CME Group SASB Metrics – Security & Commodity Exchanges

SASB broadly defines "sustainability" as the corporate activities that maintain or enhance the ability of the company to create value over the long term. SASB standards are intended for use in communications to investors regarding sustainability issues that are likely to impact corporate ability to create value over the long term. Use of SASB standards is voluntary. The following disclosure is based on SASB's "Security and Commodity Exchanges" industry-specific standard. While not all disclosure topics within the "Security and Commodity Exchanges" industry-specific standard may be relevant to CME Group's "sustainability" (as defined by SASB), in the interest of transparency, the below table provides requested information on a best efforts basis for 2024.

SASB CODE	DESCRIPTION	CME GROUP RESPONSE
PROMOTING TRANSPARENT & EFFICIENT CAPITAL MARKETS		
FN-EX-410a.1	(1) Number and (2) average duration of (a) halts related to public release of information and (b) pauses related to volatility	As a derivatives marketplace (not an equity marketplace), CME Group's markets do not include equities of listed companies and, therefore, CME Group does not (and is not required to) halt its markets based on the public release of information. CME Group has several measures in place on its CME Globex electronic trading platform (CME Globex) that are designed to operate its markets in an efficient and orderly manner during volatile market conditions, including the following: • **Daily Price Limits:** Price limits represent the maximum price range permitted for a futures contract in each trading session. If a price limit is hit, the market remains open; however, it cannot trade above/below that price range. • **Circuit Breakers:** A series of price limits that, when reached, pause a market for a particular period of time to allow markets to reset. • **Velocity Logic:** CME Globex monitors for potentially significant price movements in extremely small time increments. Velocity logic works in conjunction with price banding to address market prices that move too far, too fast. If a velocity logic violation occurs, the applicable futures market is automatically temporarily suspended, as are all associated options markets. • **Market-Wide Circuit Breakers:** A control in CME Group equity products that suspends trading upon the activation of a market-wide regulatory halt pursuant to New York Stock Exchange Rule 7.12 or Nasdaq Stock Market Rule 4121. During 2024, 386 circuit breakers were triggered and 1,124 velocity logic events occurred in CME Group's markets. The duration of the pause or suspension is based on the applicable contract and activity in the market. During 2024, there were no market-wide circuit breakers.
FN-EX-410a.2	Percentage of trades generated from automated trading systems	The primary venue for trading CME Group futures and options is CME Globex, a resilient open access platform that provides global connectivity to CME Group markets. CME Group employs many policies, procedures and controls that assist in the mitigation of risks associated with any type of electronic trading on CME Globex, including robust protocols for risk management, operational and technological resiliency, market surveillance and cybersecurity. A highly granular and precise audit trail of all CME Globex activity allows us to identify and monitor the trading activity of participants on CME Globex both on a real-time and post-trade basis. The audit trail also allows us to identify activity originating from automated trading systems. Automated trading systems are used by nearly every type of participant, from farmers to market makers. Automated trading systems allow these participants to provide deep liquidity with narrow bid-ask spreads, reduce price and execution risk, minimize market impact and reduce costs. We believe that open interest—the total number of open futures and options contracts held by market participants at the end of each day—is a reliable measure of the sustainability of our markets. Open interest is a measure of market liquidity and the ability of a participant to efficiently initiate or offset a futures or options position. These metrics are available in the Daily Bulletin—Exchange Overall Volume and Open Interest on our Investor Relations page under Financial and Other Reports—Volume Reports. The notional volume traded and market depth data published daily for our cash markets businesses are also reliable measures of the sustainability of our cash Treasury and FX markets. These metrics are available in the UST Market Profile and FX Market Profile tools on the CME Group website.
FN-EX-410a.3	Description of alert policy regarding timing and nature of public release of information	As a derivatives marketplace (not an equity marketplace), CME Group's markets do not include equities of listed companies and, therefore, CME Group does not (and is not required to) have an alert policy relating to listed companies' public release of information or company developments that may affect a stock price (positively or negatively).
FN-EX-410a.4	Description of policy to encourage or require listed companies to publicly disclose environmental, social, and governance (ESG) information	As a derivatives marketplace (not an equity marketplace), CME Group's markets do not include equities of listed companies and, therefore, CME Group does not (and is not required to) have such a disclosure policy. As a derivatives marketplace, our focus is on developing products and services for our clients' evolving risk management needs, including for those industries most affected by climate change, such as energy, metals and agriculture. As the global marketplace evolves, we are in conversations with market participants to assist us with offering the necessary enhancements to our current contracts or to develop new trading products that best meet their changing needs and sustainability goals. See the Sustainable Solutions pillar disclosures as part of our Corporate Citizenship reporting and our website for more information on our suite of sustainable products. We also highlight that our leaders participate in and share their expertise with a number of high-profile initiatives and industry-led working groups, committees and taskforces designed to develop market-wide approaches to advancing more sustainable financial markets.

SASB CODE	DESCRIPTION	CME GROUP RESPONSE
MANAGING CONFLICTS OF INTEREST		
FN-EX-510a.1	Total amount of monetary losses as a result of legal proceedings associated with fraud, insider trading, anti-trust, anti-competitive behavior, market manipulation, malpractice, or other related financial industry laws or regulations	In accordance with applicable securities laws and regulations, CME Group includes a description of material legal proceedings (including of the type, if any, described in FN-EX-510a.1) in our annual and quarterly filings on Forms 10-K and Form 10-Q, respectively. During 2024, the only legal and regulatory matter disclosed by CME Group in such filings was the putative class action complaint filed January 15, 2014 in the Circuit Court of Cook County, Chancery Division, against CME Group and the Board of Trade of the City of Chicago, Inc. (CBOT). The plaintiffs, certain Class B shareholders of CME Group and Class B members of CBOT, allege breach of contract and breach of implied covenant of good faith and fair dealing for violations of their core rights granted in the defendants' respective Certificate of Incorporation. Based on its investigation to date, the company believes that it has strong factual and legal defenses to the claims.
FN-EX-510a.2	Discussion of processes for identifying and assessing conflicts of interest	CME Group has adopted a Code of Conduct that applies to its employees, internal consultants and temporary personnel resources. The Code of Conduct builds on CME Group's business principle of "leading with conviction and integrity" by setting the tone for a culture of compliance, ethical conduct and accountability, and providing greater detail about the behavior expected from our colleagues. The Code of Conduct is supplemented by a more detailed, separate Conflicts of Interest Policy, which sets forth the process for identifying, monitoring and managing actual and potential conflicts of interest. CME Group seeks to ensure that a conflict of interest does not adversely affect the interests of its organization, its clients, its shareholders or other stakeholders. CME Group employees, internal consultants and temporary personnel resources are required to disclose potential conflicts of interest, including but not limited to, those relating to personal relationships, outside business activities, financial interests and opportunities. These disclosures are reviewed and approved by the Compliance Department and management, as appropriate. In addition, CME Group colleagues must certify to the Code of Conduct and to the Conflicts of Interest Policy on an annual basis. CME Group Board members are subject to the Board of Directors Code of Ethics, which requires that Board members avoid any circumstance that creates or appears to create a conflict between a Board member's own interests and the interests of the company. The Nominating and Governance Committee is responsible for overseeing Board members' compliance with the Board of Directors Code of Ethics. Board members must certify to this Code of Ethics on an annual basis. When identifying a situation where an actual or potential conflict of interest cannot be avoided, Compliance recommends appropriate actions to manage, document and, as applicable, report the situation. CME Group's program to address conflicts of interest includes: • Written policies (CME Group Code of Conduct, CME Group Conflicts of Interest Policy, Board of Directors Code of Ethics, Confidentiality and Data Protection Policy, Personal Trading Policy, Anti-Financial Crime Policy) • Disclosure obligations to identify, assess and manage potential conflicts of interest • Regular, ongoing reviews by Compliance of disclosures under our Conflicts of Interest Policy • Regular and ad hoc awareness raising measures, including as required based on our operation of regulated businesses • Separate supervision and segregation of functions • Confidentiality and information barriers • Checks, controls, monitoring and escalation in the case of non-compliance • Documentation and reporting to management and on an aggregated basis at the Board committee level • Reporting avenues, including a third-party operated helpline with anonymous reporting in all permitted locations

SASB CODE	DESCRIPTION	CME GROUP RESPONSE
MANAGING BUSINESS CONTINUITY & TECHNOLOGY RISKS		
FN-EX-550a.1	(1) Number of significant market disruptions and (2) duration of downtime	During 2024, CME Group's markets did not have any significant market disruptions.
FN-EX-550a.2	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of customers affected	No material data breaches that required reporting under data privacy laws occurred during 2024.
FN-EX-550a.3	Description of efforts to prevent technology errors, security breaches, and market disruptions	CME Group has robust programs, policies and procedures reasonably designed to prevent technology incidents, security breaches and market disruptions. **TECHNOLOGY** CME Group maintains policies, standards, procedures and other documentation regarding its secure software development lifecycle, change management, availability management and capacity planning, among others, which contribute to the prevention of technology incidents. **INFORMATION SECURITY** Our Global Information Security Program is designed and operated to mitigate information security risks and threats to the company. Its intent is to safeguard the confidentiality, integrity and availability of CME Group's information and services. The program is designed to strengthen the integrity of the global markets we support, protect CME Group's information assets, maintain client, third party and employee trust, support our pursuit of strategic objectives, contribute to shareholder value and preserve our reputation and brand. We implement technical, physical and administrative safeguards to protect the confidential and sensitive information of our clients, third parties, employees and other information under CME Group's stewardship. We manage cybersecurity risk to the organization as part of our business strategy, risk management and financial functions in alignment with our overall Enterprise Risk Management (ERM) Program and regularly engage with the Risk Committee of the Board of Directors and the Board of Directors as a whole regarding the effectiveness of the program and the management of our cybersecurity risks. The program is led by CME Group's Chief Information Security Officer (CISO). The CISO reports directly to our Chief Information Security Officer, a member of our Management Team, and indirectly to our Risk Committee. As part of our program, CME Group operates a Cyber Defense Center that virtually links 24/7 to our international cybersecurity teams and serves as a global hub for cybersecurity risk management activities, including log collection, event monitoring, threat detection and incident response, resiliency, operations, vulnerability management and the proactive collection and processing of both open source and proprietary threat and intelligence feeds allowing the company to efficiently manage, investigate and respond to cybersecurity events. Our Global Information Security team conducts analyses and aims to prevent, detect and respond to systemic events that might threaten our company, industry or the economy. The program includes a Cyber Defense team, which manages the Incident Response Plan. The plan outlines our cyber and incident response policies and governs our incident response lifecycle, which divides overall incident response into serial phases. We identify, assess and manage material risks from cybersecurity threats through our program as follows: • We deploy a defense-in-depth strategy, acknowledging the importance of people, processes and technology in upholding information security. The strategy incorporates multiple layers of controls, including, monitoring, vulnerability management, identity and access management and security assessments. • Our program is aligned with the National Institute of Standards and Technology Cybersecurity Framework (NIST) and other technical standards and frameworks. • We have a robust cybersecurity defense response plan that provides a documented framework for handling security incidents and facilitates coordination across multiple parts of the company. • We invest in threat intelligence and operate a Cyber Defense Center, which acts as our hub of information sharing and threat intelligence analysis. • We incorporate external expertise and reviews into our cybersecurity risk management program and continue to engage leading professional consulting firms to assist our company in incorporating cybersecurity best practices. • We provide annual cybersecurity awareness and ongoing phishing training, and we routinely conduct cybersecurity attack simulation exercises, which includes participation from various levels of management. • Following a risk-based approach, we conduct due diligence reviews of our third party providers for potential cybersecurity risks to the company. We also maintain a cross-functional Third Party Risk Management (TPRM) Program, which partners with our Global Information Security, Information Governance, and Operational Resilience teams, among others, to manage and monitor third party risk presented by CME Group vendors and certain third parties of third parties (fourth parties). The teams conduct initial due diligence on vendors and monitor cyber-related incidents and known vulnerabilities with the goal of enhancing processes, improving risk management and partnering on exit planning and testing for certain vendors associated with essential functions. • We have insurance against certain cybersecurity and privacy risks and attacks. • We are an active participant in the financial services industry and government forums and information sharing programs, designed to improve both internal and sector cybersecurity defense. These valuable external partnerships are established and maintained in order to gain more timely, comprehensive and actionable threat information across geographies and industries and to facilitate the exchange of best practices and security techniques. They allow for a high degree of collaboration and cooperation with local, state, federal, and international law enforcement and intelligence agencies, industry groups, and other private sector chief information security officers. • We regularly test the design and effectiveness of our information security controls and processes through a program of testing performed by internal and independent third-party teams. Remediation of gaps and opportunities identified through testing are tracked through to closure. Testing activities support a variety of regulatory requirements and external industry certifications held by CME Group.

SASB CODE	DESCRIPTION	CME GROUP RESPONSE
MANAGING BUSINESS CONTINUITY & TECHNOLOGY RISKS *(CONTINUED)*		
FN-EX-550a.3 *(continued)*	Description of efforts to prevent technology errors, security breaches, and market disruptions *(continued)*	**MARKET REGULATION DEPARTMENT** The CME Group Market Regulation Department is responsible for monitoring our markets to identify and prevent potential rule violations, including disruptive trading practices. The department utilizes sophisticated regulatory systems to conduct market and trade practice surveillance. A key element of our Regulation Program is educating our market participants about the requirements and expectations detailed in our rulebooks and trading advisories. When violations are identified and disciplinary action may be warranted, enforcement proceedings are conducted before a disciplinary panel, and appropriate disciplinary actions are taken. **OPERATIONAL RESILIENCE PROGRAM** The CME Group Operational Resilience (OpRes) Program serves to mitigate potential impacts to our markets, clients, assets and employees and to safeguard the effective availability of critical products and services. The program is designed to help ensure that CME Group can respond appropriately to incidents while protecting the interests of its stakeholders, the safety of employees and protecting its reputation and brand. Our OpRes team continually identifies new and changing business risks to our operations across all CME Group locations through internal monitoring and planning, industry and agency partnerships and various information sharing organizations across the globe. The OpRes team works with departments and employees across the company to assess risks at varying levels of severity. We have developed a framework for mitigating these risks designed to help ensure our business and our markets continue to operate effectively through various resiliency strategies. Key aspects of the OpRes Program include: • System Resilience (Disaster Recovery) is the intersection of Operational Resilience efforts and the technology that supports the delivery of CME Group's critical business services. Not limited to a catastrophic event, System Resilience prepares for and identifies alternative ways that critical processes can be completed when dependencies (including systems) are not available. The System Resilience Program works to mitigate risk by helping ensure CME Group can recover its systems following an event that impacts the delivery of technology services through production environments or deployments. This is done by establishing requirements, approving system design, and testing that systems can meet their requirements – including their ability to recover with their applicable recovery time objectives as identified within the Business Resilience business impact analyses and/or by applicable regulatory mandate. • The Business Resilience Program is designed to help ensure CME Group can rapidly adapt and respond to internal or external changes – demands, disruptions or threats – while prioritizing essential business operations and safeguarding people and assets. • The Operational Resilience team monitors and prepares for unique, high-risk events that fall outside routine, all-hazards planning activities through the Crisis Analysis and Response (CAR) Program, like the Russian invasion of Ukraine or tensions with China. The CAR Program helps CME Group prepare for certain extreme but plausible events and provides a framework for response to events that are unique and sometimes geopolitical in nature. Through the CAR Program, CME Group ensures that the appropriate expertise is gathered from across the enterprise to evaluate, plan for and manage any incidents that may impact our markets, customers, employees, and reputation. CAR is involved in the planning efforts around things like major geopolitical changes or ongoing unrest where market structure, sanctions, and cyber threats may be in play. We generally align the program with industry-best practices classified in applicable U.S. and international standards stemming from our categorization as a systemically important market utility and systemically important derivatives clearing organization. **INFORMATION GOVERNANCE AND DATA PRIVACY** CME Group is committed to protecting its proprietary, confidential and personal data, including information relating to its business, customers, vendors, strategic partners, employees and other third parties. We have an established Information Governance and Privacy Program which is designed to support our company in managing Chicago Mercantile Exchange Inc.'s data and corporate information in compliance with applicable laws and regulations and reducing risk associated with our data. **THIRD PARTY RISK MANAGEMENT** CME Group maintains a TPRM Program designed to identify, assess and manage potential risks relating to the engagement of certain third parties that support CME Group in delivering its business strategy, including the operation of its markets. TPRM monitors third parties who present moderate to critical risk throughout their engagement lifecycle. The program coordinates with Procurement, Legal, Global Information Security, Information Governance/Privacy and OpRes teams allowing our contracts and vendor renewals to align to our risk management posture, provide adequate assurance and meet regulatory requirements. The OpRes team works with TPRM to help provide assurances that third-party vendors impacting our critical operations have business continuity and disaster recovery plans to minimize service interruptions and control issues whenever unforeseen disturbances arise involving a third party's operation. **INSURANCE** We maintain insurance coverage that may, subject to the terms and conditions of the policy and payment of significant deductibles, cover certain aspects of cybersecurity issues. **MONITORING, TESTING AND AUDIT** We have adopted a risk-based approach to our monitoring, testing and auditing practices, which is consistent with our overall ERM Program and the levels of acceptable appetite for managing key risks associated with our business and strategy as approved by the Board of Directors. Through this program, we provide a comprehensive review of our risk management practices and endeavor, in an ongoing manner, to provide assurances that enterprise risks, including those relating to technology errors, security breaches and market disruptions, are identified, assessed, measured, prioritized and reported by management responsible for the respective risks. The CME Group Internal Audit function and our IT Controls and Compliance team conduct independent testing and monitoring utilizing various methods to verify compliance with written policies and procedures, validate control effectiveness and assess risk exposure from identified control weaknesses or gaps. In addition, our regulated businesses are subject to examinations from multiple regulatory bodies, including the CFTC. We conduct internal security audits and vulnerability assessments as well as internal and external penetration tests, tests of our cyber security incident response protocols and regulatory IT control testing. CME Group has obtained the ISO27001 information security certification, an international standard signifying that CME Group manages information security with processes that preserve the confidentiality, integrity and availability of information. Our Data Privacy Program is subject to periodic internal audits and external assessments.

SASB CODE	DESCRIPTION	CME GROUP RESPONSE
ACTIVITY MEASURES		
FN-EX-000.A	Average daily number of trades executed by product or asset class	**FUTURES AND OPTIONS ON FUTURES CONTRACTS (in thousands)** CME Group reports trading activity in its futures contracts by volume. Volume is calculated by counting the number of contracts that have been bought and sold over a given time. The following summarizes average daily contract volume for 2024. **Aggregate Average Daily Volume: 26,528** **Average Daily Volume by Product Line:** Interest rates: 13,716 Equity indexes: 6,847 Foreign exchange: 1,030 Agricultural commodities: 1,711 Energy: 2,488 Metals: 736 **Average Daily Volume by Venue:** CME Globex: 24,510 Open outcry: 1,023 Privately negotiated: 995 **CASH MARKETS BUSINESS (In Billions)** CME Group reports trading activity in its cash markets business by notional value. Notional value is calculated by multiplying the contract unit by the contract's price. The following summarizes related average daily notional value for 2024: U.S. Repos: $328.4 European Repo: €290.1 U.S. Treasury: $101.9 Spot FX: $59.5 We report these market statistics in our periodic reports filed with the U.S. Securities Exchange Commission and they are also available on our website at http://investor.cmegroup.com/volume, including greater detail on average daily volume.
FN-EX-000.B	Average daily volume traded, by product or	See the information provided above under FN-EX-000.A.

NOTES: This report is limited to operations controlled by CME Group Inc. All amounts regarding contract volume are for CME Group's listed futures and options on futures contracts unless otherwise noted. Total contract volume includes contracts that are traded on our exchange(s) and cleared through our clearing house and certain cleared-only contracts. Volume is measured in round turns, which is considered a completed transaction that involves a purchase and an offsetting sale of a contract.