MAPPING GUIDE

Mapping to the New York State DFS Cybersecurity Regulation

What is the New York State DFS Cybersecurity Regulation?

The New York State DFS Cybersecurity Regulation (23 NYCRR 500) was implemented by the New York State Department of Financial Services (DFS) to help financial services firms doing business in New York minimize their security risks. The regulation was designed to help protect the financial services industry in New York, which represents about 30% of the state's gross domestic product.
Link to the rule: https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

The Rule calls for specific security requirements, including:

- Maintenance of a cybersecurity program
- Written policies and procedures
- Risk assessments
- Monitoring and testing
- Audit trails
- Access controls
- Application security
- Encryption
- Data retention
- Specific hiring and training practices
- Incident response planning

Who is bound by the regulation?

The NYDFS Cybersecurity Regulation covers any organization that is regulated by the New York DFS, including:

- Licensed lenders
- State-chartered banks
- Trust companies
- Service contract providers
- Private bankers
- Mortgage companies
- Insurance companies doing business in New York
- Non-U.S. banks licensed to operate in New York

Institutions are bound by the regulation if they:

- Have more than 10 employees, including contractors, of the covered entity or affiliates located in New York.
- Have more than $5 million in gross annual revenue from New York operations by the covered entity and affiliates in each of the last three years
- Have more than $10 million in year-end total assets, including affiliate assets
- Directly or indirectly operate, maintain, use, or control any information systems

The Rule mandates regulated entities meet certain security standards, including:

- Cybersecurity program
- Audit trails
- Access controls
- Training and monitoring
- Third Party Service Monitoring

Section	Title	Description	Imprivata FairWarning Capabilities
500.02	Cybersecurity Program	The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: • Identify and assess internal and external cybersecurity risks that may threaten the security orintegrity of Nonpublic Information stored on the Covered Entity's Information Systems; • Use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts; • Detect Cybersecurity Events; • Respond to identified or detected Cybersecurity Events to mitigate any negative effects	User access management and audit log monitoring are essential elements of a cybersecurity program. Imprivata FairWarning helps financial services firms detect unauthorized access and mitigate any negative effects associated with this access.
500.06	Audit Trail	Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: • Are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; • Include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity Each Covered Entity shall maintain records required by Section 500.06(a)(1) not fewer than 5 years; and Section 500.06(a)(2) not fewer than 3 years	Imprivata FairWarning helps financial services firms detect and respond to cybersecurity events captured within audit logs. In addition, audit log records are maintained in compliance with the DFS regulation.

Section	Title	Description	Imprivata FairWarning Capabilities
500.07	Access Privileges	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment, each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	Imprivata FairWarning helps financial services firms detect and respond to cybersecurity events captured within audit logs. In addition, audit log records are maintained in compliance with the DFS regulation.
500.11	Third-Party Service Provider Security Policy	Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable: • The identification and risk assessment of Third Party Service Providers; • Minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity; • Due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and • Periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.	Imprivata FairWarning helps financial services firms assess what access third parties have to a covered entities' nonpublic data. With this insight, customers can perform due diligence to enact appropriate access controls over third-party service providers.
500.14	Training and Monitoring	• Implement risk-based policies, procedures, and controls to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, nonpublic information by Authorized users; • Provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment	Imprivata FairWarning helps financial services firms detect unauthorized access or use of/tampering with nonpublic information. Firms can use insights from this monitoring in security awareness training to educate staff on the necessity of proper access and handling of nonpublic data.