying levels of payments and blockchain technology adoption and infrastructure, and increased network, payment processing, banking, and other costs; • compliance with anti- bribery laws, including compliance with the Foreign Corrupt Practices Act, the U. K. Bribery Act 2010, and other local anticorruption laws; • difficulties collecting in foreign currencies and associated foreign currency exposure; • difficulties holding, repatriating, and transferring funds held in offshore bank accounts; • difficulties **adapting to foreign customary commercial practices,** enforcing contracts and collecting accounts receivable, longer payment cycles and other collection difficulties; • restrictions on crypto asset trading; • stringent local labor laws and regulations; • potentially adverse tax developments and consequences; • antitrust and competition regulations; and • regional economic and political conditions. We have limited experience with international regulatory environments and market practices and may not be able to penetrate or successfully operate in the markets we choose to enter. In addition, we may incur significant expenses as a result of our international expansion, and we may not be successful. We may face limited brand recognition in certain parts of the world that could lead to non- acceptance or delayed acceptance of our products and services by customers in new markets. We may also face challenges in complying with local laws and regulations. **For example, we may be subject to regulatory frameworks that are evolving, have not undergone extensive rulemaking, and could result in uncertain outcomes for our customers and / or our ability to offer competitive products in the broader cryptoeconomy.** Our failure to successfully manage these risks could harm our international operations and have an adverse effect on our business, operating results, and financial condition. Disputes with our customers could adversely impact our brand and reputation and our business, operating results, and financial condition. From time to time we have been, and may in the future be, subject to claims and disputes with our customers with respect to our products and services, such as regarding the execution and settlement of crypto asset trades, fraudulent or unauthorized transactions, account takeovers, deposits and withdrawals of crypto assets, failures or malfunctions of our systems and services, or other issues relating to our products services. For example, during periods of heavy Trading Volumes, we have received increased customer complaints. Additionally, the ingenuity of criminal fraudsters, combined with many consumer users' susceptibility to fraud, may cause our customers to be subject to ongoing account takeovers and identity fraud issues. While we have taken measures to detect and reduce the risk of fraud, there is no guarantee that they will be successful and, in any case, require continuous improvement and optimization for continually evolving forms of fraud to be effective. There can be no guarantee that we will be successful in detecting and resolving these disputes or defending ourselves in any of these matters, and any failure may result in impaired relationships with our customers, damage to our brand and reputation, and substantial fines and damages. In some cases, the measures we have implemented to detect and deter fraud have led to poor customer experiences, including indefinite account inaccessibility for some of our customers, which increases our customer support costs and can compound damages. We could incur significant costs in compensating our customers, such as if a transaction was unauthorized, erroneous, or fraudulent. We could also incur significant legal expenses resolving and defending claims, even those without merit. To the extent we are found to have failed to fulfill our regulatory obligations, we could also lose our authorizations or licenses or become subject to conditions that could make future operations more costly, impair our ability to grow, and adversely impact our operating results. We currently are, and may in the future become, subject to investigation and enforcement action by state, federal, and international consumer protection agencies, including the Consumer Financial Protection Bureau (the " CFPB "), the Federal Trade Commission (the " FTC "), state attorneys general in the United States, the U. K. Financial Conduct Authority, the U. K. Financial Ombudsman Service, and the U. K. Office of Fair Trading, each of which monitors customer complaints against us and, from time to time, escalates matters for investigation and potential enforcement against us. While certain of our customer agreements contain arbitration provisions with class action waiver provisions that may limit our exposure to consumer class action litigation, some federal, state, and foreign courts have refused or may refuse to enforce one or more of these provisions, and there can be no assurance that we will be successful in enforcing these arbitration provisions, including the class action waiver provisions, in the future or in any given case. Legislative, administrative, or regulatory developments may directly or indirectly prohibit or limit the use of pre- dispute arbitration clauses

and class action waiver provisions. Any such prohibitions or limitations on or discontinuation of the use of such arbitration or class action waiver provisions could subject us to additional lawsuits, including additional consumer class action litigation, and significantly limit our ability to avoid exposure from consumer class action litigation. We may suffer losses due to staking, delegating, and other related services we provide to our customers. Certain supported crypto assets enable holders to earn rewards by participating in decentralized governance, bookkeeping and transaction confirmation activities on their underlying blockchain networks, such as through staking activities, including staking through validation, delegating, and baking. We currently provide and expect to continue to provide such services for certain supported crypto assets to our customers in order to enable them to earn rewards based on crypto assets that we hold on their behalf. For instance, as a service to customers, we operate staking nodes on certain blockchain networks utilizing customers' crypto assets and pass through the rewards received to those customers, less a service fee. In other cases, upon customers' instructions, we may delegate our customers' assets to third- party service providers that are unaffiliated with us. Some networks may further require customer assets to be transferred into smart contracts on the underlying blockchain networks not under our or anyone' s control. If our validator, any third- party service providers, or smart contracts fail to behave as expected, suffer cybersecurity attacks, experience security issues, or encounter other problems, our customers' assets may be irretrievably lost. In addition, certain blockchain networks dictate requirements for participation in the relevant decentralized governance activity, and may impose penalties, or " slashing, " if the relevant activities are not performed correctly, such as if the staker, delegator, or baker acts maliciously on the network, " double signs " any transactions, or experience extended downtimes. If we or any of our service providers are slashed by the underlying blockchain network, our customers' assets may be confiscated, withdrawn, or burnt by the network, resulting in losses for which we may be responsible. Furthermore, certain types of staking require the payment of transaction fees on the underlying blockchain network and such fees can become significant as the amount and complexity of the transaction grows, depending on the degree of network congestion and the price of ~~Ethereum~~ **the network token** . If we experience a high volume of such staking requests from our customers on an ongoing basis, we could incur significant costs. Any penalties or slashing events could damage our brand and reputation, cause us to suffer financial losses, discourage existing and future customers from utilizing our products and services, and adversely impact our business ~~. We launched a beta of Coinbase NFT, a peer- to- peer marketplace for minting, purchasing, showcasing, and discovering non- fungible tokens (NFTs), which may further expose us to legal, regulatory, and other risks that could adversely affect our business, operating results, and financial condition. In April 2022, we launched a beta of Coinbase NFT, a peer- to- peer marketplace that simplifies the purchasing, showcasing, and discovery of NFTs. While NFTs and cryptocurrencies are similar in that both are based on blockchain technology, unlike cryptocurrency units, which are fungible, NFTs have unique identification codes and often reference content. As NFTs are a relatively new and emerging type of digital asset, the regulatory, commercial, and legal framework governing NFTs is likely to evolve both in the United States and internationally and implicates issues regarding a range of matters, including, but not limited to, intellectual property rights, privacy and cybersecurity, fraud, anti- money laundering, money transmission, sanctions, and currency, commodity, and securities law compliance. For example, NFTs raise various intellectual property law considerations, including relating to ownership, copyrights, trademarks and rights of publicity. The creator of an NFT will often have, or purport to have, all rights to the content of the NFT and can determine what rights to assign to a buyer, such as the right to display, modify, or copy the content. Risks associated with purchasing or selling items associated with content created by third parties through peer- to- peer transactions, include, among other things, the risk of purchasing counterfeit items or items alleged to be counterfeit, mislabeled items, items that are vulnerable to metadata decay, items on smart contracts with bugs, items related to content that infringes intellectual property rights, and items that may become untransferable. To the extent we are directly or indirectly involved in a dispute between creators and buyers on our NFT marketplace, it could adversely affect the success of our NFT marketplace and harm our business, operating results, and financial condition. Further, NFTs have in particular been subject to actual and attempted theft through hacking, social engineering, phishing, and fraudulently inducing individuals into delivering NFTs or providing access to NFTs to an unauthorized third party. Despite our best efforts, the safeguards we have implemented or may implement in the future to protect against these cybersecurity threats may be insufficient to prevent a malicious actor, and any such activity on Coinbase NFT could result in reputational harm, or costs or losses associated with mitigation efforts against these incidents. Moreover, it is difficult to predict how the legal and regulatory framework around NFTs will develop and how such developments will impact our business and our NFT marketplace since the market for NFTs is relatively nascent. Regulators may apply existing or new regulations to NFT transactions. Further, NFT transactions also raise issues regarding compliance with laws of foreign jurisdictions, many of which present complex compliance issues and may conflict with one another. We may also experience media, legislative, or regulatory scrutiny of our actions or decisions related to our content enforcement practices with respect to our NFT marketplace either as a result of our perceived failure to respond expeditiously or appropriately to the sharing of content perceived as objectionable or as a result of our decisions to remove content or suspend participation on our NFT marketplace by persons who violate our content standards and terms of service. Any such negative publicity could have an adverse effect on the size, engagement, and loyalty of our user base and demand for our NFT marketplace, which could result in decreased revenue and adversely affect our business, operating results, and financial condition. Additionally, similar to other aspects of our business, our NFT marketplace is reliant on certain third- party partners, including payment processors, payment gateways, and cloud computing services and data centers. If any of these third parties do not adequately or appropriately provide their services or perform their responsibilities to us, or our customers on our behalf, we may be unable to procure alternatives in a timely and efficient manner and on acceptable terms, or at all, and we may be subject to business disruptions, losses or costs to remediate any of the deficiencies, customer dissatisfaction, reputational damage, legal or regulatory proceedings, or other adverse consequences which could harm our business. The launch of our NFT marketplace also subjects us to risks similar to those associated with any new product offering, including, but not limited to, our ability to accurately anticipate market demand and acceptance, our ability to successfully launch the NFT marketplace, creator and buyer~~

~~acceptance, technical issues with the operation of the NFT marketplace, and legal and regulatory risks as discussed above~~ . We may not be able to generate sufficient cash to service our debt and other obligations, including our obligations under the 2026 Convertible Notes and Senior Notes. Our ability to make payments on our indebtedness, including the 2026 Convertible Notes and Senior Notes, and our other obligations will depend on our financial and operating performance, which is subject to prevailing economic and competitive conditions and to certain financial, business and other factors beyond our control. We may be unable to attain a level of cash flows from operating activities sufficient to permit us to pay the principal, premium, if any, and interest on our indebtedness, including each series of the 2026 Convertible Notes and Senior Notes, and other obligations. If we are unable to service our debt and other obligations from cash flows, we may need to refinance or restructure all or a portion of our debt obligations prior to maturity. Our ability to refinance or restructure our debt and other obligations will depend upon the condition of the capital markets and our financial condition at such time. Any refinancing or restructuring could be at higher interest rates and may require us to comply with more onerous covenants, which could further restrict our business operations. If our cash flows are insufficient to service our debt and other obligations, we may not be able to refinance or restructure any of these obligations on commercially reasonable terms or at all and any refinancing or restructuring could have a material adverse effect on our business, operating results, or financial condition. Statutory, contractual or other restrictions may also limit our subsidiaries' ability to pay dividends or make distributions, loans or advances to us. For these reasons, we may not have access to any assets or cash flows of our subsidiaries to make interest and principal payments on each series of the 2026 Convertible Notes and Senior Notes. If our cash flows are insufficient to fund our debt and other obligations and we are unable to refinance or restructure these obligations, we could face substantial liquidity problems and may be forced to reduce or delay investments and capital expenditures, or to sell material assets or operations to meet our debt and other obligations. We cannot assure you that we would be able to implement any of these alternative measures on satisfactory terms or at all or that the proceeds from such alternatives would be adequate to meet any debt or other obligations when due. If it becomes necessary to implement any of these alternative measures, our business, operating results, or financial condition could be materially and adversely affected. We have a substantial amount of indebtedness and other obligations, which could adversely affect our financial position and prevent us from fulfilling our obligations under the 2026 Convertible Notes and Senior Notes. We have a substantial amount of indebtedness and other obligations. As of December 31, ~~2022~~ **2023** , we had approximately $ 3. ~~44~~ **01** billion in aggregate principal amount of outstanding long- term indebtedness (excluding crypto asset borrowings), which includes $ ~~2~~ **1** . ~~0~~ **7** billion of our Senior Notes and $ 1. ~~44~~ **27** billion of our 2026 Convertible Notes. Our substantial indebtedness and other obligations may: • make it difficult for us to satisfy our financial obligations, including making scheduled principal and interest payments on our 2026 Convertible Notes, Senior Notes, and our other obligations; • limit our ability to use our cash flow for working capital, capital expenditures, acquisitions or other general business purposes; • increase our cost of borrowing; • require us to use a substantial portion of our cash flow from operations to make debt service payments and pay our other obligations when due; • limit our flexibility to plan for, or react to, changes in our business and industry; • place us at a competitive disadvantage compared to our less leveraged competitors; and • increase our vulnerability to the impact of adverse economic and industry conditions, including changes in interest rates and foreign exchange rates. We provide secured loans to our customers, which exposes us to credit risks and may cause us to incur financial or reputational harm. We provide ~~consumer and~~ commercial loans to qualified customers secured by their crypto or fiat asset holdings on our platform, which exposes us to the risk of our borrowers' inability to repay such loans. In addition, such activity results in us being subject to certain lending laws and regulations in the applicable jurisdiction and as a result we may be subject to additional regulatory scrutiny. In the future we may enter into credit arrangements with financial institutions to obtain more capital. Any termination or interruption in the financial institutions' ability to lend to us could interrupt our ability to provide capital to qualified customers to the extent we rely on such credit lines to continue to offer or to grow such products. Further, our credit approval process, pricing, loss forecasting, and scoring models may contain errors or may not adequately assess creditworthiness of our borrowers, or may be otherwise ineffective, resulting in incorrect approvals or denials of loans. It is also possible that loan applicants could provide false or incorrect information. While we have procedures in place to manage our credit risk, such as conducting due diligence on our customers and running stress test simulations to monitor and manage exposures, including any exposures resulting from loans collateralized with crypto assets, we remain subject to risks associated with our borrowers' creditworthiness and our approval process. Such risks are heightened following the 2022 Events. Borrower loan loss rates may be significantly affected by economic downturns or general economic conditions beyond our control and beyond the control of individual borrowers. In particular, loss rates on loans may increase due to factors such as prevailing market conditions in the cryptoeconomy, the price of Bitcoin and other crypto assets, which have experienced significant fluctuations, the amount of liquidity in the markets, and other factors. Borrowers may seek protection under federal bankruptcy law or similar laws. If a borrower of a loan files for bankruptcy (or becomes the subject of an involuntary petition), a stay may go into effect that will automatically put any pending collection actions on the loan on hold and prevent further collection action absent bankruptcy court approval. The efficacy of our security interest in customer collateral is not guaranteed under applicable state law or the Uniform Commercial Code and therefore we may be exposed to loss in the event of a customer default, even if we appear to be secured against such default. While we have not incurred any material losses to date, if any of the foregoing events were to occur, our reputation and relationships with borrowers, and our financial results, could be harmed. We intend to continue to explore other products, models, and structures for offering ~~consumer and~~ commercial financing, and other forms of credit and loan products. Some of those models or structures may require, or be deemed to require, additional data, procedures, partnerships, licenses, regulatory approvals, or capabilities that we have not yet obtained or developed. We are exposed to transaction losses due to chargebacks, refunds or returns as a result of fraud or uncollectability that may adversely impact our business, operating results, and financial condition. Certain of our products and services are paid for by electronic ~~transfer~~ **transfers** from bank accounts **,** which exposes us to risks associated with returns and insufficient funds. Furthermore, some of our products and services are paid for by credit

and debit cards through payment processors , which exposes us to risks associated with chargebacks and refunds. These ~~claims~~ risks could arise from fraud, misuse, unintentional use, settlement delay, insufficiency of funds, or other activities. Also, criminals are using increasingly sophisticated methods to engage in illegal activities, such as counterfeiting and fraud. If we are unable to collect such amounts from the customer, or if the customer refuses or is unable, due to bankruptcy or other reasons, to reimburse us, we bear the loss for the amount of the chargeback, refund, or return. While we have policies and procedures to manage and mitigate these risks, we cannot be certain that such processes will be effective. Our failure to limit chargebacks and fraudulent transactions could increase the number of returns, refunds and chargebacks that we have to process. In addition, if the number of returns, refunds and chargebacks increases, card networks or our banking partners could require us to increase reserves, impose penalties on us, charge additional or higher fees, or terminate their relationships with us. Failure to effectively manage risk and prevent fraud could increase our chargeback, refund, and return losses or cause us to incur other liabilities. Increases in chargebacks, refunds, returns, or other liabilities could have an adverse effect on our operating results, financial condition, and cash flows. We route orders through third- party trading venues in connection with our Coinbase Prime trading service. The loss or failure of any such trading venues may adversely affect our business. In connection with our Prime trading service, we routinely route customer orders to third- party exchanges or other trading venues. In connection with these activities, we generally hold cash and other crypto assets with such third- party exchanges or other trading venues in order to effect customer orders. If we were to experience a disruption in our access to these third- party exchanges and trading venues, our Prime trading service could be adversely affected to the extent that we are limited in our ability to execute order flow for our Prime customers. In addition, while we have policies and procedures to help mitigate our risks related to routing orders through third- party trading venues, if any of these third- party trading venues experience any technical, legal, regulatory or other adverse events, such as shutdowns, delays, system failures, suspension of withdrawals, illiquidity, insolvency, or loss of customer assets, we might not be able to fully recover the cash and other crypto assets that we have deposited with these third parties, and these risks may be heightened following the 2022 Events. For example, in connection with the 2022 Events, we were not able to recover an immaterial amount of cash deposited at FTX. As a result, our business, operating results and financial condition could be adversely affected. We have historically had a highly active acquisition and investment strategy and, while we have been less active in acquisitions and investments due to current market conditions, we may from time to time make acquisitions and investments, which could require significant management attention, disrupt our business, result in dilution to our stockholders, and adversely affect our financial results. As part of our business strategy, we have historically been highly active in acquiring and investing in order to, among other things, add specialized employees, complementary companies, products, services, licenses, or technologies. While in 2022 and 2023 , we reduced our activity with respect to acquisitions and investments due to market conditions, we may still from time to time make further acquisitions and investments. As part of our business strategy, we continue to routinely conduct discussions and evaluate opportunities for possible acquisitions, strategic investments, entries into new businesses, joint ventures, and other transactions. In the future, the pace and scale of our acquisitions may increase and may include larger acquisitions than we have done historically. We also invest in companies and technologies, many of which are private companies and technologies that are highly speculative in nature. In the future, we may not be able to find other suitable acquisition and investment candidates, and we may not be able to complete acquisitions or make investments on favorable terms, if at all. In some cases, the costs of such acquisitions may be substantial, and there is no assurance that we will receive a favorable return on investment for our acquisitions. We may in the future be required to write off acquisitions or investments. For example, we recorded gross impairment charges ~~of $ 101. 4 million~~ on our strategic investments in various companies and technologies for the year ended December 31, 2022, primarily as a result of adverse economic conditions and disruption in ~~2022~~ the crypto asset markets . To the extent the adverse economic conditions continue for a prolonged period or there continue to be disruptions in the crypto asset markets , our strategic investments could be further impaired. Moreover, our previous and future acquisitions may not achieve our goals, and any future acquisitions we complete could be viewed negatively by customers, developers, advertisers, or investors. For example, in February 2019, we announced the acquisition of Neutrino S. r. l., a blockchain intelligence platform, whose founders were directly affiliated with the software firm the Hacking Team, which purportedly sold software with surveillance capabilities to governments with authoritarian regimes, resulting in reputational harm to our business, a loss of customers, and increased cost. In addition, if we fail to successfully close or integrate any acquisitions, or integrate the products or technologies associated with such acquisitions into our company, our net revenue and operating results could be adversely affected. Our ability to acquire and integrate companies, products, services, licenses, employees, or technologies in a successful manner is unproven. Any integration process may require significant time and resources, and we may not be able to manage the process successfully, including successfully securing regulatory approvals which may be required to close the transaction and to continue to operate the target firm' s business or products in a manner that is useful to us. We may not successfully evaluate or utilize the acquired products, services, technology, or personnel, or accurately forecast the financial impact of an acquisition transaction, including accounting charges. We may have to pay cash, incur debt, or issue equity securities to pay for any such acquisition, any of which could adversely affect our financial results. The sale of equity or issuance of debt to finance any such acquisitions could result in dilution to our stockholders, which, depending on the size of the acquisition, may be significant. The incurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations. If we fail to develop, maintain, and enhance our brand and reputation, our business, operating results, and financial condition may be adversely affected. Our brand and reputation are key assets and a competitive advantage. Maintaining, protecting, and enhancing our brand depends largely on the success of our marketing efforts, ability to provide consistent, high- quality, and secure products, services, features, and support, and our ability to successfully secure, maintain, and defend our rights to use the " Coinbase " mark and other trademarks important to our brand. We believe that the importance of our brand will increase as competition further intensifies. Our brand and reputation could be harmed if we fail to achieve these objectives

or if our public image were to be tarnished by negative publicity, unexpected events, or actions by third parties. Unfavorable publicity about us, including our products, services, technology, customer service, personnel, and crypto asset or crypto asset platforms generally could diminish confidence in, and the use of, our products and services. Moreover, to the extent that we acquire a company and maintain that acquired company' s separate brand, we could experience brand dilution or fail to retain positive impressions of our own brand to the extent such impressions are instead attributed to the acquired company' s brand. In addition, because we are a founder- led company, actions by, or unfavorable publicity about, Brian Armstrong, our co- founder and Chief Executive Officer, may adversely impact our brand and reputation. Such negative publicity also could have an adverse effect on the size and engagement of our customers and could result in decreased revenue, which could have an adverse effect on our business, operating results, and financial condition. Key business metrics and other estimates are subject to inherent challenges in measurement and to change as our business evolves, and our business, operating results, and financial condition could be adversely affected by real or perceived inaccuracies in those metrics or any changes in metrics we disclose. We regularly review key business metrics, including the number of our ~~Verified Users and~~ MTUs, our Trading Volume ~~and Assets on Platform~~ , and other measures to evaluate growth trends, measure our performance, and make strategic decisions. These key metrics are calculated using ~~both~~ internal company ~~data and third- party~~ data and have not been validated by an independent third- party. While these numbers are based on what we believe to be reasonable estimates for the applicable period of measurement at the time of reporting, there are inherent challenges in such measurements. If we fail to maintain an effective analytics platform, our key metrics calculations may be inaccurate, and we may not be able to identify those inaccuracies. Additionally, ~~while~~ we ~~believe~~ **have in** the **past and may in the future, calculate key business metrics using** third- party data **. While** we **believe the third- party data we have used in the past or may** use **in the future** is reliable, we have not independently verified **and may not in the future independently verify** the accuracy or completeness of the data contained in such sources and ~~we cannot~~ **there can** be **no** ~~assured~~ **assurance** that such data is free of error. Any inaccuracy in the third- party data we use could cause us to overstate or understate our key metrics. We regularly review our processes for calculating these metrics, and from time to time we make adjustments to improve their accuracy. Additionally, ~~certain of~~ our ~~key business metrics, including Verified Users and~~ MTUs ~~, are~~ **metric is** measured at a point in time and as our products and internal processes for calculating these metrics evolve over time, a previously reported number could fluctuate. We generally will not update previously disclosed key business metrics for any such inaccuracies or adjustments that are immaterial. Our key business metrics may also be impacted by compliance or fraud- related bans, technical incidents, or false or spam accounts in existence on our platform. We regularly deactivate fraudulent and spam accounts that violate our terms of service, and exclude these users from the calculation of our key business metrics; however, we may not succeed in identifying and removing all such accounts from our platform. Additionally, users are not prohibited from having more than one account and ~~both~~ our ~~Verified Users and MTU~~ **MTUs** ~~metrics~~ **metric** may overstate the number of unique customers who have registered an account on our platform as one customer may register for, and use, multiple accounts with different email addresses, phone numbers, or usernames. Furthermore, MTUs may overstate the number of unique consumers due to differences in product architecture or user behavior, which may cause MTUs to fluctuate. For example, a user may currently have a Coinbase Wallet account that is unlinked to their registered account on our platform, but then choose to link these accounts in the future as our product offerings evolve. To the extent that the user had activity in both their Wallet and their registered account in the measurement period, what was previously captured as two unique MTUs would now be counted as a single MTU. If **MTUs** ~~our~~ **or our other key business** metrics provide us with incorrect or incomplete information about users and their behavior, we may make inaccurate conclusions about our business. We may change our key business metrics from time to time, which may be perceived negatively. Given the rapid evolution of the crypto markets and our revenue sources, we regularly evaluate whether our key business metrics remain meaningful indicators of the performance of our business. As a result of these evaluations, **in the past** we have decided to make changes, and in the future may make additional changes, to our key business metrics, including eliminating or replacing existing metrics ~~. For example, in order to provide more relevant insight into our current business performance and align with how management views the business, beginning with our Quarterly Report on Form 10- Q for the three months ending March 31, 2023, we do not plan to report Verified Users as a key business metric in our future periodic filings. Moreover, we will no longer present Assets on Platform as a key business metric because this metric is comprised of the aggregate of our " customer crypto liabilities " and our " customer custodial cash liabilities, " which are each set forth on our consolidated balance sheets. For more information see " Management' s Discussion and Analysis of Financial Condition and Results of Operations — Key Business Metrics " in Part II, Item 7 of this Annual Report on Form 10- K~~ . Further if investors or the media perceive any changes to our key business metrics disclosures negatively, our business could be adversely affected. Unfavorable media coverage could negatively affect our business. We receive a high degree of media coverage in the cryptoeconomy and around the world. Unfavorable publicity regarding, for example, our product changes, product quality, litigation or regulatory activity, privacy practices, terms of service, employment matters, the use of our products, services, or supported crypto assets for illicit or objectionable ends, the actions of our customers, or the actions of other companies that provide similar services to ours, has in the past, and could in the future, adversely affect our reputation. Further, we have in the past, and may in the future, be the target of social media campaigns criticizing actual or perceived actions or inactions that are disfavored by our customers, employees, or society at- large, which campaigns could materially impact our customers' decisions to trade on our platform. Any such negative publicity could have an adverse effect on the size, activity, and loyalty of our customers and result in a decrease in net revenue, which could adversely affect our business, operating results, and financial condition. Our platform may be exploited to facilitate illegal activity such as fraud, money laundering, gambling, tax evasion, and scams. If any of our customers use our platform to further such illegal activities, our business could be adversely affected. Our platform may be exploited to facilitate illegal activity including fraud, money laundering, gambling, tax evasion, and scams. We or our partners may be specifically targeted by individuals seeking to conduct fraudulent transfers, and it may be difficult or impossible for us to detect and avoid

such transactions in certain circumstances. The use of our platform for illegal or improper purposes could subject us to claims, individual and class action lawsuits, and government and regulatory investigations, prosecutions, enforcement actions, inquiries, or requests that could result in liability and reputational harm for us. Moreover, certain activities that may be legal in one jurisdiction may be illegal in another jurisdiction, and certain activities that are at one time legal may in the future be deemed illegal in the same jurisdiction. As a result, there is significant uncertainty and cost associated with detecting and monitoring transactions for compliance with local laws. In the event that a customer is found responsible for intentionally or inadvertently violating the laws in any jurisdiction, we may be subject to governmental inquiries, enforcement actions, prosecuted, or otherwise held secondarily liable for aiding or facilitating such activities. Changes in law have also increased the penalties for money transmitters for certain illegal activities, and government authorities may consider increased or additional penalties from time to time. Owners of intellectual property rights or government authorities may seek to bring legal action against money transmitters, including us, for involvement in the sale of infringing or allegedly infringing items. Any threatened or resulting claims could result in reputational harm, and any resulting liabilities, loss of transaction volume, or increased costs could harm our business. Moreover, while fiat currencies can be used to facilitate illegal activities, crypto assets are relatively new and, in many jurisdictions, may be lightly regulated or largely unregulated. Many types of crypto assets have characteristics, such as the speed with which digital currency transactions can be conducted, the ability to conduct transactions without the involvement of regulated intermediaries, the ability to engage in transactions across multiple jurisdictions, the irreversible nature of certain crypto asset transactions, and encryption technology that anonymizes these transactions, that make crypto assets susceptible to use in illegal activity. U. S. federal and state and foreign regulatory authorities and law enforcement agencies, such as the Department of Justice **(“ DOJ ”)** , SEC, CFTC, FTC, or the Internal Revenue Service (“ IRS ”), and various state securities and financial regulators have taken and continue to take legal action against persons and entities alleged to be engaged in fraudulent schemes or other illicit activity involving crypto assets. We also support crypto assets that incorporate privacy- enhancing features, and may from time to time support additional crypto assets with similar functionalities. These privacy- enhancing crypto assets obscure the identities of sender and receiver, and may prevent law enforcement officials from tracing the source of funds on the blockchain. Facilitating transactions in these crypto assets may cause us to be at increased risk of liability arising out of anti- money laundering and economic sanctions laws and regulations. While we believe that our risk management and compliance framework is designed to detect significant illicit activities conducted by our potential or existing customers, we cannot ensure that we will be able to detect all illegal activity on our platform. **Base, an open source permissionless L2 protocol built on the Ethereum blockchain developed by us, has been in the past, and may in the future, be a target for scam tokens or other illegal activity. For example, in August 2023, a number of fraudulent tokens were identified and traded on Base blockchain. As we continue to develop Base, and in light of this fraudulent activity, we continue to invest in improving our security processes, including through our in- house blockchain monitoring capabilities, third- party tools for identifying malicious and out of pattern events, and the monitoring of contract source code and bytecode on Base against a database of known scam code patterns. While to date, such illegal or fraudulent activity on Base has not had a material impact on our business, operating results, financial condition, or cash flows, future illegal activity may have an adverse impact on our business, operating results, financial condition or cash flows and our efforts to identify and remedy such illegal or fraudulent activity may not be successful.** If any of our customers use our platform to further such illegal activities, our business could be adversely affected. Our compliance and risk management methods might not be effective and may result in outcomes that could adversely affect our reputation, operating results, and financial condition. Our ability to comply with applicable complex and evolving laws, regulations, and rules is largely dependent on the establishment, maintenance, and scaling of our compliance, **internal** audit, and reporting systems to continuously keep pace with our customer activity and transaction volume, as well as our ability to attract and retain qualified compliance and other risk management personnel. While we have devoted significant resources to develop policies and procedures to identify, monitor, and manage our risks, and expect to continue to do so in the future, we cannot assure you that our policies and procedures are and will always be effective or that we have been and will always be successful in monitoring or evaluating the risks to which we are or may be exposed in all market environments or against all types of risks, including unidentified or unanticipated risks. Our risk management policies and procedures rely on a combination of technical and human controls and supervision that are subject to error and failure. Some of our methods for managing risk are discretionary by nature and are based on internally developed controls and observed historical market behavior, and also involve reliance on standard industry practices. These methods may not adequately prevent losses, particularly as they relate to extreme market movements, which may be significantly greater than historical fluctuations in the market. Further, as a result of the 2022 Events or similar market disruptions in the future, we may reevaluate our risk management policies and procedures. Accordingly, in the future, we may identify gaps in such policies and procedures or existing gaps may become higher risk, and may require significant resources and management attention. Our risk management policies and procedures also may not adequately prevent losses due to technical errors if our testing and quality control practices are not effective in preventing failures. In addition, we may elect to adjust our risk management policies and procedures to allow for an increase in risk tolerance, which could expose us to the risk of greater losses. Regulators periodically review our compliance with our own policies and procedures and with a variety of laws and regulations. We have received in the past and may from time to time receive additional examination reports citing violations of rules and regulations and inadequacies in existing compliance programs, and requiring us to enhance certain practices with respect to our compliance program, including due diligence, training, monitoring, reporting, and recordkeeping. If we fail to comply with these, or do not adequately remediate certain findings, regulators could take a variety of actions that could impair our ability to conduct our business, including, but not limited to, delaying, denying, withdrawing, or conditioning approval of certain products and services. In addition, regulators have broad enforcement powers to censure, fine, issue cease and desist orders, prohibit us from engaging in some of our business activities, or revoke our licenses. We face significant intervention by regulatory authorities, including

extensive examination and surveillance activities, and will continue to face the risk of significant intervention by regulatory authorities in the future. In the case of non- compliance or alleged non- compliance, we could be subject to investigations and proceedings that may result in substantial penalties or civil lawsuits, including by customers, for damages which can be significant. Any of these outcomes would adversely affect our reputation and brand and our business, operating results, and financial condition. Some of these outcomes could adversely affect our ability to conduct our business. We hold certain investments in DeFi protocols and may suffer losses if they do not function as expected. We hold investments in various DeFi protocols. These protocols achieve their investment purposes through self- executing smart contracts that allow users to invest crypto assets in a pool from which other users can borrow without requiring an intermediate party to facilitate these transactions. These investments earn interest to the investor based on the rates at which borrowers repay the loan, and can generally be withdrawn with no restrictions. However, these DeFi protocols are subject to various risks, including **uncertain regulatory and compliance conditions in large markets such as the United States,** the risk that the underlying smart contract is insecure, the risk that borrowers may default and the investor will not be able to recover its investment, the risk that any underlying collateral may experience significant volatility, and the risk of certain core developers with protocol administration rights can make unauthorized or harmful changes to the underlying smart contract. If any of these risks materialize, our investments in these DeFi protocols may be adversely impacted. We may suffer losses due to abrupt and erratic market movements. The crypto asset market has been characterized by significant volatility and unexpected price movements, and experienced significant declines in 2022. Certain crypto assets may become more volatile and less liquid in a very short period of time, which was the case following the 2022 Events, resulting in market prices being subject to erratic and abrupt market movement, which could harm our business. For instance, abrupt changes in volatility or market movement can lead to extreme pressures on our platform and infrastructure that can lead to inadvertent suspension of services across parts of the platform or the entire platform. As a result, from time to time we experience outages. For example, in ~~2022~~ **2023**, we experienced approximately ~~17~~ **16** outages, with an average outage duration of ~~44~~ **57**. ~~7~~ **4** minutes. Outages can lead to increased customer service expense, can cause customer loss and reputational damage, result in inquiries and actions by regulators, and can lead to other damages for which we may be responsible. Risks Related to Crypto Assets Due to unfamiliarity and some negative publicity associated with crypto asset platforms, confidence or interest in crypto asset platforms may decline. Crypto asset platforms are relatively new. Many of our competitors are unlicensed, unregulated, operate without supervision by any governmental authorities, and do not provide the public with significant information regarding their ownership structure, management team, corporate practices, cybersecurity, and regulatory compliance. As a result, customers and the general public may lose confidence or interest in crypto asset platforms, including regulated platforms like ours. Since the inception of the cryptoeconomy, numerous crypto asset platforms have been sued, investigated, or shut down due to fraud, manipulative practices, business failure, and security breaches. In many of these instances, customers of these platforms were not compensated or made whole for their losses. Larger platforms like us are more appealing targets for hackers and malware, and may also be more likely to be targets of regulatory enforcement actions. For example, in February 2014, Mt. Gox, the then largest crypto asset platform worldwide, filed for bankruptcy protection in Japan after an estimated 700, 000 Bitcoins were stolen from its wallets. In May 2019, Binance, one of the world' s largest platforms, was hacked, resulting in losses of approximately $ 40 million, and in February 2021, Bitfinex settled a long-running legal dispute with the State of New York related to Bitfinex' s alleged misuse of over $ 800 million of customer assets. The 2022 Events resulted in a loss of confidence in the broader cryptoeconomy, adverse reputational impact to crypto asset platforms, increased negative publicity surrounding crypto more broadly, heightened scrutiny by regulators and lawmakers and a call for increased regulations of crypto assets and crypto asset platforms. In addition, there have been reports that a significant amount of crypto asset trading volume on crypto asset platforms is fabricated and false in nature, with a specific focus on unregulated platforms located outside the United States. Such reports may indicate that the market for crypto asset platform activities is significantly smaller than otherwise understood. Negative perception, a lack of stability and standardized regulation in the cryptoeconomy, and the closure or temporary shutdown of crypto asset platforms due to fraud, business failure, hackers or malware, or government mandated regulation, and associated losses suffered by customers may continue to reduce confidence or interest in the cryptoeconomy and result in greater volatility of the prices of assets, including significant depreciation in value. Any of these events could have an adverse impact on our business and our customers' perception of us, including decreased use of our platform and loss of customer demand for our products and services. Depositing and withdrawing crypto assets into and from our platform involve risks, which could result in loss of customer assets, customer disputes and other liabilities, which could adversely impact our business. In order to own, transfer and use a crypto asset on its underlying blockchain network, a person must have a private and public key pair associated with a network address, commonly referred to as a " wallet. " Each wallet is associated with a unique " public key " and " private key " pair, each of which is a string of alphanumerical characters. To deposit crypto assets held by a customer onto our platform or custody platform, a customer must " sign " a transaction that consists of the private key of the wallet from where the customer is transferring crypto assets, the public key of a wallet that we control which we provide to the customer, and broadcast the deposit transaction onto the underlying blockchain network. Similarly, to withdraw crypto assets from our platform or custody platform, the customer must provide us with the public key of the wallet that the crypto assets are to be transferred to, and we would be required to " sign " a transaction authorizing the transfer. In addition, some crypto networks require additional information to be provided in connection with any transfer of crypto assets to or from our platforms. A number of errors can occur in the process of depositing or withdrawing crypto assets into or from our platform, such as typos, mistakes, or the failure to include the information required by the blockchain network. For instance, a user may incorrectly enter our wallet' s public key or the desired recipient' s public key when depositing and withdrawing from our platforms, respectively. Alternatively, a user may transfer crypto assets to a wallet address that the user does not own, control or hold the private keys to. In addition, each wallet address is only compatible with the underlying blockchain network on which it is created. For instance, a Bitcoin wallet address can only be used to send and receive Bitcoins.

If any Ethereum or other crypto assets are sent to a Bitcoin wallet address, or if any of the foregoing errors occur, all of the customer' s sent crypto assets will be permanently and irretrievably lost with no means of recovery. We have encountered and expect to continue to encounter similar incidents with our customers. Such incidents could result in customer disputes, damage to our brand and reputation, legal claims against us, and financial liabilities, any of which could adversely affect our business. Moreover, we hold customer assets one- to- one at all times and we have procedures to process redemptions and withdrawals expeditiously, following the terms of the applicable user agreements. We have not experienced excessive redemptions or withdrawals, or prolonged suspended redemptions or withdrawals, of crypto assets to date. However, similar to traditional financial institutions, we may experience temporary process- related withdrawal delays. For example, we, and traditional financial institutions, may experience such delays if there is a significant volume of withdrawal requests that is vastly beyond anticipated levels. This does not mean we cannot or will not satisfy withdrawals, but this may mean a temporary delay in satisfying withdrawal requests, which we still expect to be satisfied within the withdrawal timelines set forth in the applicable user agreements **or otherwise communicated by us** . To the extent we have process- related delays, even if brief or due to blockchain network congestion **or heightened redemption activity** , and within the terms of an applicable user agreement **or otherwise communicated by us** , we may experience increased customer complaints and damage to our brand and reputation and face additional regulatory scrutiny, any of which could adversely affect our business. A temporary or permanent blockchain " fork " to any supported crypto asset could adversely affect our business. Blockchain protocols, including Bitcoin and Ethereum, are open source. Any user can download the software, modify it, and then propose that Bitcoin, Ethereum, or other blockchain protocols users and miners adopt the modification. When a modification is introduced and a substantial majority of users and miners consent to the modification, the change is implemented and the Bitcoin, Ethereum or other blockchain protocol networks, as applicable, remain uninterrupted. However, if less than a substantial majority of users and miners consent to the proposed modification, and the modification is not compatible with the software prior to its modification, the consequence would be what is known as a " fork " (i. e., " split ") of the impacted blockchain protocol network and respective blockchain, with one prong running the pre- modified software and the other running the modified software. The effect of such a fork would be the existence of two parallel versions of the Bitcoin, Ethereum, or other blockchain protocol network, as applicable, running simultaneously, but with each split network' s crypto asset lacking interchangeability. Both Bitcoin and Ethereum protocols have been subject to " forks " that resulted in the creation of new networks, including Bitcoin Cash ABC, Bitcoin Cash SV, Bitcoin Diamond, Bitcoin Gold, Ethereum Classic, EthereumPOW, and others. Some of these forks have caused fragmentation among platforms as to the correct naming convention for forked crypto assets. Due to the lack of a central registry or rulemaking body, no single entity has the ability to dictate the nomenclature of forked crypto assets, causing disagreements and a lack of uniformity among platforms on the nomenclature of forked crypto assets, and which results in further confusion to customers as to the nature of assets they hold on platforms. In addition, several of these forks were contentious and as a result, participants in certain communities may harbor ill will towards other communities. As a result, certain community members may take actions that adversely impact the use, adoption, and price of Bitcoin, Ethereum, or any of their forked alternatives. Furthermore, hard forks can lead to new security concerns. For instance, when the Ethereum and Ethereum Classic networks split in July 2016, replay attacks, in which transactions from one network were rebroadcast on the other network to achieve " double- spending, " plagued platforms that traded Ethereum through at least October 2016, resulting in significant losses to some crypto asset platforms. Similar replay attacks occurred in connection with the Bitcoin Cash and Bitcoin Cash SV network split in November 2018. Another possible result of a hard fork is an inherent decrease in the level of security due to the splitting of some mining power across networks, making it easier for a malicious actor to exceed 50 % of the mining power of that network, thereby making crypto assets that rely on proof- of- work more susceptible to attack, as has occurred with Ethereum Classic. We do not believe that we are required to support any fork or airdrop or provide the benefit of any forked or airdropped crypto asset to our customers. However, we have in the past and may in the future continue to be subject to claims by customers arguing that they are entitled to receive certain forked or airdropped crypto assets by virtue of crypto assets that they hold with us. If any customers succeed on a claim that they are entitled to receive the benefits of a forked or airdropped crypto asset that we do not or are unable to support, we may be required to pay significant damages, fines or other fees to compensate customers for their losses. Future forks may occur at any time. A fork can lead to a disruption of networks and our information technology systems, cybersecurity attacks, replay attacks, or security weaknesses, any of which can further lead to temporary or even permanent loss of our and our customers' assets. Such disruption and loss could cause us to be exposed to liability, even in circumstances where we have no intention of supporting an asset compromised by a fork. We currently support, and expect to continue to support, certain smart contract- based crypto assets. If the underlying smart contracts for these crypto assets do not operate as expected, they could lose value and our business could be adversely affected. We currently support, and expect to continue to support, various crypto assets that represent units of value on smart contracts deployed on a third- party blockchain. Smart contracts are programs that store and transfer value and execute automatically when certain conditions are met. Since smart contracts typically cannot be stopped or reversed, vulnerabilities in their programming and design can have damaging effects. For instance, in April 2018, a batch overflow bug was found in many Ethereum- based ERC20- compatible smart contract tokens that allowed hackers to create a large number of smart contract tokens, causing multiple crypto asset platforms worldwide to shut down ERC20- compatible token trading. Similarly, in March 2020, a design flaw in the MakerDAO smart contract caused forced liquidations of crypto assets at significantly discounted prices, resulting in millions of dollars of losses to users who had deposited crypto assets into the smart contract. If any such vulnerabilities or flaws come to fruition, smart contract- based crypto assets, including those held by our customers on our platforms, may suffer negative publicity, be exposed to security vulnerabilities, decline significantly in value, and lose liquidity over a short period of time. In some cases, smart contracts can be controlled by one or more " admin keys " or users with special privileges, or " super users. " These users have the ability to unilaterally make changes to the smart contract, enable or disable features on the smart contract, change how the smart contract

receives external inputs and data, and make other changes to the smart contract. For smart contracts that hold a pool of reserves, these users may also be able to extract funds from the pool, liquidate assets held in the pool, or take other actions that decrease the value of the assets held by the smart contract in reserves. Even for crypto assets that have adopted a decentralized governance mechanism, such as smart contracts that are governed by the holders of a governance token, such governance tokens can be concentrated in the hands of a small group of core community members, who would be able to make similar changes unilaterally to the smart contract. If any such super user or group of core members unilaterally make adverse changes to a smart contract, the design, functionality, features and value of the smart contract, its related crypto assets may be harmed. In addition, assets held by the smart contract in reserves may be stolen, misused, burnt, locked up or otherwise become unusable and irrecoverable. These super users can also become targets of hackers and malicious attackers. If an attacker is able to access or obtain the super user privileges of a smart contract, or if a smart contract' s super users or core community members take actions that adversely affect the smart contract, our customers who hold and transact in the affected crypto assets may experience decreased functionality and value of the applicable crypto assets, up to and including a total loss of the value of such crypto assets. Although we do not control these smart contracts, any such events could cause customers to seek damages against us for their losses, result in reputational damage to us, or in other ways adversely impact our business. From time to time, we may encounter technical issues in connection with the integration of supported crypto assets and changes and upgrades to their underlying networks, which could adversely affect our business. In order to support any supported crypto asset, a variety of front and back- end technical and development work is required to implement our wallet, custody, trading, staking and other solutions for our customers, and to integrate such supported crypto asset with our existing technical infrastructure. For certain crypto assets, a significant amount of development work is required and there is no guarantee that we will be able to integrate successfully with any existing or future crypto asset. In addition, such integration may introduce software errors or weaknesses into our platform, including our existing infrastructure. Even if such integration is initially successful, any number of technical changes, software upgrades, soft or hard forks, cybersecurity incidents, or other changes to the underlying blockchain network may occur from time to time, causing incompatibility, technical issues, disruptions, or security weaknesses to our platform. If we are unable to identify, troubleshoot and resolve any such issues successfully, we may no longer be able to support such crypto asset, our customers' assets may be frozen or lost, the security of our hot, warm, or cold wallets may be compromised, and our platform and technical infrastructure may be affected, all of which could adversely impact our business. If miners or validators of any supported crypto asset demand high transaction fees, our operating results may be adversely affected. We charge miner fees when a customer sends certain crypto assets from their Coinbase account to a non- Coinbase account. We estimate the miner fee based on the cost that we will incur to process the withdrawal transaction on the underlying blockchain network. In addition, we also pay miner fees when we move crypto assets for various operational purposes, such as when we transfer crypto assets between our hot and cold wallets, for which we do not charge our customers. However, miner fees have been and may continue to be unpredictable. **If** ~~Even though Bitcoin' s miner fees have continued to decrease, if~~ the block rewards for miners on any blockchain network are not sufficiently high to incentivize miners, miners may demand higher transaction fees, or collude to reject low transaction fees and force users to pay higher fees. Although we generally attempt to pass miner fees relating to customer withdrawals through to our customers, we have in the past incurred, and expect to incur from time to time, losses associated with the payment of miner fees in excess of what we charge our customers, resulting in adverse impacts on our operating results. Future developments regarding the treatment of crypto assets for U. S. and foreign tax purposes could adversely impact our business. Due to the new and evolving nature of crypto assets and the absence of comprehensive legal and tax guidance with respect to crypto asset products and transactions, many significant aspects of the U. S. and foreign tax treatment of transactions involving crypto assets, such as the purchase and sale of crypto assets on our platform, as well as the provision of staking rewards and other crypto asset incentives and rewards products, are uncertain, and it is unclear whether, when and what guidance may be issued in the future on the treatment of crypto asset transactions for U. S. and foreign ~~income~~ tax purposes. In 2014, the IRS released Notice 2014- 21, discussing certain aspects of " virtual currency " for U. S. federal income tax purposes and, in particular, stating that such virtual currency (i) is " property, " (ii) is not " currency " for purposes of the rules relating to foreign currency gain or loss, and (iii) may be held as a capital asset. ~~In 2019~~ **From time to time** , the IRS **has** released ~~Revenue~~ **other notices and** ~~Ruling~~ **rulings relating** ~~2019- 24 and a set of " Frequently Asked Questions " (which have been periodically updated), that provide additional guidance, including guidance~~ to ~~the effect that, under certain circumstances, hard forks of digital currencies are taxable events giving rise to ordinary income and guidance with respect to the determination of~~ the tax ~~basis~~ **treatment** of virtual currency **or crypto assets reflecting the IRS' s position on certain issues** . **The IRS has** ~~However, this guidance does~~ not ~~address~~ **addressed many** other significant aspects of the U. S. federal income tax treatment of crypto assets and related transactions. There continues to be uncertainty with respect to the timing, character and amount of income inclusions for various crypto asset transactions including, but not limited to lending and borrowing crypto assets, staking ~~rewards~~ and other crypto asset incentives and ~~rewards~~ products that we offer. Although we believe our treatment of crypto asset transactions for federal income tax purposes is consistent with existing **positions from** ~~guidance provided by~~ the IRS and **/ or** existing U. S. federal income tax principles, because of the rapidly evolving nature of crypto asset innovations and the increasing variety and complexity of crypto asset transactions and products, it is possible the IRS and various U. S. states may disagree with our treatment of certain crypto asset offerings for U. S. tax purposes, which could adversely affect our customers and the vitality of our business. Similar uncertainties exist in the foreign markets in which we operate **with respect to direct and indirect taxes** , ~~affecting~~ **and these uncertainties and potential adverse interpretations of tax law could impact the amount of tax we and** our non- U. S. ~~customer base, and these uncertainties and potential adverse interpretations of tax law could affect our non- U. S.~~ customers **are required to pay,** and the vitality of our platforms outside of the United States. There can be no assurance that the IRS, the U. S. state revenue agencies or other foreign tax authorities, will not alter their respective positions with respect to crypto assets in the future or that a court would uphold the

treatment set forth in existing ~~guidance~~ **positions** . It also is unclear what additional ~~guidance~~ **tax authority positions, regulations, or legislation** may be issued in the future on the treatment of existing crypto asset transactions and future crypto asset innovations **under** ~~for purposes of~~ U. S. ~~tax~~ **federal, U. S. state** or ~~other~~ foreign tax ~~regulations~~ **law** . Any such **developments** ~~alteration of existing IRS, U. S. state and foreign tax authority positions or additional guidance regarding crypto asset products and transactions~~ could result in adverse tax consequences for holders of crypto assets and could have an adverse effect on the value of crypto assets and the broader crypto assets markets. Future technological and operational developments that may arise with respect to crypto assets may increase the uncertainty with respect to the treatment of crypto assets for U. S. and foreign tax purposes. The uncertainty regarding tax treatment of crypto asset transactions impacts our customers, and could impact our business, both domestically and abroad. Our tax information reporting obligations with respect to crypto transactions are subject to change. Although we believe we are compliant with U. S. tax reporting and withholding requirements with respect to our customers' crypto asset transactions, the exact scope and application of such requirements, including but not limited to U. S. onboarding requirements through ~~Form~~ **Forms** ~~W~~ **W9 and W8** , backup withholding, **non- resident alien withholding,** and Form 1099 **and Form 1042- S** reporting obligations, is not entirely clear for all of the crypto asset transactions that we facilitate. In November 2021, the U. S. Congress passed the Infrastructure Investment and Jobs Act (the " IIJA "), providing that **brokers (which appear to include** exchanges such as Coinbase **)** would be responsible for reporting to the IRS the transactions of their customers in digital assets, including transfers to other exchanges or non- exchanges. In **August 2023,** ~~their~~ -- **the** ~~current form,~~ **U. S. Treasury Department and the IRS released proposed regulations on tax information reporting in connection with** the IIJA ~~' s new provisions~~ **(the " Proposed Regulations ")** for reporting transactions with respect to digital assets ~~will become effective beginning with Form 1099s filed in 2024~~ . **The Proposed Regulations** ~~In connection with the IIJA, it is expected that the IRS will~~ introduce new rules related to our tax reporting and withholding obligations on our customer transactions in ~~the future, likely in~~ ways that differ from our existing compliance protocols and ~~where~~ there is risk that we ~~do~~ **will** not have proper records to ensure compliance for certain legacy customers **or transactions** . If the IRS determines that we are not in compliance with our tax reporting or withholding requirements with respect to customer crypto asset transactions, we may be exposed to significant **taxes and** penalties, which could adversely affect our financial position. **The Proposed Regulations** ~~We anticipate guidance from the IRS regarding tax reporting and withholding obligations with respect to customer crypto asset transactions that~~ will ~~likely~~ require us to invest substantially in new compliance measures and that may require significant retroactive compliance efforts, which also **could adversely affect our financial position. Further, final regulations may differ materially from the Proposed Regulations, which could cause additional compliance efforts, and which** could adversely affect our financial position. Similarly, it is likely that new rules for reporting crypto assets under the global " common reporting standard " as well as the " crypto- asset reporting framework " will be implemented on our international operations, creating new obligations and a need to invest in new onboarding and reporting infrastructure. Such rules are under discussion today by the member and observer states of the " Organization for Economic Cooperation and Development " and by the European Commission on behalf of the member states of the European Union. These new rules may give rise to potential liabilities or disclosure requirements for prior customer arrangements and new rules that affect how we onboard our customers and report their transactions to taxing authorities. **Additionally, the European Union has issued directives, commonly referred to as " CESOP " (the Central Electronic System of Payment information), requiring payment service providers in the European Union to report cross- border fiat transactions to taxing authorities on a quarterly basis beginning in January 2024. Any actual or perceived failure by us to comply with the above or any other emerging tax regulations that apply to our operations could harm our business.** The nature of our business requires the application of complex financial accounting rules, and there is limited guidance from accounting standard setting bodies **on certain topics** . If financial accounting standards undergo significant changes, our operating results could be adversely affected. The accounting rules and regulations that we must comply with are complex and subject to interpretation by the Financial Accounting Standards Board (the " FASB "), the SEC, and various **other** bodies formed to promulgate and interpret appropriate accounting principles. ~~A~~ **Recent actions and public comments from the FASB and the SEC have focused on the integrity of financial reporting and internal controls and many companies' accounting policies are being subjected to heightened scrutiny by regulators and the public. Further, there has been limited precedent for the financial accounting of crypto assets and related valuation and revenue recognition. Moreover, a** change in these principles or interpretations could have a significant effect on our reported financial results, and may even affect the reporting of transactions completed before the announcement or effectiveness of a change. For example, on March 31, 2022, the staff of the SEC issued Staff Accounting Bulletin No. 121 ~~, or~~ **("** SAB 121 **")** , which ~~represents~~ **represented** a significant change regarding how a company safeguarding crypto assets held for its platform users reports such crypto assets on its balance sheet and ~~requires~~ **required** retrospective application as of January 1, 2022. **While** ~~Moreover, recent actions and public comments from~~ the ~~FASB and~~ **legal status of SAB 121 is currently uncertain following a U. S. Government Accountability Office decision concluding that** the SEC **failed to follow proper administrative procedures in its issuance of SAB 121, SAB 121 remains applicable at this time. Additionally, historically, including for the reporting periods included in this Annual Report on Form 10- K, we** have ~~focused on the integrity of financial reporting and internal controls. In addition, many companies' accounting policies are being subjected to heightened scrutiny by regulators and the public. Further, there has been limited precedent for the financial accounting of crypto assets and related valuation and revenue recognition. Currently, we account~~ **accounted** for the crypto assets we hold for investment and operating purposes as intangible assets with indefinite useful lives, which requires us to measure these crypto assets at cost less impairment. As a result of the high volatility in the cryptoeconomy and of crypto asset prices, ~~which may continue to experience significant declines,~~ we **have** ~~may continue to record~~ **recorded** impairment charges on the crypto assets we hold ~~in a particular period~~ . For example, for the ~~year~~ **years** ended December 31, **2023 and** 2022, we recorded gross impairment charges of $ **96. 8 million and $** 757. 3 million **, respectively,** due to the observed market price of crypto assets decreasing below the carrying

value during ~~the~~ **these** ~~period~~ **periods** . ~~In May~~ **However, in December** ~~2022~~ **2023** , the FASB **issued** ~~added a project to its technical agenda to improve the accounting~~ **Accounting Standards Update No. 2023- 08, Intangibles — Goodwill and Other — Crypto Assets (ASU 2023- 08): Accounting** for and ~~disclosure~~ **Disclosure** of ~~certain~~ **Crypto Assets (" ASU 2023- 08 "), which represents a significant change in how entities that hold** crypto assets **will account for certain of** ~~. In October and December 2022, the~~ **those** ~~FASB tentatively decided that~~ **holdings. ASU 2023- 08 will require us to measure** crypto assets ~~within~~ **that meet** the scope ~~of the project should be~~ **criteria at fair value and to reflect changes in fair value in net income each reporting period. The amendments in ASU 2023- 08 will also require us to present crypto assets** measured at fair value ~~with~~ **separately from other intangible assets on the balance sheet and** changes in **the** fair value ~~recorded~~ **measurement of crypto assets separately from changes** in **the carrying amounts of other intangible assets on** the income statement. ~~On February~~ **The amendments in ASU 2023- 08 are effective for fiscal years beginning after December 15, 2024, with early adoption permitted before then. We have elected to early adopt the updated standard effective as of January** 1, ~~2023~~ **2024** ~~, the FASB further clarified that the scope of the project excludes crypto assets issued and created by the reporting entity and its related parties and directed its staff to draft a proposed Accounting Standards Update (" ASU ") with a public comment period for 75 days. The FASB has not publicly communicated a timeline for the issuance of the proposed ASU. As such, there remains significant uncertainty on how companies can account for crypto assets transactions, crypto assets, and related revenue~~ . Uncertainties in or changes to regulatory or financial accounting standards could result in the need to change our accounting methods and restate our financial statements and impair our ability to provide timely and accurate financial information, which could adversely affect our financial statements, result in a loss of investor confidence, and more generally impact our business, operating results, and financial condition. Risks Related to Government Regulation and Privacy Matters The cryptoeconomy is novel. As a result, policymakers are just beginning to consider what a regulatory regime for crypto would look like and the elements that would serve as the foundation for such a regime. This less developed consideration of crypto may harm our ability to effectively react to proposed legislation and regulation of crypto assets or crypto asset platforms adverse to our business. As crypto assets have grown in both popularity and market size, various U. S. federal, state, and local and foreign governmental organizations, consumer agencies and public advocacy groups have been examining the operations of crypto networks, users and platforms, with a focus on how crypto assets can be used to launder the proceeds of illegal activities, fund criminal or terrorist enterprises, and the safety and soundness of platforms and other service providers that hold crypto assets for users. Many of these entities have called for heightened regulatory oversight, and have issued consumer advisories describing the risks posed by crypto assets to users and investors. For instance, in September 2022, the White House published a fact sheet described as the first- ever " Comprehensive Framework for Responsible Development of Digital Assets, " which encouraged " agencies to issue guidance and rules to address current and emergent risks in the digital asset ecosystem. " ~~The cryptoeconomy is novel. As a result, many policymakers are just beginning to consider what a regulatory regime for crypto would look like and the elements that would serve as the foundation for such a regime.~~ Competitors, including traditional financial services, have spent years cultivating professional relationships with relevant policymakers on behalf of their industry so that those policymakers may understand that industry, the current legal landscape affecting that industry, and the specific policy proposals that could be implemented in order to responsibly develop that industry. The lobbyists working for these competitors have similarly spent years developing and working to implement strategies to advance these industries. Members of the cryptoeconomy have started to engage policymakers directly and with the help of external advisors and lobbyists **. For example** , ~~but~~ **in order to advance our mission, in February 2022 we launched our Coinbase Innovation Political Action Committee to support crypto- forward political candidates and initiatives. Further, in December 2023, we together with a number of other crypto and blockchain market participants supported the launch of the Fairshake Political Action Committee to support political candidates in the 2024 U. S. presidential election who support crypto and blockchain innovation and responsible regulation. However,** this work is in a relatively nascent stage ~~and progress in this area could suffer setbacks following the 2022 Events~~ . As a result, new laws and regulations may be proposed and adopted in the United States and internationally, or existing laws and regulations may be interpreted in new ways, that harm the cryptoeconomy or crypto asset platforms, which could adversely impact our business **. Additionally, our political activities to further our mission may be perceived unfavorably by investors and the public and have an adverse impact on our brand and reputation** . Our consolidated balance sheets may not contain sufficient amounts or types of regulatory capital to meet the changing requirements of our various regulators worldwide, which could adversely affect our business, operating results, and financial condition. We are required to possess sufficient financial soundness and strength to adequately support our regulated subsidiaries. We may from time to time incur indebtedness and other obligations which could make it more difficult to meet these capitalization requirements or any additional regulatory requirements. In addition, although we are not a bank holding company for purposes of United States law or the law of any other jurisdiction, as a global provider of financial services and in light of the changing regulatory environment in various jurisdictions, we could become subject to new capital requirements introduced or imposed by the United States and international regulators. Any change or increase in these regulatory requirements could have an adverse effect on our business, operating results, and financial condition. As a financial institution licensed to, among other things, engage in money transmission in the United States, to conduct virtual currency business activity in New York, and issue electronic money in Europe, we are subject to strict rules governing how we manage and hold customer fiat currency and crypto assets. We maintain complex treasury operations to manage and move customer fiat currency and crypto assets across our platforms and to comply with regulatory requirements. However, it is possible we may experience errors in fiat currency and crypto asset handling, accounting, and regulatory reporting that lead us to be out of compliance with these requirements. In addition, regulators may increase the amount of fiat currency reserves that we are required to maintain for our operations, as has happened in the past. For instance, in 2017, the Hawaii Division of Financial Institutions imposed a new policy whereby digital currency businesses are required to maintain cash reserves in an amount equal to the aggregate face value of digital currency

funds held on behalf of customers, making our operations in Hawaii impracticable and forcing us to shut down operations in the state at the time. Any similar events can lead to sanctions, penalties, changes to our business operations, or the revocation of licenses. Frequent launch of new products and services, including Learning Rewards ~~(formerly " Earn ") ~~campaigns, margin trading, lending functions, and the addition of new payment rails increase these risks. Many of the crypto assets in which we facilitate trading are subject to regulatory authority by the CFTC. Any fraudulent or manipulative activity in a crypto asset occurring on our platform could subject us to increased regulatory scrutiny, regulatory enforcement, and litigation. The CFTC has stated and judicial decisions involving CFTC enforcement actions have confirmed that at least some crypto assets, including Bitcoin, **ether, litecoin, and stablecoins, such as USDC, USDT and BUSD,** fall within the definition of a " commodity " under the CEA. As a result, the CFTC has general enforcement authority to police against manipulation and fraud in at least some spot crypto asset markets. From time to time, manipulation, fraud, and other forms of improper trading by market participants have resulted in, and may in the future result in, CFTC investigations, inquiries, enforcement action, and similar actions by other regulators, government agencies, and civil litigation. Such investigations, inquiries, enforcement actions, and litigation may cause us to incur substantial costs and could result in negative publicity. Certain transactions in crypto assets may constitute " retail commodity transactions " subject to regulation by the CFTC as futures contracts. If crypto asset transactions we facilitate are deemed to be such retail commodity transactions, we would be subject to additional regulatory requirements, licenses and approvals, and potentially face regulatory enforcement, civil liability, and significant increased compliance and operational costs. Any transaction in a commodity, including a crypto asset, entered into with or offered to retail investors using leverage, margin, or other financing arrangements (a " retail commodity transaction ") is subject to CFTC regulation as a futures contract unless such transaction results in actual delivery within 28 days. The meaning of " actual delivery " has been the subject of commentary and litigation, and in 2020, the CFTC adopted interpretive guidance addressing the " actual delivery " of a crypto asset. To the extent that crypto asset transactions that we facilitate or facilitated are deemed retail commodity transactions, including pursuant to current or subsequent rulemaking or guidance by the CFTC, we may be subject to additional regulatory requirements and oversight, and we could be subject to judicial or administrative sanctions if we do not or did not at a relevant time possess appropriate registrations. The CFTC has previously brought enforcement actions against entities engaged in retail commodity transactions without appropriate registrations **, as well as recent enforcement settled orders against developers of decentralized platforms** . Particular crypto assets or transactions therein could be deemed " commodity interests " (e. g., futures, options, swaps) or security- based swaps subject to regulation by the CFTC or SEC, respectively. If a crypto asset that we facilitate trading in is deemed a commodity interest or a security- based swap, we would be subject to additional regulatory requirements, registrations and approvals, and potentially face regulatory enforcement, civil liability, and significant increased compliance and operational costs. Commodity interests, as such term is defined by the CEA and CFTC rules and regulations, are subject to more extensive supervisory oversight by the CFTC, including registrations of entities engaged in, and platforms offering, commodity interest transactions. This CFTC authority extends to crypto asset futures contracts and swaps, including transactions that are based on current and future prices of crypto assets and indices of crypto assets. To the extent that a crypto asset in which we facilitate or facilitated trading or transactions in a crypto asset which we facilitate or facilitated are deemed to fall within the definition of a commodity interest, including pursuant to subsequent rulemaking or guidance by the CFTC, we may be subject to additional regulatory requirements and oversight and could be subject to judicial or administrative sanctions if we do not or did not at a relevant time possess appropriate registrations as an exchange (for example, as a designated contract market for trading futures or options on futures, or as a swaps execution facility for trading swaps) or as a registered intermediary (for example, as a futures commission merchant or introducing broker). Such actions could result in injunctions, cease and desist orders, as well as civil monetary penalties, fines, and disgorgement, as well as reputational harm. The CFTC has previously brought enforcement actions against entities engaged in crypto asset activities for failure to obtain appropriate exchange, execution facility and intermediary registrations. Furthermore, the CFTC and the SEC have jointly adopted regulations defining " security- based swaps, " which include swaps based on single securities and narrow- based indices of securities. If a crypto asset is deemed to be a security, certain transactions referencing that crypto asset could constitute a security- based swap. A crypto asset or transaction therein that is based on or references a security or index of securities, whether or not such securities are themselves crypto assets, could also constitute a security- based swap. To the extent that a crypto asset in which we facilitate or have facilitated trading or transactions in a crypto asset which we facilitate or have facilitated are deemed to fall within the definition of a security- based swap, including pursuant to subsequent rulemaking or guidance by the CFTC or SEC, we may be subject to additional regulatory requirements and oversight by the SEC and could be subject to judicial or administrative sanctions if we do not or did not a relevant time possess appropriate registrations as an exchange (for example, as a security- based swaps execution facility) or as a registered intermediary (for example, as a security- based swap dealer or broker- dealer). This could result in injunctions, cease and desist orders, as well as civil monetary penalties, fines, and disgorgement, as well as reputational harm. We obtain and process a large amount of sensitive customer data. Any real or perceived improper use of, disclosure of, or access to such data could harm our reputation, as well as have an adverse effect on our business. We obtain and process large amounts of sensitive data, including personal data related to our customers and their transactions, such as their names, addresses, social security numbers, visa information, copies of government- issued identification, facial recognition data (from scanning of photographs for identity verification), trading data, tax identification, and bank account information. We face risks, including to our reputation, in the handling and protection of this data, and these risks will increase as our business continues to expand, including through our acquisition of, and investment in, other companies and technologies. Federal, state, and international laws and regulations governing privacy, data protection, and e- commerce transactions require us to safeguard our customers', employees', and service providers' personal data. We have administrative, technical, and physical security measures and controls in place and maintain a robust information security program. However, our security measures, or the security measures of companies we acquire, may be inadequate or breached as a result of third-

party action, employee or service provider error, malfeasance, malware, phishing, hacking attacks, system error, trickery, advances in computer capabilities, new discoveries in the field of cryptography, inadequate facility security or otherwise, and, as a result, someone may be able to obtain unauthorized access to sensitive information, including personal data, on our systems. We could be the target of a cybersecurity incident, which could result in harm to our reputation and financial losses. Additionally, our customers have been and could be targeted in cybersecurity incidents like an account takeover, which could result in harm to our reputation and financial losses. For example, in 2021, third parties independently obtained login credentials and personal information for at least 6, 000 customers and used those credentials to exploit a vulnerability that previously existed in the account recovery process. Coinbase reimbursed impacted customers approximately $ 25. 1 million. Additionally, privacy and data protection laws are evolving, and these laws may be interpreted and applied in a manner that is inconsistent with our data handling safeguards and practices that could result in fines, lawsuits, and other penalties, and significant changes to our or our third- party partners **'** business practices and products and service offerings. Our future success depends on the reliability and security of our platform. To the extent that the measures we, any companies we acquire, or our third- party business partners have taken prove to be insufficient or inadequate, or to the extent we discover a security breach suffered by a company we acquire following the closing of such acquisition, we may become subject to litigation, breach notification obligations, or regulatory or administrative sanctions, which could result in significant fines, penalties, damages, harm to our reputation, or loss of customers. If our own confidential business information or sensitive customer information were improperly disclosed, our business could be adversely affected. Additionally, a party who circumvents our security measures could, among other effects, appropriate customer information or other proprietary data, cause interruptions in our operations, or expose customers to hacks, viruses, and other disruptions. Depending on the nature of the information compromised, in the event of a data breach or other unauthorized access to our customer data, we may also have obligations to notify customers and regulators about the incident, and we may need to provide some form of remedy, such as a subscription to credit monitoring services, pay significant fines to one or more regulators, or pay compensation in connection with a class- action settlement (including under the private right of action under the California Consumer Privacy Act of 2018 (the " CCPA "), which is expected to increase security breach litigation). Such breach notification laws continue to evolve and may be inconsistent from one jurisdiction to another **. In the United States, the SEC has adopted rules for mandatory disclosure of cybersecurity incidents suffered by public companies, as well as cybersecurity governance and risk management** . Complying with these obligations could cause us to incur substantial costs and could increase negative publicity surrounding any incident that compromises customer data **. Any failure or perceived failure by us to comply with these laws may also subject us to enforcement action or litigation, any of which could harm our business** . Additionally, the financial exposure from the events referenced above could either not be insured against or not be fully covered through any insurance that we may maintain, and there can be no assurance that the limitations of liability in any of our contracts would be enforceable or adequate or would otherwise protect us from liabilities or damages as a result of the events referenced above. Any of the foregoing could have an adverse effect on our business, reputation, operating results, and financial condition. Furthermore, we may be required to disclose personal data pursuant to demands from individuals, regulators, government agencies, and law enforcement agencies in various jurisdictions with conflicting privacy and security laws, which could result in a breach of privacy and data protection policies, notices, laws, rules, court orders, and regulations. Additionally, changes in the laws and regulations that govern our collection, use, and disclosure of customer data could impose additional requirements with respect to the retention and security of customer data, could limit our marketing activities, and have an adverse effect on our business, operating results, and financial condition. We are subject to laws, regulations, and industry requirements related to data privacy, data protection and information security, and user protection across different markets where we conduct our business, including in the United States, European Economic Area (the " EEA ") and Asia- Pacific region and industry requirements and such laws, regulations, and industry requirements are constantly evolving and changing. Any actual or perceived failure to comply with such laws, regulations, and industry requirements, or our privacy policies, could harm our business. Various local, state, federal, and international laws, directives, and regulations apply to our collection, use, retention, protection, disclosure, transfer, and processing of personal data. These data protection and privacy laws and regulations are subject to uncertainty and continue to evolve in ways that could adversely impact our business. These laws have a substantial impact on our operations both outside and in the United States, either directly or as a data processor and handler for various offshore entities. In the United States, state and federal lawmakers and regulatory authorities have increased their attention on the collection and use of user data. In the United States, non- sensitive user data generally may be used under current rules and regulations, subject to certain restrictions, so long as the person does not affirmatively " opt- out " of the collection or use of such data. If an " opt- in " model or additional required " opt- outs " were to be adopted in the United States, less data may be available, and the cost of data likely would increase. For example, California enacted the CCPA (effective January 2020) and the California Privacy Rights Act (the " CPRA ") (effective January 2023), which expands upon and amends the CCPA. The CCPA and the CPRA require covered companies to, among other things, provide new disclosures to California users, and affords such users new privacy rights such as the ability to opt- out of certain sales of personal information and expanded rights to access and require deletion of their personal information, opt out of certain personal information sharing, and receive detailed information about how their personal information is collected, used, and shared. The CCPA provides for civil penalties for violations, as well as a private right of action for security breaches that may increase security breach litigation. ~~Potential uncertainty surrounding the CCPA and CPRA may increase our compliance costs and potential liability, particularly in the event of a data breach, and could have a material adverse effect on our business, including how we use personal information, our financial condition, the results of our operations or prospects.~~ Other states have followed California' s lead. For example, in 2021, Virginia passed the Consumer Data Protection Act (the " CDPA ") (effective January 2023) and Colorado passed the Colorado Privacy Act (the " CPA ") (effective July 2023) to provide comparable consumer privacy rights to the CCPA / CPRA. We cannot fully predict the impact of the CCPA, CPRA,

CDPA, CPA, or other similar laws or regulations on our business or operations, but compliance may require us to modify our data processing practices and policies incurring costs and expense. Further, to the extent multiple state- level laws are introduced with inconsistent or conflicting standards, it may require costly and difficult efforts to achieve compliance with such laws ~~that~~ **. Our failure or perceived failure to comply with the CCPA, CPRA, CDPA, CPA, or other similar laws or regulations passed in the future** could **have a material adverse effect** ~~expose us to fines and penalties for non- compliance~~ **on our business** ~~, particularly regarding legal obligations in the wake of a data breach~~ **including how we use personal information, our business, operating results, and financial condition** . Further, in October 2022, the CFPB re- opened the public comment period in connection with an inquiry that it launched in October 2021 into the data use and protection business practices of several large payments companies. The impact of this inquiry is uncertain and could result in stringent restrictions on the use of customer data. Additionally, many foreign countries and governmental bodies, including Australia, Brazil, Kenya, the European Union, India, Japan, Philippines, Indonesia, Singapore, United Kingdom, Switzerland, and numerous other jurisdictions in which we operate or conduct our business, have laws and regulations concerning the collection, use, processing, storage, and deletion of personal information obtained from their residents or by businesses operating within their jurisdiction. These laws and regulations often are more restrictive than those in the United States. Such laws and regulations may require companies to implement new privacy and security policies, permit individuals to access, correct, and delete personal information stored or maintained by such companies, inform individuals of security breaches that affect their personal information, require that certain types of data be retained on local servers within these jurisdictions, and, in some cases, obtain individuals' affirmative opt- in consent to collect and use personal information for certain purposes. In Europe, the General Data Protection Regulation (the " GDPR ") took effect on May 25, 2018. As a result of our presence in Europe and our service offering in the European Union, we are subject to the GDPR, which imposes stringent E. U. data protection requirements, and could increase the risk of non- compliance and the costs of providing our products and services in a compliant manner. A breach of the GDPR could result in regulatory investigations, reputational damage, fines and sanctions, orders to cease or change our processing of our data, enforcement notices, or assessment notices (for a compulsory audit). We may also face civil claims including representative actions and other class action type litigation (where individuals have suffered harm), potentially amounting to significant compensation or damages liabilities, as well as associated costs, diversion of internal resources, and reputational harm. Administrative fines under the GDPR can amount up to 20 million Euros or four percent of the group' s annual global turnover, whichever is highest. Additionally, the United Kingdom (the " U. K. ") implemented its own Data Protection Act, effective in May 2018 and statutorily amended in 2019, which is further supplemented by the U. K. GDPR, which came into effect on January 1, 2021. The U. K. GDPR is based on the E. U. GDPR which applied in the U. K. before that date, with some changes to make it work more effectively in a U. K. context, including its own derogations, for how GDPR is applied in the U. K. From the beginning of 2021 (when the transitional period following Brexit expired), we have to continue to comply with the E. U. GDPR as well as the U. K.' s Data Protection Act and U. K. GDPR, with each regime having the ability to result in fines up to the greater of € 20 million (£ 17. 5 million) or 4 % of global turnover. Both the E. U. GDPR (covering the EEA) as well as U. K. and Swiss data protection laws impose strict rules on the transfer of personal data out of the E. U., U. K., or Switzerland to a " third country, " including the United States. ~~These obligations may be interpreted and applied in a manner that is inconsistent from one jurisdiction to another and may conflict with other requirements or our practices.~~ On ~~July 16, 2020, the Court of Justice of the European Union (the " CJEU ") invalidated the E. U.- U. S., Privacy Shield (under which personal data could be transferred from the E. U. to U. S. entities that had self- certified under the Privacy Shield scheme) on the grounds that the Privacy Shield failed to offer adequate protections to E. U. personal data transferred to the United States. In addition, while the CJEU upheld the adequacy of the standard contractual clauses (a standard form of contract approved by the European Commission as an adequate personal data transfer mechanism, and potential alternative to the Privacy Shield), it made clear that reliance on them alone may not necessarily be sufficient in all circumstances. Use of the standard contractual clauses must now be assessed on a case by case basis taking into account the legal regime applicable in the destination country, in particular applicable surveillance laws and rights of individuals. The use of standard contractual clauses for the transfer of personal data specifically to the United States remains under review by a number of European data protection supervisory authorities, along with those of some other E. U. member states. German and Irish supervisory authorities have indicated, and enforced in recent rulings, that the standard contractual clauses alone provide inadequate protection for E. U.- U. S. data transfers. Further, on~~ June 4, 2021 the European Commission finalized new versions of the Standard Contractual Clauses, with the Implementing Decision now in effect. The U. K. Information Commissioner' s Office of the Data Protection Authority published the U. K. version of the Standard Contractual Clauses (the " SCCS "), and by March 2024, we will be required to use and honor these clauses for transfers of U. K. residents' personal data to a foreign country that does not have adequate data protection. **Effective July 10, 2023, the new E. U.- U. S. Data Privacy Framework (" DPF ") has been recognized as adequate under E. U. law to allow transfers of personal data from the E. U. to certified companies in the U. S. However, the DPF is subject to further legal challenge which could cause the legal requirements for personal data transfers from the E. U. to the U. S. to become uncertain once again. E. U. data protection authorities have and may again block the use of certain U. S.- based services that involve the transfer of personal data to the U. S. In the E. U. and other markets, potential new rules and restrictions on the flow of data across borders could increase the cost and complexity of doing business in those regions.** While we maintain a **DPF** ~~Privacy Shield~~ certification, we **still** rely on the standard contractual clauses for intercompany data transfers from the European Union to the United States ~~and have reviewed and amended any existing vendor agreements that rely only on Privacy Shield as the data transfer mechanism~~ . As supervisory authorities continue to issue further guidance on personal data, we could suffer additional costs, complaints, or regulatory investigations or fines, and if we are otherwise unable to transfer personal data between and among countries and regions in which we operate, it could affect the manner in which we provide our services, the geographical location or segregation of our relevant systems and operations and could adversely affect our financial

results. We are also subject to evolving E. U. privacy laws on cookies and e- marketing. In the European Union, regulators are increasingly focusing on compliance with requirements in the online behavioral advertising ecosystem, and an E. U. regulation known as the ePrivacy Regulation will significantly increase fines for non- compliance once in effect. In the European Union, informed consent, including a prohibition on pre- checked consents and a requirement to ensure separate consents for each cookie, is required for the placement of a cookie or similar technologies on a user' s device and for direct electronic marketing. As regulators start to enforce the strict approach in recent guidance, this could lead to substantial costs, require significant systems changes, limit the effectiveness of our marketing activities, divert the attention of our technology personnel, negatively impact our efforts to understand users, adversely affect our margins, increase costs, and subject us to additional liabilities. There is a risk that as we expand, we may assume liabilities for breaches experienced by the companies we acquire. Additionally, there are potentially inconsistent world- wide government regulations pertaining to data protection and privacy. Despite our efforts to comply with applicable laws, regulations and other obligations relating to privacy, data protection, and information security, it is possible that our practices, offerings, or platform could fail, or be alleged to fail to meet applicable requirements. For instance, the overall regulatory framework governing the application of privacy laws to blockchain technology is still highly undeveloped and likely to evolve. **Further there are also changes in the regulatory landscape relating to new and evolving technologies, such as generative AI, which we have and continue to find new ways to leverage in our products and internal operations.** Our failure, or the failure by our third- party providers or partners, to comply with applicable laws or regulations and to prevent unauthorized access to, or use or release of personal data, or the perception that any of the foregoing types of failure has occurred, even if unfounded, could subject us to audits, inquiries, whistleblower complaints, adverse media coverage, investigations, severe criminal, or civil sanctions, damage our reputation, or result in fines or proceedings by governmental agencies and private claims and litigation, any of which could adversely affect our business, operating results, and financial condition. Risks Related to Third Parties Our current and future services are dependent on payment networks and acquiring processors, and any changes to their rules or practices could adversely impact our business. We rely on banks and other payment processors to process customers' payments in connection with the purchase of crypto assets on our platform and we pay these providers fees for their services. From time to time, payment networks have increased, and may increase in the future, the interchange fees and assessments that they charge for transactions that use their networks. Payment networks have imposed, and may impose in the future, special fees on the purchase of crypto assets, including on our platform, which could negatively impact us and significantly increase our costs. Our payment card processors may have the right to pass any increases in interchange fees and assessments on to us, and may impose additional use charges which would increase our operating costs and reduce our operating income. We could attempt to pass these increases along to our customers, but this strategy might result in the loss of customers to our competitors that may not pass along the increases, thereby reducing our revenue and earnings. If competitive practices prevent us from passing along the higher fees to our customers in the future, we may have to absorb all or a portion of such increases, thereby increasing our operating costs and reducing our earnings. We may also be directly or indirectly liable to the payment networks for rule violations. Payment networks set and interpret their network operating rules and have alleged from time to time that various aspects of our business model violate these operating rules. If such allegations are not resolved favorably, they may result in significant fines and penalties or require changes in our business practices that may be costly and adversely affect our business. The payment networks could adopt new operating rules or interpret or reinterpret existing rules that we or our processors might find difficult or even impossible to follow, or costly to implement. As a result, we could lose our ability to give customers the option of using cards to fund their purchases or the choice of currency in which they would like their card to be charged. If we are unable to accept cards or are limited in our ability to do so, our business would be adversely affected. We depend on major mobile operating systems and third- party platforms for the distribution of certain products. If Google Play, the Apple App Store, or other platforms prevent customers from downloading our apps, our ability to grow may be adversely affected. We rely upon third- party platforms for the distribution of certain products and services. Our Coinbase and Coinbase Wallet apps are provided as free applications through both the Apple App Store and the Google Play Store, and are also accessible via mobile and traditional websites. The Google Play Store and Apple App Store are global application distribution platforms and the main distribution channels for our apps. As such, the promotion, distribution, and operation of our apps are subject to the respective platforms' terms and policies for application developers, which are very broad and subject to frequent changes and re- interpretation. Further, these distribution platforms often contain restrictions related to crypto assets that are uncertain, broadly construed, and can limit the nature and scope of services that can be offered. For example, Apple App Store' s restrictions related to crypto assets have disrupted the proposed launch of many features within the Coinbase and Coinbase Wallet apps, including our Learning Rewards ~~(formerly " Earn ")~~ and NFT transfer services and access to decentralized applications. If our products are found to be in violation of any such terms and conditions, we may no longer be able to offer our products through such third- party platforms. There can be no guarantee that third- party platforms will continue to support our product offerings, or that customers will be able to continue to use our products. For example, in November 2013, our iOS app was temporarily removed by Apple from the Apple App Store. In December 2019, we were similarly instructed by Apple to remove certain features relating to decentralized applications from our application to comply with the Apple App Store' s policies. Any changes, bugs, technical or regulatory issues with third- party platforms, our relationships with mobile manufacturers and carriers, or changes to their terms of service or policies could degrade our products' functionalities, reduce or eliminate our ability to distribute our products, give preferential treatment to competitive products, limit our ability to deliver high quality offerings, or impose fees or other charges, any of which could affect our product usage and harm our business. Risks Related to Intellectual Property Our intellectual property rights are valuable, and any inability to protect them could adversely impact our business, operating results, and financial condition. Our business depends in large part on our proprietary technology and our brand. We rely on, and expect to continue to rely on, a combination of trademark, trade dress, domain name, copyright, and trade secrets, as well as confidentiality and license agreements with our employees,

contractors, consultants, and third parties with whom we have relationships, to establish and protect our brand and other intellectual property rights. However, our efforts to protect our intellectual property rights may not be sufficient or effective. Our proprietary technology and trade secrets could be lost through misappropriation or breach of our confidentiality and license agreements, and any of our intellectual property rights may be challenged, which could result in them being narrowed in scope or declared invalid or unenforceable. There can be no assurance that our intellectual property rights will be sufficient to protect against others offering products, services, or technologies that are substantially similar to ours and that compete with our business. We do not intend to monetize our patents or attempt to block third parties from competing with us by asserting our patents offensively, but our ability to successfully defend intellectual property challenges from competitors and other parties may depend, in part, on our ability to counter- assert our patents defensively. Effective protection of our intellectual property may be expensive and difficult to maintain, both in terms of application and registration costs as well as the costs of defending and enforcing those rights. As we have grown, we have sought to obtain and protect our intellectual property rights in an increasing number of countries, a process that can be expensive and may not always be successful. In some instances, patent applications or patents may be abandoned or allowed to lapse, resulting in partial or complete loss of patent rights in a relevant jurisdiction. Further, intellectual property protection may not be available to us in every country in which our products and services are available. For example, some foreign countries have compulsory licensing laws under which a patent owner must grant licenses to third parties. In addition, many countries limit the enforceability of patents against certain third parties, including government agencies or government contractors. In these countries, patents may provide limited or no benefit. We may also agree to license our patents to third parties as part of various patent pools and open patent projects. Those licenses may diminish our ability, though, to counter- assert our patents against certain parties that may bring claims against us. We have been, and in the future may be, sued by third parties for alleged infringement of their proprietary rights. In recent years, there has been considerable patent, copyright, trademark, domain name, trade secret and other intellectual property development activity in the cryptoeconomy, as well as litigation, based on allegations of infringement or other violations of intellectual property, including by large financial institutions. Furthermore, individuals and groups can purchase patents and other intellectual property assets for the purpose of making claims of infringement to extract settlements from companies like ours. Our use of third- party intellectual property rights also may be subject to claims of infringement or misappropriation. We cannot guarantee that our internally developed or acquired technologies and content do not or will not infringe the intellectual property rights of others. From time to time, our competitors or other third parties may claim that we are infringing upon or misappropriating their intellectual property rights, and we may be found to be infringing upon such rights. Any claims or litigation could cause us to incur significant expenses and, if successfully asserted against us, could require that we pay substantial damages or ongoing royalty payments, prevent us from offering our products or services or using certain technologies, force us to implement expensive work- arounds, or impose other unfavorable terms. We expect that the occurrence of infringement claims is likely to grow as the crypto assets market grows and matures. Accordingly, our exposure to damages resulting from infringement claims could increase and this could further exhaust our financial and management resources. Further, during the course of any litigation, we may make announcements regarding the results of hearings and motions, and other interim developments. If securities analysts and investors regard these announcements as negative, the market price of our Class A common stock may decline. Even if intellectual property claims do not result in litigation or are resolved in our favor, these claims, and the time and resources necessary to resolve them, could divert the resources of our management and require significant expenditures. Any of the foregoing could prevent us from competing effectively and could have an adverse effect on our business, operating results, and financial condition ~~. Moreover, in April 2022, we launched a beta of Coinbase NFT. Providing a peer- to- peer marketplace, at scale, that simplifies the purchasing, showcasing and discovery of NFTs involves a complex interplay of intellectual property rights; rights in underlying decentralized and proprietary technology; and contractual relationships among platforms, rights owners, and end users, all on a global basis. The rights associated with or underlying various NFTs are often poorly understood or defined, which increases the likelihood that a rights owner will bring claims against us or involve us in a dispute amongst NFT buyers and sellers. As Coinbase NFT matures, the volume of disputes will likely increase, and we may be required to devote significant resources to anticipating, responding to or even resolving claims among users. Intellectual property owners may also lobby and litigate to obtain favorable legislation or judicial decisions that would require us to play a more proactive role- and assume more liability-- for claims that we may have under existing law. All of this could lead to increasing levels of claims involving intellectual property rights~~ . Our platform contains third- party open source software components, and failure to comply with the terms of the underlying open source software licenses could harm our business. Our platform contains software modules licensed to us by third- party authors under " open source " licenses. We also make certain of our own software available to users for free under various open source licenses. Use and distribution of open source software may entail greater risks than use of third- party commercial software, as open source licensors generally do not provide support, warranties, indemnification or other contractual protections regarding infringement claims or the quality of the code. In addition, the public availability of such software may make it easier for others to compromise our platform. Some open source licenses contain requirements that we make available source code for modifications or derivative works we create based upon the type of open source software we use, or grant other licenses to our intellectual property. If we combine our proprietary software with open source software in a certain manner, we could, under certain open source licenses, be required to release the source code of our proprietary software to the public. This would allow our competitors to create similar offerings with lower development effort and time and ultimately could result in a loss of our competitive advantages. Alternatively, to avoid the public release of the affected portions of our source code, we could be required to expend substantial time and resources to re- engineer some or all of our software. We have not recently conducted an extensive audit of our use of open source software and, as a result, we cannot assure you that our processes for controlling our use of open source software in our platform are, or will be, effective. If we are held to have breached or failed to fully comply with all the terms and conditions of an open source software license, we could

face litigation, infringement or other liability, or be required to seek costly licenses from third parties to continue providing our offerings on terms that are not economically feasible, to re- engineer our platform, to discontinue or delay the provision of our offerings if re- engineering could not be accomplished on a timely basis or to make generally available, in source code form, our proprietary code, any of which could adversely affect our business, operating results, and financial condition. Moreover, the terms of many open source licenses have not been interpreted by U. S. or foreign courts. As a result, there is a risk that these licenses could be construed in a way that could impose unanticipated conditions or restrictions on our ability to provide or distribute our platform. From time to time, there have been claims challenging the ownership of open source software against companies that incorporate open source software into their solutions. As a result, we could be subject to lawsuits by parties claiming ownership of what we believe to be open source software. Risks Related to Our Employees and Other Service Providers The loss of one or more of our key personnel, or our failure to attract and retain other highly qualified personnel in the future, could adversely impact our business, operating results, and financial condition. We operate in a relatively new industry that is not widely understood and requires highly skilled and technical personnel. We believe that our future success is highly dependent on the talents and contributions of our senior management team, including Mr. Armstrong, our co- founder and Chief Executive Officer, members of our executive team, and other key employees across product, engineering, risk management, finance, compliance and legal, and marketing. Our future success depends on our ability to attract, develop, motivate, and retain highly qualified and skilled employees. Due to the nascent nature of the cryptoeconomy, the pool of qualified talent is extremely limited, particularly with respect to executive talent, engineering, risk management, and financial regulatory expertise. We face intense competition for qualified individuals from numerous software and other technology companies. To attract and retain key personnel, we incur significant costs, including salaries and benefits and equity incentives. Even so, these measures may not be enough to attract and retain the personnel we require to operate our business effectively. The loss of even a few key employees or senior leaders, or an inability to attract, retain and motivate additional highly skilled employees required for the planned expansion of our business could adversely impact our operating results and impair our ability to grow. Our culture emphasizes innovation, and if we cannot maintain this culture, our business and operating results could be adversely impacted. We believe that our entrepreneurial and innovative corporate culture has been a key contributor to our success. We encourage and empower our employees to develop and launch new and innovative products and services, which we believe is essential to attracting high quality talent, partners, and developers, as well as serving the best, long- term interests of our company. If we cannot maintain this culture, we could lose the innovation, creativity and teamwork that has been integral to our business. Additionally, from time to time, we realign our resources and talent to implement stage- appropriate business strategies, including furloughs, layoffs, or reductions in force. In such cases, we may find it difficult to prevent a negative effect on employee morale or attrition beyond our planned reduction, in which case our products and services may suffer and our business, operating results, and financial condition could be adversely impacted. In the event of employee or service provider misconduct or error, our business may be adversely impacted. Employee or service provider misconduct or error could subject us to legal liability, financial losses, and regulatory sanctions and could seriously harm our reputation and negatively affect our business. Such misconduct could include engaging in improper or unauthorized transactions or activities, misappropriation of customer funds, insider trading and misappropriation of information, failing to supervise other employees or service providers, improperly using confidential information, as well as improper trading activity such as spoofing, layering, wash trading, manipulation and front- running. Employee or service provider errors, including mistakes in executing, recording, or processing transactions for customers, could expose us to the risk of material losses even if the errors are detected. Although we have implemented processes and procedures and provide trainings to our employees and service providers to reduce the likelihood of misconduct and error, these efforts may not be successful. Moreover, the risk of employee or service provider error or misconduct may be even greater for novel products and services and is compounded by the fact that many of our employees and service providers are accustomed to working at tech companies which generally do not maintain the same compliance customs and rules as financial services firms. This can lead to high risk of confusion among employees and service providers with respect to compliance obligations, particularly including confidentiality, data access, trading, and conflicts. It is not always possible to deter misconduct, and the precautions we take to prevent and detect this activity may not be effective in all cases. If we were found to have not met our regulatory oversight and compliance and other obligations, we could be subject to regulatory sanctions, financial penalties, restrictions on our activities for failure to properly identify, monitor and respond to potentially problematic activity and seriously damage our reputation. Our employees, contractors, and agents could also commit errors that subject us to financial claims for negligence, as well as regulatory actions, or result in financial liability. Further, allegations by regulatory or criminal authorities of improper trading activities could affect our brand and reputation. Our officers, directors, employees, and large stockholders may encounter potential conflicts of interests with respect to their positions or interests in certain crypto assets, entities, and other initiatives, which could adversely affect our business and reputation. We frequently engage in a wide variety of transactions and maintain relationships with a significant number of crypto projects, their developers, members of their ecosystem, and investors. These transactions and relationships could create potential conflicts of interests in management decisions that we make. For instance, certain of our officers, directors, and employees are active investors in crypto projects themselves, and may make investment decisions that favor projects that they have personally invested in. Many of our large stockholders also make investments in these crypto projects. In addition, our co- founder and Chief Executive Officer, Mr. Armstrong, is involved in a number of initiatives related to the cryptoeconomy and more broadly. For example, Mr. Armstrong currently serves as the chief executive officer of ResearchHub Technologies, Inc., a scientific research development platform. This and other initiatives he is involved in could divert Mr. Armstrong' s time and attention from overseeing our business operations which could have a negative impact on our business. Moreover, we may in the future be subject to litigation as a result of his involvement with these other initiatives. Similarly, certain of our directors, officers, employees, and large stockholders may hold crypto assets that we are considering supporting for trading on our platform, and may be more supportive

of such listing notwithstanding legal, regulatory, and other issues associated with such crypto assets. While we have instituted policies and procedures to limit and mitigate such risks, there is no assurance that such policies and procedures will be effective, or that we will be able to manage such conflicts of interests adequately. If we fail to manage these conflicts of interests, or we receive unfavorable media coverage with respect to actual or perceived conflicts of interest, our business may be harmed and the brand, reputation and credibility of our company may be adversely affected. General Risk Factors Adverse economic conditions may adversely affect our business. Our performance is subject to general economic conditions, and their impact on the crypto asset markets and our customers. The United States and other key international economies have experienced cyclical downturns from time to time in which economic activity declined resulting in lower consumption rates, restricted credit, reduced profitability, weaknesses in financial markets, bankruptcies, and overall uncertainty with respect to the economy. Adverse general economic conditions have impacted the cryptoeconomy, although the extent of which remains uncertain and dependent on a variety of factors, including market adoption of crypto assets, global trends in the cryptoeconomy, central bank monetary policies, **instability in the global banking system** and other events beyond our control. Geopolitical developments, such as trade wars and foreign exchange limitations can also increase the severity and levels of unpredictability globally and increase the volatility of global financial and crypto asset markets. For example, the capital and credit markets have experienced extreme volatility and disruptions, resulting in steep declines in the value of crypto assets. To the extent general economic conditions and crypto assets markets materially deteriorate or the current decline continues for a prolonged period, our ability to generate revenue and to attract and retain customers could suffer and our business, operating results and financial condition could be adversely affected. Moreover, even if general economic conditions improve, there is no guarantee that the cryptoeconomy will similarly improve. Further, in 2022, a number of blockchain protocols and crypto financial firms, and in particular protocols and firms involving high levels of financial leverage such as high- yield lending products or derivatives trading, suffered from insolvency and liquidity crises leading to the 2022 Events. Some of the 2022 Events are alleged **or have been held** to be the result of fraudulent activity by insiders, including misappropriation of customer funds and other illicit activity and internal controls failures. ~~To the extent~~ **In connection with** ~~there~~ **the 2022** ~~is additional economic impact of these events~~ **Events** ~~, which remains unknown and difficult to predict~~, concerns **were** ~~have been~~ raised about the potential for a market condition where the failure of one company leads to the financial distress of other companies **, which has the potential to** ~~. Forced selling by distressed companies may also~~ depress the prices of assets used as collateral by other firms. If ~~this~~ **such a** market condition **were to** ~~becomes~~ **become** widespread in the cryptoeconomy, ~~including as a result of the 2022 Events,~~ we ~~may~~ **could** suffer from increased counterparty risk, including defaults or bankruptcies of major customers or counterparties, which could lead to significantly reduced activity on our platform and fewer available crypto market opportunities in general. Further, forced selling of crypto assets by distressed companies could lead to lower crypto asset prices and **may lead to** a ~~consequent~~ reduction in our revenue. To the extent that conditions in the general economic and crypto ~~assets~~ **asset** markets **were to** materially deteriorate, our ability to attract and retain customers may suffer **. Actual events involving limited liquidity, defaults, non- performance or other adverse developments that affect financial institutions, transactional counterparties or other companies in the financial services industry, or the financial services industry generally, or concerns or rumors about any such events or other similar risks, have in the past and may in the future lead to market- wide liquidity problems. For example, in March 2023, Silvergate Capital Corp. announced it would wind down operations and liquidate Silvergate Bank. Soon after, the FDIC was appointed receiver of Silicon Valley Bank and Signature Bank. In connection with these issues and issues with other financial institutions, the prices of fiat- backed stablecoins, including USDC, were temporarily impacted and may be similarly impacted again in the future. Further, if the instability in the global banking system continues or worsens, there could be additional negative ramifications, such as additional all market- wide liquidity problems or impacted access to deposits and investments for customers of affected banks and certain banking partners, and our business, operating results and financial condition could be adversely affected** . We are a remote- first company which subjects us to heightened operational risks. Our employees and service providers work from home and we are a remote- first company. This subjects us to heightened operational risks. For example, technologies in our employees' and service providers' homes may not be as robust as in our offices and could cause the networks, information systems, applications, and other tools available to employees and service providers to be more limited or less reliable than in our offices. Further, the security systems in place at our employees' and service providers' homes may be less secure than those used in our offices, and while we have implemented technical and administrative safeguards to help protect our systems as our employees and service providers work from home, we may be subject to increased cybersecurity risk, which could expose us to risks of data or financial loss, and could disrupt our business operations. There is no guarantee that the data security and privacy safeguards we have put in place will be completely effective or that we will not encounter risks associated with employees and service providers accessing company data and systems remotely. We also face challenges due to the need to operate with the remote workforce and are addressing those challenges to minimize the impact on our ability to operate. Being a remote- first company may make it more difficult for us to preserve our corporate culture and our employees may have decreased opportunities to collaborate in meaningful ways. Further, we cannot guarantee that being a remote- first company will not have a negative impact on employee morale and productivity. Any failure to preserve our corporate culture and foster collaboration could harm our future success, including our ability to retain and recruit personnel, innovate and operate effectively, and execute on our business strategy. ~~Health epidemics, including the COVID- 19 pandemic, have had or could have an adverse effect on our business, operations, and the markets in which we operate. The ongoing COVID- 19 pandemic, including the resurgence of cases related to the spread of new variants, and the imposition of related public health measures have resulted in increased volatility and uncertainty in the cryptoeconomy. Moreover, we rely on third party service providers to perform certain functions and any disruptions to a service providers' business operations resulting from business restrictions, quarantines, or restrictions on the ability of personnel to perform their jobs could have an adverse impact on our service providers' ability to provide~~

~~services to us. The ongoing COVID- 19 pandemic and the related public health measures could adversely impact our strategic business plans and growth strategy, reduce demand for our products and services, reduce the availability and productivity of our employees, service providers, and third- party resources, cause us to experience an increase in costs due to emergency measures, and otherwise adversely impact our business. We are currently unable to accurately predict the full impact that the COVID- 19 pandemic will have on our business, operations, and the markets in which we operate due to numerous uncertainties, including variants of the COVID- 19 virus, any further resurgences, the extent and effectiveness of containment actions and other public health measures, the distribution and public acceptance of vaccines and treatments, and the impact of these and other factors on our employees and the users of our platform. The COVID- 19 pandemic, as well as any subsequent recovery period, may also have the effect of heightening many of the other risks described in this " Risk Factors " section. Investors' expectations of our performance relating to environmental~~ **Environmental** , social and governance factors may impose additional costs and expose us to new risks. There is an increasing focus from certain investors, **regulators,** employees, users and other stakeholders concerning corporate responsibility, specifically related to environmental, social and governance matters ~~, or~~ **(“** ESG **”)** . Some investors may use these non- financial performance factors to guide their investment strategies and, in some cases, may choose not to invest in us if they believe our policies and actions relating to corporate responsibility are inadequate. The growing investor demand for measurement of non- financial performance is addressed by third- party providers of sustainability assessment and ratings on companies. The criteria by which our corporate responsibility practices are assessed may change due to the constant evolution of the sustainability landscape, which could result in greater expectations of us and cause us to undertake costly initiatives to satisfy such new criteria. If we elect not to or are unable to satisfy such new criteria, investors may conclude that our policies and actions with respect to corporate social responsibility are inadequate. We may face reputational damage in the event that we do not meet the ESG standards set by various constituencies. Furthermore, if our competitors' corporate social responsibility performance is perceived to be better than ours, potential or current investors may elect to invest with our competitors instead. In addition, in the event that we communicate certain initiatives and goals regarding environmental, social and governance matters, we could fail, or be perceived to fail, in our achievement of such initiatives or goals, or we could be criticized for the scope of such initiatives or goals. If we fail to satisfy the expectations of investors, employees and other stakeholders or our initiatives are not executed as planned, our reputation and business, operating results and financial condition could be adversely impacted ~~. For example, in order to advance our mission, in February 2022 we launched our Coinbase Innovation Political Action Committee to support crypto- forward political candidates and initiatives. However, our political activities to further our mission may not be successful or may be perceived unfavorably by investors and the public and have an adverse impact on our brand and reputation. Our management team has limited experience managing a public company. Our management team has limited experience managing a publicly traded company, interacting with public company investors, and complying with the increasingly complex laws pertaining to public companies. Our management team may not successfully or efficiently manage our transition to being a public company subject to significant regulatory oversight and reporting obligations under the federal securities laws and the continuous scrutiny of securities analysts and investors. These new obligations and constituents will require significant attention from our senior management and could divert their attention away from the day- to- day management of our business, which could adversely affect our business, operating results, and financial condition~~ . Changes in U. S. and foreign tax laws, as well as the application of such laws, could adversely impact our financial position and operating results. We are subject to complex tax laws and regulations in the United States and a variety of foreign jurisdictions. All of these jurisdictions have in the past and may in the future make changes to their corporate income tax rates and other income tax laws which could increase our future income tax provision. For example, our future income tax obligations could be adversely affected by earnings that are lower than anticipated in jurisdictions where we have lower statutory rates and by earnings that are higher than anticipated in jurisdictions where we have higher statutory rates, by changes in the valuation of our deferred tax assets and liabilities, by changes in the amount of unrecognized tax benefits, or by changes in tax laws, regulations, accounting principles, or interpretations thereof, including changes with possible retroactive application or effect. Our determination of our tax liability is subject to review and may be challenged by applicable U. S. and foreign tax authorities. Any adverse outcome of such a challenge could harm our operating results and financial condition. The determination of our worldwide provision for income taxes and other tax liabilities requires significant judgment and, in the ordinary course of business, there are many transactions and calculations where the ultimate tax determination is complex and uncertain. Moreover, as a multinational business, we have subsidiaries that engage in many intercompany transactions in a variety of tax jurisdictions where the ultimate tax determination is complex and uncertain. Our existing corporate structure and intercompany arrangements have been implemented in a manner we believe is in compliance with current prevailing tax laws. Furthermore, as we operate in multiple taxing jurisdictions, the application of tax laws can be subject to diverging and sometimes conflicting interpretations by tax authorities of these jurisdictions. It is not uncommon for taxing authorities in different countries to have conflicting views with respect to, among other things, the characterization and source of income or other tax items, the manner in which the arm' s- length standard is applied for transfer pricing purposes, or with respect to the valuation of intellectual property. The taxing authorities of the jurisdictions in which we operate may challenge our tax treatment of certain items or the methodologies we use for valuing developed technology or intercompany arrangements, which could impact our worldwide effective tax rate and harm our financial position and operating results. Further, any changes in the tax laws governing our activities may increase our tax expense, the amount of taxes we pay, or both. For example, the Tax Cuts and Jobs Act (the " TCJA "), enacted on December 22, 2017, significantly reformed the U. S. federal tax code, reducing the U. S. federal corporate income tax rate, making sweeping changes to the rules governing international business operations, and imposing new limitations on a number of tax benefits, including deductions for business interest and the use of net operating loss carryforwards. **Effective beginning in 2022, the TCJA also eliminated the option to immediately deduct research and development expenditures and required taxpayers to amortize domestic expenditures over five years and foreign**

expenditures over fifteen years. The Inflation Reduction Act of 2022 (the " Inflation Reduction Act "), enacted on August 16, 2022, further amended the U. S. federal tax code, imposing a 15 % minimum tax on " adjusted financial statement income " of certain corporations as well as an excise tax on the repurchase or redemption of stock by certain corporations, beginning in the 2023 tax year **. In addition, over the last several years, the Organization for Economic Cooperation and Development has been working on a Base Erosion and Profit Shifting Project that, if implemented, would change various aspects of the existing framework under which our tax obligations are determined in many of the countries in which we do business. As of July 2023, nearly 140 countries have approved a framework that imposes a minimum tax rate of 15 %, among other provisions. As this framework is subject to further negotiation and implementation by each member country, the timing and ultimate impact of any such changes on our tax obligations are uncertain** . There can be no assurance that future tax law changes will not increase the rate of the corporate income tax, impose new limitations on deductions, credits or other tax benefits, or make other changes that may adversely affect our business, cash flows or financial performance. In addition, the IRS has yet to issue guidance on a number of important issues regarding the tax treatment of cryptocurrency and the products we provide to our customers and from which we derive our income. In the absence of such guidance, we will take positions with respect to any such unsettled issues. There is no assurance that the IRS or a court will agree with the positions taken by us, in which case tax penalties and interest may be imposed that could adversely affect our business, cash flows or financial performance. We also are subject to non- income taxes, such as payroll, sales, use, value- added, digital services, net worth, property, and goods and services taxes in the United States and various foreign jurisdictions. Specifically, we may be subject to new allocations of tax as a result of increasing efforts by certain jurisdictions to tax activities that may not have been subject to tax under existing tax principles. Companies such as ours may be adversely impacted by such taxes. Tax authorities may disagree with certain positions we have taken. As a result, we may have exposure to additional tax liabilities that could have an adverse effect on our operating results and financial condition. As a result of these and other factors, the ultimate amount of tax obligations owed may differ from the amounts recorded in our financial statements and any such difference may harm our operating results in future periods in which we change our estimates of our tax obligations or in which the ultimate tax outcome is determined. Our ability to use our deferred tax assets may be subject to certain limitations under U. S. or foreign law. Realization of our deferred tax assets, in the form of future domestic or foreign tax deductions **, credits** ~~from the amortization~~ or other **tax benefits** ~~recovery of capitalized expenses~~ , will depend on future taxable income, and there is a risk that some or all of such tax assets could be subject to limitation or otherwise unavailable to offset future income tax liabilities, all of which could adversely affect our operating results. For example, future changes in our stock ownership, the causes of which may be outside of our control, could result in an ownership change under Section 382 of the Internal Revenue Code of 1986, as amended (the " Code "), which could limit our use of such tax assets in certain circumstances. Similarly, additional changes may be made to U. S. (federal and state) and foreign tax laws which could further limit our ability to fully utilize these tax assets against future taxable income. Under the ~~recently passed~~ Inflation Reduction Act, our ability to utilize tax deductions or losses from prior years may be limited by the imposition of the 15 % minimum tax if, in future years, such minimum tax applies to us. Therefore, we may be required to pay **additional** U. S. federal income taxes in future years despite any **available** future tax deductions ~~or~~ **,** U. S. federal net operating loss (" NOL ") carryforwards **, credits or other tax benefits** that we accumulate. Fluctuations in currency exchange rates could harm our operating results and financial condition. Revenue generated and expenses incurred from our international operations are often denominated in the currencies of the local countries. Accordingly, changes in the value of foreign currencies relative to the U. S. dollar can affect our revenue and operating results reflected in our U. S. dollar- denominated financial statements. Our financial results are also subject to changes in exchange rates that impact the settlement of transactions in non- functional currencies. As a result, it could be more difficult to detect underlying trends in our business and operating results. To the extent that fluctuations in currency exchange rates cause our operating results to differ from expectations of investors, the market price of our Class A common stock could be adversely impacted. From time to time, we may engage in currency hedging activities to limit the risk of foreign currency exchange **rate** fluctuations. To the extent we use hedging instruments to hedge exposure to fluctuations in foreign currency exchange rates, the use of such hedging instruments may not offset any or more than a portion of the adverse financial effects of unfavorable movements in foreign exchange rates over the limited time the hedges are in place, and may introduce additional risks if we are unable to structure effective hedges with such instruments. If our estimates or judgment relating to our critical accounting ~~policies~~ **estimates** prove to be incorrect, our operating results could be adversely affected. The preparation of financial statements in conformity with generally accepted accounting principles (" GAAP ") requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as provided in the section titled " Management' s Discussion and Analysis of Financial Condition and Results of Operations ~~-~~ — Critical Accounting ~~Policies and~~ Estimates " in Part II, Item ~~8~~ **7** of this Annual Report on Form 10- K. The results of these estimates form the basis for making judgments about the carrying values of assets, liabilities, and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant estimates and judgments **that comprise our critical accounting estimates** involve the ~~identification~~ **valuation** of ~~performance~~ **assets acquired and liabilities assumed in business** ~~obligations~~ **combinations** ~~in revenue recognition~~ **, valuation of strategic investments** , evaluation of tax positions, **and** ~~inter- company transactions, valuation~~ **evaluation** of **legal** ~~assets acquired~~ and ~~liabilities assumed in business combinations, and the valuation of stock- based awards and crypto assets we hold, among others~~ **other contingencies** . Our operating results may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our operating results to fall below the expectations of analysts and investors, resulting in a decline in the trading price of our Class A common stock. We may be adversely affected by natural disasters, pandemics, and other catastrophic events, and by man- made problems such as terrorism, that could disrupt our business operations, and our business continuity and disaster recovery plans may not

adequately protect us from a serious disaster. Natural disasters or other catastrophic events may also cause damage or disruption to our operations, international commerce, and the global economy, and could have an adverse effect on our business, operating results, and financial condition. Our business operations are subject to interruption by natural disasters, fire, power shortages, and other events beyond our control. In addition, our global operations expose us to risks associated with public health crises, such as pandemics and epidemics, which could harm our business and cause our operating results to suffer. For example, the ~~ongoing effects of the~~ COVID- 19 pandemic and the **related** precautionary measures that we ~~have~~ adopted have **in the past** resulted, and could ~~continue to~~ **in the future** result, in difficulties or changes to our customer support, or create operational or other challenges, any of which could adversely impact our business and operating results. Further, acts of terrorism, labor activism or unrest, and other geopolitical unrest, including ~~the~~ ongoing **regional** ~~conflict~~ **conflicts** ~~in Ukraine~~ **around the world** , could cause disruptions in our business or the businesses of our partners or the economy as a whole. In the event of a natural disaster, including a major earthquake, blizzard, or hurricane, or a catastrophic event such as a fire, power loss, or telecommunications failure, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in development of our platform, lengthy interruptions in service, breaches of data security, and loss of critical data, all of which could have an adverse effect on our future operating results. We do not maintain insurance sufficient to compensate us for the potentially significant losses that could result from disruptions to our services. Additionally, all the aforementioned risks may be further increased if we do not implement a disaster recovery plan or our partners' disaster recovery plans prove to be inadequate. To the extent natural disasters or other catastrophic events concurrently impact data centers we rely on in connection with private key restoration, customers will experience significant delays in withdrawing funds, or in the extreme we may suffer loss of customer funds. The requirements of being a public company, including maintaining adequate internal control over our financial and management systems, may strain our resources, divert management' s attention, and affect our ability to attract and retain executive management and qualified board members. As a public company we incur significant legal, accounting, and other expenses. We are subject to reporting requirements of the Exchange Act, the Sarbanes- Oxley Act of 2002, the rules subsequently implemented by the SEC, the rules and regulations of the listing standards of The Nasdaq Stock Market LLC (" Nasdaq ") and other applicable securities rules and regulations. Stockholder activism, the current political and social environment and the current high level of government intervention and regulatory reform may lead to substantial new regulations and disclosure obligations, which will likely result in additional compliance costs and could impact the manner in which we operate our business in ways we cannot currently anticipate. Compliance with these rules and regulations may strain our financial and management systems, internal controls, and employees. The Exchange Act requires, among other things, that we file annual, quarterly, and current reports with respect to our business and operating results. Moreover, the Sarbanes- Oxley Act of 2002 requires, among other things, that we maintain effective disclosure controls and procedures, and internal control over financial reporting. In order to maintain and, if required, improve our disclosure controls and procedures, and internal control over financial reporting to meet this standard, significant resources and management oversight may be required. If we encounter material weaknesses or deficiencies in our internal control over financial reporting, we may not detect errors on a timely basis and our consolidated financial statements may be materially misstated. Effective internal control is necessary for us to produce reliable financial reports and is important to prevent fraud. We have incurred and expect to continue to incur significant expenses and devote substantial management effort toward ensuring compliance with the annual auditor attestation requirements of Section 404 of the Sarbanes- Oxley Act of 2002. As a result of the complexity involved in complying with the rules and regulations applicable to public companies, our management' s attention may be diverted from other business concerns, which could harm our business, operating results, and financial condition. Although we have already hired additional employees to assist us in complying with these requirements, our finance team is small and we may need to hire more employees in the future, or engage outside consultants, which will increase our operating expenses. We might require additional capital to support business growth, and this capital might not be available. We have funded our operations since inception primarily through debt, equity financings and revenue generated by our products and services. We cannot be certain when or if our operations will generate sufficient cash to fully fund our ongoing operations or the growth of our business. We intend to continue to make investments in our business ~~to respond to business challenges~~ , including developing new products and services, enhancing our operating infrastructure, expanding our international operations, and acquiring complementary businesses and technologies, all of which may require us to secure additional funds. Additional financing may not be available on terms favorable to us, if at all, including due to general macroeconomic conditions, crypto market conditions ~~,~~ **and any disruptions in** the ~~2022 Events~~ **crypto market, instability in the global banking system, increasing regulatory uncertainty and scrutiny** or other unforeseen factors. In the event of a downgrade of our credit rating, our ability to raise additional financing may be adversely affected and any future debt offerings or credit arrangements we propose to enter into may be on less favorable terms or terms that may not be acceptable to us. In addition, even if debt financing is available, the cost of additional financing may be significantly higher than our current debt. If we incur additional debt, the debt holders would have rights senior to holders of our common stock to make claims on our assets, and the terms of any debt could restrict our operations, including our ability to pay dividends on our common stock. Furthermore, we have authorized the issuance of " blank check " preferred stock and common stock that our board of directors could use to, among other things, issue shares of our capital stock in the form of blockchain tokens, implement a stockholder rights plan, or issue other shares of preferred stock or common stock. We may issue shares of capital stock, including in the form of blockchain tokens, to our customers in connection with customer reward or loyalty programs. If we issue additional equity securities, including in the form of blockchain tokens, stockholders will experience dilution, and the new equity securities could have rights senior to those of our currently authorized and issued common stock. The trading prices for our common stock may be highly volatile, which may reduce our ability to access capital on favorable terms or at all. In addition, a slowdown or other sustained adverse downturn in the general economic or crypto asset markets could adversely affect our business and the value of our Class A common stock. Because our decision to raise capital in the

future will depend on numerous considerations, including factors beyond our control, we cannot predict or estimate the amount, timing, or nature of any future issuances of securities. As a result, our stockholders bear the risk of future issuances of debt or equity securities reducing the value of our Class A common stock and diluting their interests. Our inability to obtain adequate financing or financing on terms satisfactory to us, when we require it, could significantly limit our ability to continue supporting our business growth and responding to business challenges. Risks Related to Ownership of Our Class A Common Stock The market price of our Class A common stock may be volatile, and could decline significantly and rapidly. Market volatility may affect the value of an investment in our Class A common stock and could subject us to litigation. Prior to the listing of our Class A common stock on Nasdaq, there was no public market for shares of our Class A common stock. Technology stocks have historically experienced high levels of volatility. The market price of our Class A common stock also could be subject to wide fluctuations in response to the risk factors described in this Annual Report on Form 10- K and others beyond our control, including: • the number of shares of our Class A common stock publicly owned and available for trading; • overall performance of the equity markets or publicly- listed financial services and technology companies; • our actual or anticipated operating performance and the operating performance of our competitors; • changes in the projected operational and financial results we provide to the public or our failure to meet those projections; • failure of securities analysts to initiate or maintain coverage of us, changes in financial estimates by any securities analysts who follow our company, or our failure to meet the estimates or the expectations of investors; • any major change in our board of directors, management, or key personnel; • if we issue additional shares of capital stock, including in the form of blockchain tokens, in connection with customer reward or loyalty programs; • issuance of shares of our Class A common stock, whether in connection with an acquisition or upon conversion of some or all of our outstanding 2026 Convertible Notes; • the highly volatile nature of the cryptoeconomy and the prices of crypto assets; • rumors and market speculation involving the cryptoeconomy or us or other companies in our industry; • announcements by us or our competitors of significant innovations, new products, services, features, integrations or capabilities, acquisitions, strategic investments, partnerships, joint ventures, or capital commitments; and • other events or factors, including those resulting from ~~COVID- 19,~~ political instability and acts of war or terrorism, **regional conflicts around the world, government shutdowns, bank failures** or responses to these events ~~, including the current conflict in Ukraine~~ . Furthermore, the stock market has recently experienced extreme price and volume fluctuations that have affected and continue to affect the market prices of equity securities of many companies and financial services and technology companies in particular. These fluctuations often have been unrelated or disproportionate to the operating performance of those companies. These broad market and industry fluctuations, as well as general macroeconomic, political and market conditions such as recessions, interest rate changes, or international currency fluctuations, may negatively impact the market price of our Class A common stock. In the past, companies that have experienced volatility in the market price of their stock have been subject to securities class action litigation. We are currently subject to stockholder litigation **and in June 2023 the SEC filed the June 2023 SEC Complaint,** as described in the section titled " Legal Proceedings " in Part I, Item 3 of this Annual Report on Form 10- K, and may continue to be the target of ~~this~~ **these** ~~type~~ **types** of ~~litigation~~ **actions or additional regulatory uncertainty and scrutiny** in the future. Securities ~~litigation~~ **or regulatory actions** against us could result in substantial costs and divert our management' s attention from other business concerns, which could harm our business. The dual class structure of our common stock has the effect of concentrating voting control with those stockholders, including our directors, executive officers, and 5 % stockholders, and their respective affiliates. As a result of this structure, our Chief Executive Officer has control over key decision making as a result of his control of a majority of our voting stock. This ownership will limit or preclude your ability to influence corporate matters, including the election of directors, amendments of our organizational documents, and any merger, consolidation, sale of all or substantially all of our assets, or other major corporate transaction requiring stockholder approval. Our Class B common stock has twenty votes per share, and our Class A common stock has one vote per share. Mr. Armstrong is currently able to exercise voting rights with respect to a majority of the voting power of our outstanding capital stock and, along with our directors, other executive officers, and 5 % stockholders, and their affiliates, these stockholders hold in the aggregate a substantial majority of the voting power of our capital stock. Because of the twenty- to- one voting ratio between our Class B common stock and our Class A common stock, the holders of our Class B common stock, including Mr. Armstrong, collectively are expected to continue to control a significant percentage of the combined voting power of our common stock and therefore be able to control all matters submitted to our stockholders for approval until the earliest to occur of (i) the date fixed by the board of directors that is no less than 61 days and no more than 180 days after the date that the aggregate number of shares of Class B common stock held by Brian Armstrong and his affiliates is less than 25 % of the aggregate number of shares of Class B common stock held by Mr. Armstrong and his affiliates on April 1, 2021, the date of effectiveness of the registration statement on Form S- 1 for the listing of our Class A common stock on Nasdaq; (ii) the date and time specified by affirmative vote of the holders of at least 66- 2 / 3 % of the outstanding shares of Class B common stock, voting as a single class, and the affirmative vote of at least 66- 2 / 3 % of the then serving members of our board of directors, which must include the affirmative vote of Mr. Armstrong, if either (A) Mr. Armstrong is serving on our board of directors and has not been terminated for cause or resigned except for good reason (as each term is defined in our restated certificate of incorporation) from his position as our Chief Executive Officer or (B) Mr. Armstrong has not been removed for cause or resigned from the position of Chairman of the board of directors; and (iii) the death or disability (as defined in our restated certificate of incorporation) of Mr. Armstrong, when all outstanding shares of Class B common stock will convert automatically into shares of Class A common stock. Holders of our Class A common stock are not entitled to vote separately as a single class except under certain limited circumstances. This concentrated control may limit or preclude your ability to influence corporate matters for the foreseeable future, including the election of directors, amendments of our organizational documents, and any merger, consolidation, sale of all or substantially all of our assets, or other major corporate transaction requiring stockholder approval. In addition, this may prevent or discourage unsolicited acquisition proposals or offers for our capital stock that you may believe are in your best interest as one of our stockholders. In

addition, Mr. Armstrong has the ability to control the management and major strategic investments of our company as a result of his position as our Chief Executive Officer and his ability to control the election or replacement of our directors. As a board member and officer, Mr. Armstrong owes a fiduciary duty to our stockholders and must act in good faith in a manner he reasonably believes to be in the best interests of our stockholders. As a stockholder, even a controlling stockholder, Mr. Armstrong is entitled to vote his shares, and shares over which he has voting control, in his own interests, which may not always be in the interests of our stockholders generally. Future transfers by holders of Class B common stock will generally result in those shares converting to Class A common stock, subject to limited exceptions, such as certain transfers effected for estate planning purposes. The conversion of Class B common stock to Class A common stock will have the effect, over time, of increasing the relative voting power of those holders of Class B common stock, including Mr. Armstrong, who retain their shares in the long term. Moreover, it is possible that one or more of the persons or entities holding our Class B common stock could gain significant voting control as other holders of Class B common stock sell or otherwise convert their shares into Class A common stock. The dual class structure of our common stock may adversely affect the trading market for our Class A common stock. Certain stock index providers ~~, such as S & P Dow Jones,~~ exclude companies with multiple classes of shares of common stock from being added to certain stock indices ~~, including the S & P 500~~. In addition, several stockholder advisory firms and large institutional investors oppose the use of multiple class structures. As a result, the dual class structure of our common stock may prevent the inclusion of our Class A common stock in such indices, may cause stockholder advisory firms to publish negative commentary about our corporate governance practices or otherwise seek to cause us to change our capital structure, and may result in large institutional investors not purchasing shares of our Class A common stock. Any exclusion from stock indices could result in less demand for our Class A common stock. Any actions or publications by stockholder advisory firms or institutional investors critical of our corporate governance practices or capital structure could also adversely affect the value of our Class A common stock. Sales or distribution of substantial amounts of our Class A common stock, or the perception that such sales or distributions might occur, could cause the market price of our Class A common stock to decline. The sale or distribution of a substantial number of shares of our Class A common stock, particularly sales by us or our directors, executive officers, and principal stockholders, or the perception that these sales or distributions might occur in large quantities, could cause the market price of our Class A common stock to decline. **In addition** ~~As of December 31~~, ~~2022,~~ we **have filed a registration statement to register shares reserved for future** ~~had 31, 794, 551 options outstanding that, if fully exercised, would result in the~~ issuance **under** ~~of 4, 501, 924 shares of Class B common stock and the issuance of 27, 292, 627 shares of Class A common stock and 5, 328, 671 shares of Class A common stock outstanding subject to restricted stock units, or~~ **our** ~~RSUs~~ **equity compensation plans**. All of the shares of Class A common stock and Class B common stock issuable upon the exercise of stock options or vesting and settlement of ~~RSUs,~~ **restricted stock units** and **performance restricted stock units** ~~reserved for future issuance under our equity incentive plans, have been registered for public resale under the Securities Act of 1933, as amended (the " Securities Act "). Accordingly, these shares~~ will be able to be freely sold in the public market upon issuance, subject to applicable vesting requirements and compliance by affiliates with Rule 144 under the Securities Act. **Further** ~~In addition~~, certain holders of shares of our common stock will have rights, subject to some conditions, to require us to file registration statements for the public resale of shares of Class A common stock or to include such shares in registration statements that we may file for us or other stockholders. Any registration statement we file to register additional shares, whether as a result of registration rights or otherwise, could cause the market price of our Class A common stock to decline or be volatile. We also may issue our capital stock or securities convertible into our capital stock, including in the form of blockchain tokens, from time to time in connection with a financing, an acquisition, investments, pursuant to customer rewards, loyalty programs, and other incentive plans, or otherwise. Any such issuance could result in substantial dilution to our existing stockholders and cause the market price of our Class A common stock to decline. If securities or industry analysts do not publish or cease publishing research, or publish inaccurate or unfavorable research, about our business, the price of our Class A common stock and its liquidity could decline. The trading market for our Class A common stock may be influenced by the research and reports that securities or industry analysts publish about us or our business, our market, and our competitors. We do not have any control over these analysts. If securities and industry analysts cease coverage of us altogether, the market price for our Class A common stock may be negatively affected. If one or more of the analysts who cover us downgrade our Class A common stock, or publish inaccurate or unfavorable research about our business, the price of our Class A common stock may decline. If one or more of these analysts cease coverage of us or fail to publish reports on us regularly, demand for our Class A common stock could decrease, which might cause our Class A common stock price and trading volume to decline. In light of the unpredictability inherent in our business, our financial outlook commentary may differ from analysts' expectations, which could cause volatility to the price of our Class A common stock. We are not obligated to, and do not intend to pay dividends on any class of our common stock for the foreseeable future. We have never declared or paid any cash dividends on any class of our common stock, are not obligated to pay, and do not intend to pay any cash dividends in the foreseeable future. We anticipate that for the foreseeable future we will retain all of our future earnings for use in the development of our business and for general corporate purposes. Any determination to pay dividends in the future will be at the discretion of our board of directors. Our payment of any dividends will be subject to contractual and legal restrictions and other factors that our board of directors deems relevant. Moreover, agreements governing any future indebtedness of ours may further limit our ability to pay dividends. In addition, our ability to pay dividends is limited by law. There is no assurance that we will be able or that our board of directors will decide to declare any dividends on any class of our common stock. Accordingly, investors may have to rely on sales of their Class A common stock after price appreciation, which may never occur, as the only way to realize any future gains on their investment. Provisions in our charter documents and under Delaware law, and certain rules imposed by regulatory authorities, could make an acquisition of us, which may be beneficial to our stockholders, more difficult, limit attempts by our stockholders to replace or remove our current management, limit our stockholders' ability to obtain a favorable judicial forum for disputes

with us or our directors, officers, or employees, and limit the price of our Class A common stock. Provisions in our restated certificate of incorporation and restated bylaws may have the effect of delaying or preventing a merger, acquisition, or other change of control of our company that the stockholders may consider favorable. In addition, because our board of directors is responsible for appointing the members of our management team, these provisions may frustrate or prevent any attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors. Our restated certificate of incorporation and restated bylaws include provisions that: • permit our board of directors to establish the number of directors and fill any vacancies and newly- created directorships; • require super- majority voting to amend some provisions in our restated certificate of incorporation and restated bylaws; • authorize the issuance of " blank check " preferred stock and common stock that our board of directors could use to implement a stockholder rights plan or issue other shares of preferred stock or common stock, including blockchain tokens; • provide that only our Chief Executive Officer, the chairperson of our board of directors, or a majority of our board of directors will be authorized to call a special meeting of stockholders; • eliminate the ability of our stockholders to call special meetings of stockholders; • prohibit cumulative voting; • provide for a dual class common stock structure in which holders of our Class B common stock have the ability to control the outcome of matters requiring stockholder approval, even if they own significantly less than a majority of the outstanding shares of our Class A common stock and Class B common stock, including the election of directors and significant corporate transactions, such as a merger or other sale of our company or its assets; • provide that the board of directors is expressly authorized to make, alter, or repeal our restated bylaws; and • provide for advance notice requirements for nominations for election to our board of directors or for proposing matters that can be acted upon by stockholders at annual stockholder meetings. Moreover, Section 203 of the Delaware General Corporation Law (the " DGCL ") may discourage, delay, or prevent a change of control of our company. Section 203 imposes certain restrictions on mergers, business combinations, and other transactions between holders of 15 % or more of our common stock and us. In addition, a third party attempting to acquire us or a substantial position in our common stock may be delayed or ultimately prevented from doing so by change in ownership or control regulations to which our regulated broker- dealer subsidiaries are subject. FINRA Rule 1017 generally provides that FINRA approval must be obtained in connection with any transaction resulting in a single person or entity owning, directly or indirectly, 25 % or more of a member firm' s equity and would include a change of control of a parent company. Our restated certificate of incorporation contains an exclusive forum provision for certain claims, which could limit our stockholders' ability to obtain a favorable judicial forum for disputes with us or our directors, officers, or employees. Our restated certificate of incorporation, to the fullest extent permitted by law, provides that the Court of Chancery of the State of Delaware is the exclusive forum for any derivative action or proceeding brought on our behalf; any action asserting a claim that is based upon a breach of fiduciary duty; any action asserting a claim against us or any current or former director, officer, stockholder, employee or agent of ours, arising pursuant to the DGCL, our restated certificate of incorporation, or our restated bylaws; any action asserting a claim against us that is governed by the internal affairs doctrine; or any action asserting an " internal corporate claim " as defined in Section 115 of the DGCL. Moreover, Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over all claims brought to enforce any duty or liability created by the Securities Act or the rules and regulations thereunder and our restated certificate of incorporation provides that the federal district courts of the United States of America are, to the fullest extent permitted by law, the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act, or a Federal Forum Provision, unless we consent in writing to the selection of an alternative forum. Our decision to adopt a Federal Forum Provision followed a decision by the Supreme Court of the State of Delaware holding that such provisions are facially valid under Delaware law. While there can be no assurance that federal or state courts will follow the holding of the Delaware Supreme Court or determine that the Federal Forum Provision should be enforced in a particular case, application of the Federal Forum Provision means that suits brought by our stockholders to enforce any duty or liability created by the Securities Act must be brought in federal court and cannot be brought in state court. Section 27 of the Exchange Act creates exclusive federal jurisdiction over all claims brought to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder. The Federal Forum Provision applies to suits brought to enforce any duty or liability created by the Exchange Act to the fullest extent permitted by law. Accordingly, actions by our stockholders to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder must be brought in federal court. Our stockholders will not be deemed to have waived our compliance with the federal securities laws and the regulations promulgated thereunder. Any person or entity purchasing or otherwise acquiring or holding any interest in any of our securities will be deemed to have notice of and consented to our exclusive forum provisions, including the Federal Forum Provision. These provisions may limit our stockholders' ability to bring a claim in a judicial forum they find favorable for disputes with us or our directors, officers, or other employees, which may discourage lawsuits against us and our directors, officers, and other employees. Alternatively, if a court were to find the choice of forum provision contained in our restated certificate of incorporation to be inapplicable or unenforceable in an action, we may incur additional costs associated with resolving such action in other jurisdictions, which could harm our business, operating results, and financial condition.