Tradeweb Cybersecurity Fact Sheet

Govern: Strategy and Oversight

Strategy

As a leader in building and operating electronic marketplaces for a global network of clients across the financial ecosystem, Tradeweb Markets Inc. (herein referred to as "Tradeweb" or the "Company or "Firm") recognizes that information security is critical. Tradeweb is committed to building and maintaining defenses to protect the confidentiality, integrity, and availability of client and business information.

Approach

Tradeweb implements cybersecurity controls and frameworks, aligning with industry standards and best practices, such as those established by the National Institute of Standards and Technology ("NIST") and ISO/IEC 27001.

In alignment with the NIST Cybersecurity Framework ("CSF"), Tradeweb actively works to stay ahead of and respond to cybersecurity threats and attacks, with a strategic focus on:

- Identifying ongoing risks;
- Protecting infrastructure;
- Detecting specific threats;
- Responding to cyber security events to mitigate damage; and
- Recovering business as usual activities after an event.

These cybersecurity measures enable Tradeweb to evaluate its current threat landscape, identify and deploy effective defense strategies, and work toward a more secure future state. The objective is to mitigate cyber threats, as defined by the Tradeweb risk taxonomy, and reduce potential impacts on Tradeweb clients and the broader financial markets. As the information security landscape and associated risks evolve, so does Tradeweb's Information Security program—with a focus on preserving the confidentiality, integrity, and availability of systems and data used, owned, or managed by Tradeweb and its customers.

Information Security Program

The Company maintains a dedicated Information Security program and Cybersecurity team, led by the Global Chief Information Security Officer ("CISO"), who reports directly to the Chief Risk Officer ("CRO"). The team is responsible for proactively identifying, assessing, mitigating, monitoring, and reporting on cyber risks across Tradeweb in alignment with leading industry standards and best practices.

Tradeweb's Information Security program is grounded in the NIST Cybersecurity Framework ("CSF"), which guides the design and implementation of a comprehensive and adaptable security posture. Executive oversight is integrated through a governance structure, including a Risk Committee chaired by the CRO and comprised of senior leaders from business, technology, and corporate functions. This Committee oversees the broader risk framework, approves the Firm's risk appetite, monitors the evolving cyber threat landscape, and reviews material policy changes.

Role of Board of Directors

The Board of Directors of Tradeweb Markets Inc. exercises direct oversight of the strategic risks to the

Company. The Audit and Risk Committee of the Board reviews guidelines and policies governing the process by which senior management assesses and manages exposure to risk, including the major financial and operational risk exposures, such as those derived from cybersecurity risk, and the steps management takes to monitor and control such exposures. The Board and the Audit and Risk Committee each receive periodic reports from the CISO, CRO and Chief Administrative Officer ("CAO") to assess key cybersecurity risks for the Company and the measures implemented to mitigate them, as well as updates regarding changes to the Company's cybersecurity risk profile or newly identified material risks. In addition, the Audit and Risk Committee reports to the Board on these matters at each regularly scheduled Board meeting. The Board and Audit and Risk Committee provide feedback and recommendations accordingly.

Role of Management

Tradeweb operates on a "three lines of defense" risk governance model, with partnership and communication across the three lines. The first line of defense is comprised of the business, technology, and cybersecurity teams. The second line of defense is comprised of the Compliance and Enterprise Risk Management teams. The third line of defense is comprised of the Internal Audit function. The second and third lines of defense focus on providing the first line of defense with advisory and assurance functions for informed and actionable risk-based decisions. The Risk Committee includes the CRO, Chief Technology Officer, General Counsel, CAO, Global Head of Enterprise Risk, CISO, Head of Global Compliance, Global Head of Human Resources, Head of Internal Audit and various global heads of business lines and corporate functions.

The Risk Committee is responsible for the governance and oversight of the Risk Framework, which includes cybersecurity risks. Its responsibilities include:

- Supervising risk mitigation strategies and their implementation;
- Overseeing compliance and regulatory aspects;
- Managing crises;
- Approving risk tolerance;
- Reviewing and approving material policy changes; and
- Evaluating the effectiveness of the Company's risk management practices.

The Risk Committee regularly obtains reports from the CISO who maintains the primary responsibility for assessing and managing the cybersecurity risks, evaluating the principal cybersecurity risks for the Company, and reviewing strategies in place to mitigate them. The Risk Committee meets quarterly and reports to senior management, including the Chief Executive Officer and Chief Financial Officer. Senior management provides oversight and support in aligning cyber risk management with the Company's strategic decisions, fostering a culture of risk awareness across the Firm and allocating adequate resources to support the initiatives.

Identify

Tradeweb acknowledges its responsibility to identify risks and information security / cyber threats to the Company, leveraging a combination of technical and process controls to manage these risks, as detailed below.

Risk Assessment

Tradeweb conducts regular and systematic cybersecurity risk assessments to identify, evaluate, and prioritize risks in accordance with the enterprise Tradeweb Risk Management Policy and Tradeweb Risk Assessment Procedure. These assessments consider a range of internal and external threats, vulnerabilities, asset criticality, and business impacts. Cyber risks are:

- **Identified** through both qualitative and quantitative methods;
- **Categorized** based on their nature (e.g., operational, regulatory, third-party);

- **Scored** using a structured framework that assigns impact and likelihood values; and
- **Prioritized** in alignment with Tradeweb's risk appetite, enabling appropriate mitigation strategies to be applied and resources to be allocated efficiently.

This process supports proactive risk mitigation, informs decision-making, and promotes continuous improvement of Tradeweb's cybersecurity posture, in alignment with NIST CSF requirements for risk-based governance.

Third-Party Risk Management

Tradeweb maintains a lifecycle-based Cyber Vendor Risk Management ("CyberVRM") program designed to identify, assess, monitor, and manage cybersecurity risks associated with third-party service providers and supply chain dependencies. The program includes in-depth security assessment, ongoing monitoring, risk-based control implementation, and contractual safeguards.

Asset Management

Tradeweb maintains a structured Asset Management Lifecycle to support accurate identification, classification, security, and maintenance of organizational assets throughout their lifecycle. This includes hardware, software, data, and other information system components.

Key program elements include:

- Systematic Asset Identification and Classification;
- Centralized Asset Inventory;
- Lifecycle Governance; and
- Security and Compliance Controls.

Threat Intelligence

Tradeweb's Cyber Threat Intelligence ("CTI") team actively incorporates a diverse array of cyber threat intelligence sources to enhance situational awareness and proactively mitigate cybersecurity risks. The CTI team regularly receives information on potential cybersecurity threats from a range of sources including industry peers, third-party threat intelligence vendors, regulators, law enforcement, government, and a variety of other private and open sources. Intelligence on threat actors, tactics, techniques, and procedures ("TTPs") is correlated with Tradeweb's operational and technical environment to improve relevance and response preparedness. Threat intelligence information is integrated into risk processes for vulnerability prioritization, security monitoring strategies, incident response planning, and enterprise risk assessments. The CTI team develops intelligence reports, which are distributed to relevant stakeholders and senior management on a monthly and quarterly basis to support informed decision-making.

Penetration Testing

Tradeweb maintains a penetration testing program to proactively identify and remediate vulnerabilities across its technology ecosystem. An enterprise-wide penetration test is conducted annually by an independent, qualified third-party provider, with supplemental assessments initiated following material architectural changes to Tradeweb applications.

Throughout the year, Tradeweb conducts targeted internal and external penetration tests focused on specific applications. External tests are scoped based on each application's risk profile and are executed through rigorous, tailored assessments. To promote objectivity and introduce varied expertise, Tradeweb rotates its external testing vendors on an annual basis.

Findings—whether originating from internal or external assessments—are reviewed and addressed in alignment with Tradeweb's Threat and Vulnerability Management standards, with the goal of maintaining

consistent and effective remediation practices.

Vulnerability Management

Tradeweb operates a Vulnerability Management ("VM") program that proactively identifies, assesses, and addresses security weaknesses across its enterprise technology landscape. Internet facing and internal systems are scanned continuously using automated tools managed by the Cybersecurity team to detect known vulnerabilities in applications, operating systems, and infrastructure.

The VM program is continuously enhanced to align with evolving threats and industry best practices, encompassing regular updates to tools, scanning methodologies, and remediation workflows. Vulnerabilities are triaged based on exploitability, threat intelligence, asset criticality, and business impact to prioritize remediation of material risks.

Remediation efforts follow defined SLAs and risk thresholds, with progress monitored through a centralized system. VM findings are also integrated into Tradeweb's broader cyber risk assessments, incident response planning, and ongoing monitoring initiatives.

Secure Software Development Lifecycle ("SDLC")

Tradeweb embeds security throughout every phase of its SDLC to help build applications with confidentiality, integrity, and resilience at their core. The secure SDLC framework integrates automated tooling, manual assessments, and continuous developer education to proactively mitigate software vulnerabilities at the earliest stages.

Core security controls include Static Application Security Testing ("SAST") to detect insecure coding patterns during development, and Dynamic Application Security Testing ("DAST") to identify runtime vulnerabilities in staging and pre-production environments. Tradeweb further reinforces application security through rigorous internal and external penetration testing of systems, replicating real-world attack scenarios to validate defensive controls.

To manage risks associated with third-party components, Software Composition Analysis ("SCA") tools are utilized to identify and remediate vulnerabilities in open-source and third-party libraries. Complementing these technical safeguards, Tradeweb mandates secure coding training and regular refresher courses tailored to developer roles and emerging threat vectors. This ongoing education supports a security-first development culture aligned with the firm's overarching vulnerability and risk management standards.

Protect

Tradeweb focuses on protecting clients, business assets, and data through a set of technical and process controls, detailed below.

Identity Management and Access Control

Tradeweb has adopted stringent access control principles as referenced in the Tradeweb Access Control Policy and Tradeweb Information Security Policy, which enforce the principles of:

- **Least privilege:** Limiting users and processes to access only resources and tools necessary to perform assigned functions.
- **Separation of privileges:** Separating processes based on different needs or privilege requirements to help prevent applications or system processes from accessing more data or systems than necessary.
- **Separation of duties:** Dividing roles and responsibilities so that a single individual cannot subvert a critical function, i.e., developers have no access to Production, and the Production & non-Production environments such as Development, QA, Staging, etc. are physically and logically separated.
- **Need-to-know:** Individuals are given rights to access the minimum information to perform their job

responsibilities on a need-to-know basis.

In accordance with the Tradeweb Information Security Policy, access is granted by explicitly defining the access required to preserve the confidentiality, integrity, and availability of information. Only authenticated users or processes are allowed access to any of Tradeweb's assets. Tradeweb carries out semi-annual entitlement reviews to help keep access rights up to date.

Data Security

Tradeweb supports the confidentiality, integrity, and availability of data in transit and at rest through the proper implementation of cryptographic controls. Cryptographic keys are securely managed by the Tradeweb Cybersecurity team and are stored within a trusted network environment, accessible only to a limited number of authorized personnel.

Data Loss Prevention ("DLP") program is in place, supported by a combination of policies, processes, and technical controls to reduce the risk of data exfiltration or unauthorized exposure. Security measures include:

- Blocking USB access on endpoint devices;
- Enforcing least-privilege access to production systems;
- Email surveillance and policy-based controls;
- Restricted internet access for sensitive functions; and
- SSL decryption for granular data inspection.

Network Security

Tradeweb implemented a layered network security architecture to protect connectivity, enforce access controls, and maintain the secure flow of data across its infrastructure. Core components of this framework include rigorous segmentation, strong authentication mechanisms, and tightly governed traffic filtering to reduce attack surfaces and enforce security boundaries.

The environment is segmented to isolate production systems, internal networks, and wireless zones, limiting lateral movement and containing potential threats. Only devices recorded in the approved asset inventory are permitted to connect, and privileged or remote access, whether by internal users or third parties, must follow approved authentication protocols.

Encryption is applied to VPN and sensitive communication channels to preserve confidentiality and integrity. Strict ingress and egress controls are enforced, and inter-zone communications follow firewall policies.

Endpoint Security

Tradeweb enforces a set of endpoint security processes to align the configuration, maintenance, and security of network systems, servers, and workstations with defined security baselines. The program emphasizes proactive patching, standardized configurations, and compliance with industry benchmarks to reduce risk and maintain operational integrity.

Cloud Security

Tradeweb's Corporate Environment has a structured cloud security framework designed to protect data confidentiality, support integrity, and maintain availability across its cloud environments. This framework emphasizes strong identity governance, standardized configurations, and encrypted data handling to enforce consistent security across cloud platforms.

Cloud resources are provisioned with embedded security controls integrated into deployment workflows to promote consistency and reduce configuration drift. Access to cloud environments is restricted to authorized users through federated identity systems, with multi-factor authentication ("MFA") required for all privileged and

administrative roles.

Data in transit and at rest is secured using approved encryption protocols. Security groups, firewall rules, and service permissions are tightly scoped according to the principle of least privilege, and inter-service communications are segmented to reduce exposure and isolate workloads.

Please note that none of Tradeweb's trading systems are cloud based.

Physical and Environmental Security

Tradeweb has preventive, detective and corrective security measures in place at each of its facilities. Tradeweb enforces strict access controls, which are covered as part of the Tradeweb Information Security Policy and Tradeweb Access Control Policy, including: key card access, CCTV monitoring, 24/7 surveillance, 24/7 physical security, alarm systems, access points with locked doors, Clean Desk Policy, and automatic screen-locking. Tradeweb operates on a 'least privileged' model and only authorized Tradeweb personnel have access to or can manage any Tradeweb data and equipment.

Please note that at a minimum, valid identification, such as a driver's license, must be provided by visitors to enter a Tradeweb facility, and guests will be supervised by a permanent member of staff. They must also be registered with the building security for additional security checks prior to entering a Tradeweb office location. A forced sign in policy is also implemented at the front desk for access to any of Tradeweb's facilities.

Training and Awareness

Tradeweb has established formal standards to implement processes that foster a strong culture of cybersecurity awareness and equip employees with the knowledge necessary to protect organizational assets.

The program emphasizes the importance of educating personnel on evolving security threats, data protection best practices, and their individual roles and responsibilities in safeguarding the firm's information ecosystem.

Key training elements include:

- Mandatory annual information security training for all personnel;
- Role-based ongoing technical training aligned to employees' job functions;
- Monthly phishing simulation exercises; and
- Multi-format content delivery, including:
    - Customized and generic video modules
    - Email notifications or bulletins
    - Internal blog communications
    - Special awareness sessions
    - Ad-hoc knowledge-sharing initiatives
    - External guest speaker sessions.

Additionally, all Tradeweb employees are required to review and formally acknowledge the Code of Business Conduct and Ethics and sign confidentiality agreements.

Detect

Tradeweb uses proactive measures to detect potential information security risks and cyber threats. This approach combines technical and process controls to detect emerging risks, as outlined below, to help safeguard the client's trading activities.

Logging and Monitoring

Tradeweb employs a combination of proprietary and commercial tools to support a security logging and monitoring infrastructure capable of collecting and analyzing billions of security log events daily. These tools are configured to identify and alert on anomalous behaviors, indicators of compromise, and policy violations across the enterprise environment.

Tradeweb's Security Operations Center ("SOC") operates 24x7x365 to provide continuous monitoring and rapid response capabilities. The SOC provides tailored oversight and maintains the integrity of Tradeweb's Security Information and Event Management ("SIEM") environment. Core SOC responsibilities include:

- Real-time log ingestion, correlation, and analysis of events from networks, endpoints, applications, and cloud assets;
- Automated alerting and escalation for suspicious or unauthorized activity;
- Incident response support, including triage, ticketing, and hand-off to relevant response teams; and
- Maintenance and tuning of SIEM rules and detection logic to adapt to emerging threats.

Tradeweb's logging and monitoring program provides continuous visibility into system activity and supports threat detection and response efforts.

Intrusion Detection

Tradeweb employs a layered intrusion detection strategy designed to proactively identify and mitigate unauthorized access attempts, anomalous activity, and other malicious behaviors targeting its systems and networks. Monitoring tools are strategically placed across infrastructure components, enabling continuous visibility into network traffic, system logs, and user behavior. The intrusion detection program is continuously enhanced through regular tuning of detection signatures and behavioral baselines, informed by threat intelligence and lessons learned from incident investigations. When suspicious activity is detected, the SOC coordinates a rapid response involving forensic analysis, escalation to appropriate teams, and the implementation of targeted countermeasures to contain and remediate threats.

To further bolster Tradeweb's detection and mitigation capabilities, a dedicated Distributed Denial-of-Service ("DDoS") protection solution is implemented. This solution is designed to inspect and defend all inbound internet traffic across Tradeweb's digital assets and trading infrastructure. It provides:

- Always-on traffic scrubbing and rate-limiting for volumetric and application-layer DDoS threats;
- Global coverage to detect and absorb attacks at scale before they reach material endpoints; and
- Integration with incident response workflows to accelerate mitigation and maintain availability of services.

Respond and Recover

Tradeweb demonstrates below its commitment to rapid and effective response to information security and cybersecurity events. With dedicated teams and business continuity and disaster recovery processes in place, Tradeweb supports a consistent and coordinated approach to recovery, minimizing business and client disruption and facilitating a swift return to normal business operations.

Business Continuity ("BC") and Disaster Recovery ("DR")

Tradeweb is committed to providing uninterrupted delivery of products and services to clients. As a global institution, Tradeweb is exposed to uncontrollable events that cause varying degrees of disruption to normal business processes. The Business Continuity and Disaster Recovery program is a material component of the enterprise resiliency strategy. It is designed to plan for, respond to, and recover from business interruptions, with a view to minimize impact and facilitate service continuity both within recovery time objectives and based on prioritization of business objectives and operations.

Tradeweb's resiliency posture is continuously enhanced through a BCDR planning, testing and review program. A variety of exercises enable Tradeweb to challenge, verify, and demonstrate the Company's ability to mitigate disruption risk/impact, identify improvements, and validate recovery capabilities. The Tradeweb Business Continuity Plan establishes the requirements for the types of BCDR testing, their frequency, and test participant roles and responsibilities. This includes conducting quarterly table-top exercises and participating in industry-led exercises to help coordinate responses to material cyber security incidents.

Incident Response ("IR")

Tradeweb maintains a global Cybersecurity IR Plan that defines the enterprise-wide process for responding to suspected or confirmed information security incidents and cyberattacks. The Plan outlines roles, responsibilities, escalation paths, and procedural steps for containing, investigating, mitigating, and recovering from incidents. It also incorporates client and regulatory reporting obligations to promote timely, compliant actions that align with Tradeweb's contractual requirements.

The IR framework is supported by detailed playbooks covering Cyber Incident Response Team, Legal, Compliance, Client Services Communications, Crisis Communications, Cybersecurity Incidents, and Executive Escalation.

A structured escalation process is governed by the Incident Response Leadership Team ("IRLT"), a multidisciplinary group composed of senior leaders from across the firm. This includes a Technology IRLT, which convenes technology leadership to guide escalations involving infrastructure, platforms, or application-level threats. Both groups provide executive oversight, decision-making support, and cross-functional coordination during incident events.

Tradeweb conducts multiple tabletop exercises throughout the year as part of its operational readiness efforts, including, executive-level crisis management exercises involving the IRLT and the firm's executive leadership, as well as briefings with the Board of Directors. In parallel, technical tabletop exercises are held with Infrastructure and Security Operations teams to simulate threat scenarios, validate playbooks, and continuously improve detection, escalation, and response procedures.

In the event of an incident impacting customer data, Tradeweb will notify affected clients and regulatory authorities as required. A dedicated Incident Response Communication team, comprising representatives from Communications, Legal, Risk, Cybersecurity, Compliance, and senior management, supports efficient and coordinated stakeholder engagement.

The information included herein is provided for general informational purposes only. All information is provided "as-is". Tradeweb makes no representations or warranties, and disclaims all express, implied and statutory warranties of any kind relating to the information provided herein. Tradeweb is not liable for any damages arising out of the use or reliance on the information herein, including any consequential, incidental or indirect damages relating to the information contained herein.