GLOBAL ENTERPRISE
STRATEGIES

Global Data Sentinel's Cyber Security Solutions Help Financial Organizations Comply With Potential New Regulations

The following is taken from the November 9, 2015 Cyber Security Regulation Requirements advisory to Financial and Banking Information Infrastructure Committee (FBIIC) Members by the New York State Department of Financial Services.

Global Data Sentinel's cyber security solution can currently provide banking and financial services members with the ability to achieve compliance with the corresponding regulatory requirement.

Cyber Security Policy & Procedures

Covered entities would be required to implement and maintain written cyber security policies and procedures that address the following areas:

Regulatory Requirement	The Global Data Sentinel Solution
Information Security	Global Data Sentinel provides security at the data level, by encrypting databases, folders, files and data, regardless of whether at-rest or in-transit. As the security travels with the data, absolute security is maintained at all times.
Data Governance & Classification	Global Data Sentinel includes client-specific configuration and parameterization for the purposes of aligning with corporate governance and classification policies and procedures.
Access Controls & Identity Management	One of the four security pillars of the Global Data Sentinel is User Identity Management and Access Controls.
Business Continuity & Disaster Recovery Planning & Resources	Global Data Sentinel provides full back-up and tamper-proof versioning controls, for full BCP and DR contingency.
Capacity & Performance Planning	Global Data Sentinel provides performance monitoring all applications within a network, including: Bandwidth, Capacity, Availability, Performance and Utilization.
Systems Operations & Availability Concerns	Global Data Sentinel provides performance monitoring all applications within a network, including: Bandwidth, Capacity, Availability, Performance and Utilization.

Cyber Security Policy & Procedures *(continued)*

Regulatory Requirement	The Global Data Sentinel Solution
Systems & Network Security	Global Data Sentinel is cross-domain; meaning it works at network and/or cloud-level, including network/cloud hybrid systems.
Systems & Application Development & Quality Assurance	Global Data Sentinel provides the underlying security infrastructure for all systems and applications running on a network.
Physical Security & Environmental Controls	Global Data Sentinel can secure physical devices connected to corporate networks and/or the cloud, such as scanners/ printers, security cameras, IoT (Internet of Things).
Customer Data Privacy	Global Data Sentinel is a zero-knowledge system. All data within network and/or cloud is stored encrypted, including customer data, so that even sensitive IT personnel cannot see data. GDS is deployed as a client/server solution so the zero knowledge extends to GDS as well, with the corporate and customer data encrypted client-side.
Vendor & Third-Party Service Provider Management & Incidence Response - Including by Setting Clearly Defined Roles & Decision Making Authority	Global Data Sentinel can configure and apply these definitions, and also apply automated control according to required parameterization. Furthermore, GDS provides a "score card" of the member corporations' cyber security, so that C-level has panoramic transparency and insight into their network, application and end point device security.

Third-Party Service Provider Management

Each covered entity would be required to implement and maintain policies and procedures to ensure the security of sensitive data or systems that are accessible to, or held by, third party service providers. The policies and procedures would be required to include internal requirements for minimum preferred terms to be included in contracts with third-party service providers, including provisions requiring:

Regulatory Requirement	The Global Data Sentinel Solution
The Use of Multi-Factor Authentication to Limit Access to Sensitive Data and Systems	Global Data Sentinel utilizes multi-factor authentication, including biometric scanning and/or proximity cards. GDS can provide the hardware, or work with any 3rd party hardware member corporations wish to utilize.

Third-Party Service Provider Management *(continued)*

Regulatory Requirement	The Global Data Sentinel Solution
The Use of Encryption to Protect Sensitive Data in Transit & at Rest	Global Data Sentinel encrypts data at-rest and in-transit using AES-256 encryption and dynamic encryption keys.
Notice to be Provided in the Event of a Cyber Security Incident	Global Data Sentinel provides automated notifications and alerts in the event of a cyber security incident, it can also automatically enforce the threat response action.
The Indemnification of the Entity in the Event of a Cyber Security Incident That Results in Loss	Global Data Sentinel will consider indemnification on a case-by-case basis.
The Ability of the Entity or Its Agents to Perform Cyber Security Audits of the Third Party Vendor; & Representations & Warranties by the Third Party Vendors Concerning Information Security	Global Data Sentinel is a zero-knowledge system, meaning neither GDS or a member corporations' own IT staff are unable to access data unless those IT staff are authorized to do so. Furthermore, GDS provides a tamper-proof audit to ensure corporate policy and governance is enforced and monitored appropriately.

Multi-Factor Authentication

The Department believes that any regulation that establishes cyber security program requirements for covered entities should also address the use of multi-factor authentication as it applies to (i) customer access to web applications that captures or displays confidential information; (ii) privileged access to database servers that allow access to confidential information; and (iii) any access to internal systems or data from an external network. To this end, covered entities would be required, among other things, to implement multi-factor authentication for all access to internal systems and data from an external network.

Regulatory Requirement	The Global Data Sentinel Solution
Multi-Factor Authentication	As detailed above, Global Data Sentinel allows for multi-factor authentication when accessing hardware or software via the use of biometric scanning and/or proximity cards. GDS enables member corporations' to comply with the recommended regulatory requirements for multi-factor authentication.

Chief Information Security Officer

Each covered entity would be required to designate a qualified employee to serve as its Chief Information Security Officer ("CISO") responsible for overseeing and implementing its cyber security program and enforcing its cyber security policy. The CISO would also be required to submit to the Department an annual report, reviewed by the entity's board, assessing the cyber security program and the cyber security risks to the entity.

Regulatory Requirement	The Global Data Sentinel Solution
Designated Chief Information Security Officer & Annual Cyber Security Assessment / Report	Global Data Sentinel's "score card" is a dashboard that delivers a real-time, panoramic, transparency and insight into their network, application and end point device security. GDS believes this "score card" will support the CISO in their activities, as well as provide a benchmark for insurance underwriters seeking to assess a member corporations risk and therefore cost of any liability or cyber insurance.

Application Security

Each covered entity would be required to maintain and implement written procedures, guidelines, and standards reasonably designed to ensure the security of all applications utilized by the entity. The CISO would be required to review and update all such procedures, guidelines, and standards at least annually.

Regulatory Requirement	The Global Data Sentinel Solution
Written Procedures, Guidelines, & Standards for Application Security	Global Data Sentinel provides security that interacts at the application level.

Cyber Security Personnel & Intelligence

Each covered entity would be required to employ personnel adequate to manage the entity's cyber security risks and perform the core cyber security functions of identify, protect, detect, respond and recover. The entity would also be required to provide mandatory training to cyber security personnel and require key cyber security personnel to stay abreast of changing cyber security threats and countermeasures. Entities would be able to use third parties in meeting such requirements.

Regulatory Requirement	The Global Data Sentinel Solution
Trained Cyber Security Personnel	Global Data Sentinel allows member corporations to comply, and automates these functions for companies through the "score card" risk dashboard.

Audit

Each covered entity would be required to conduct annual penetration testing and quarterly vulnerability assessments. Entities also would be required to maintain an audit trail system.

Audit Trail Requirement	The Global Data Sentinel Solution
Logs Privileged User Access to Critical Systems	Global Data Sentinel ensures member corporations' compliance, with its user behavior analytics and tamper-proof audit logs.
Protects Log Data Stored as Part of the Audit Trail from Alteration or Tampering	Global Data Sentinel ensures member corporations' compliance, with its user behavior analytics and tamper-proof audit logs.
Protects the Integrity of Hardware from Alteration or Tampering	Global Data Sentinel ensures member corporations' compliance, with an additional hardware add-on, which can secure any device including IoT.
Logs System Events, Including Access & Alterations Made to Audit Trail Systems	Global Data Sentinel ensures member corporations' compliance, with its user behavior analytics and tamper-proof audit logs.

Notice of Cyber Security Incidents

Each covered entity would be required to immediately notify the Department of any cyber security incident that has a reasonable likelihood of materially affecting the normal operation of the entity, including any cyber security incident that meets the following criteria.

Regulatory Requirement	The Global Data Sentinel Solution
Department Must be Notified of a Cyber Security Incident That: • Triggers Certain Other Notice Provisions Under New York Law; • Of Which the Entity's Board is Notified; or • That Involves the Compromise of "Nonpublic Personal Health Information" & "Private Information" as Defined Under New York Law, Payment Card Information or any Biometric Data	In all instances, Global Data Sentinel's notification system provides the capability to notify any party automatically, such as the Department, Company, Department and Company, in any configuration the member corporation requires, depending on whether a corporation elects to notify the Department automatically or elects to be notified and review any notification prior to notifying the Department.

Global Data Sentinel - The Only Single Platform Providing Total Compliance

The First Cyber Security Ecosystem

Our system is comprised of core components that are combined to create the world's first cyber security ecosystem. While it is possible to find platforms that offer single services, like email encryption, no other company provides all of the many components required to run a truly unified cyber security system. With our unified system, there are no multi-vendor compatibility issues, complex pricing questions or multiple relationships to manage. Additionally, our platform satisfies all 25 of the criteria outlined by the NYDFS, which is simply unavailable as a single solution anywhere else.

User Behavior Analytics

Our system actually learns a user's behavior pattern in order to determine what typical user behavior is and what constitutes anomalous activity. Our system collects, correlates and analyzes numerous attributes in order to create a rich dataset that can be used, in real-time, to asses user risk. If our system deems an activity to be a threat, responses can be fully automated without requiring human intervention.

Perfect Forward Secrecy

Not only do we encrypt everything and employ zero-knowledge privacy, we also have a unique encryption key management system that rotates the keys for a much higher level of security than can be found anywhere else.