Drinker Biddle

NYDFS Regulatory Activity and Corresponding Litigation issues

DrinkerBiddle

Regulation 187: NYDFS Fiduciary/"Best Interest" Proposal

Michael Byrne

Introduction

- “Best Interest” Standard
- Background and Current Protections
- NYDFS Rationale

Timeline and Next Steps

- NYDFS Comment Review Period

- Potential Next Steps

Scope of Proposed Regulation 187

- New York-Based
- Annuity Transactions
- Life Insurance Transactions
- “Transactions” Broadly Defined

Overlap/Conflict with Other Regimes

- Federal Regulations and NAIC Suitability Model
- DOL Current and Future Fiduciary Rule
- SEC and FINRA

Potential Impact of Proposed Regulation 187

- Producer Compensation
- Uncertainty
- Compliance Costs
- Lack of Uniformity / “49 and 1”

DrinkerBiddle

Regulation 210: Life Insurance and Annuity Non-Guaranteed Elements

Bob Mancuso

Purpose of Regulation 210

- Establish standards for the determination and readjustment of non-guaranteed elements
- Ensure policy forms do not mislead policy owners as to the crediting of non-guaranteed amounts or the deduction of non-guaranteed charges
- Ensure policy forms do not contain unjust, unfair, or inequitable provisions

Key Regulation Requirements

- Board Approved Criteria – Section 48.2(a)(1)
- Policy Owner Disclosure – Section 48.3(a)
- Adverse Change Disclosure – Section 48.3(b)
- Adverse Change Filing – Section 48.4(d)
- Adverse Change Annual Reporting – Section 48.4(e)

"Adverse Change" Definition Roadmap

- Adverse Change in the Current Scale of Non-Guaranteed Elements
- Current Scale of Non-Guaranteed Elements
- Non-Guaranteed Element
- Exempt Policy Provision

Policy Owner Disclosure Method Selection

- "An insurer shall provide to a policy owner . . . the current scale of non-guaranteed elements no later than the date of issue, either in the policy, application, illustration of the policy as sold, or a special disclosure document, in a manner that will allow an easy comparison to the corresponding guarantees." Section 48.3(a).

Scope of NYDFS Adverse Change Filing

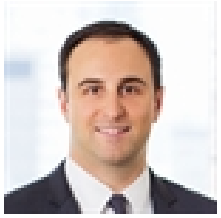
- "An insurer shall file any adverse change in the current scale of non-guaranteed elements applicable to existing life insurance policies or applicable group life insurance certificates with the superintendent at least 120 days prior to implementation."
- Note: This does not include annuities.

The End of the Beginning

- Regulation 210 will take effect on March 19, 2018.
- Adverse Change annual reporting is not required until May 1, 2019.
- On March 3, 2018, NCOIL will be meeting to discuss potentially preparing a model law based upon this NYDFS regulation.

Questions?

H. Michael Byrne
(212) 248-3182
michael.byrne@dbr.com



Robert J. Mancuso
(212) 248-3241
robert.mancuso@dbr.com

DrinkerBiddle

NYDFS – Cybersecurity Regulation

Katherine Armstrong

Regulatory Landscape - fragmented

- Federal Privacy and Data Security Regulations
  - No general federal cybersecurity (or privacy) law
  - Sector specific regulations (FCRA, HIPAA, COPPA)
  - Section 5 of FTC Act (unfair or deceptive acts or practices)
  - SEC – new cyber unit
- State Privacy and Data Security Laws
  - 48 separate state breach notification laws (South Dakota may be 49th)
  - Emergence of state specific data security laws (NYDFS Cyber Security Regs, California financial privacy laws)

Other Regulatory Regimens

- National Association of Insurance Commissioners
  - Model law follows NYDFS law and includes a safe harbor if compliant with NYDFS
  - States likely to adopt
- Outside the US
  - General Data Protection Regulation (Effective May 25, 2018)
    - Robust privacy requirements for any company processing EU Personal Data
    - Data subjects have extensive rights
    - Data security required
    - Massive fines for noncompliance

Cybersecurity Trends

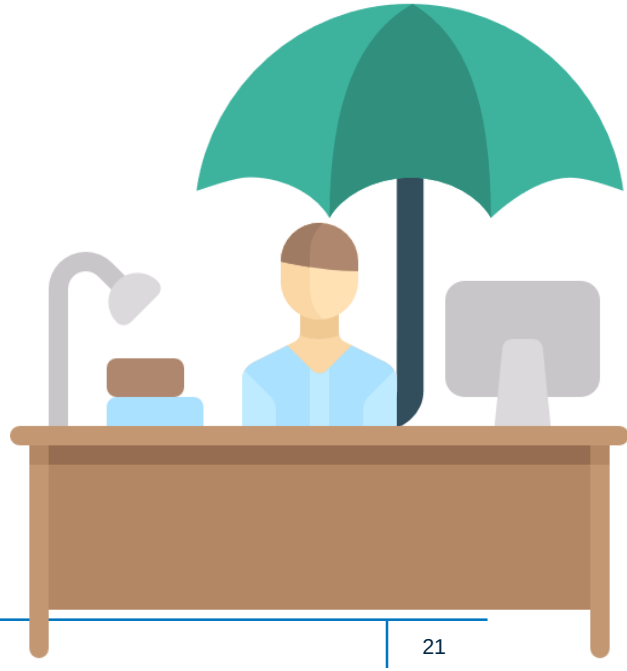
- Data Explosion
  - Amount of electronic data doubling every 18 – 24 months
- Widespread breaches continue
  - Equifax Breach – 143 million records
  - WannaCry – largest international ransomware attack (200,000 computers in over 150 countries)
- Bad guys are really smart

Goals of NYDFS Cyber Regulations

- Promote the proactive protection of sensitive information and IT systems
- Risk-based approach to cybersecurity
- Accountability for cybersecurity by the C-Suite and Board

Who is covered?

- Covered Entities are: “any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.” (500.19(c))
- Subsidiaries and other affiliates
- Whether licensee is a NY resident or not
- Vendors to covered entities



Exemptions

Limited Exemptions

- Covered Entities with
  - Fewer than 10 employees based in NY
  - Less than $5 MM in ross annual revenue in last three FYs from NY operations, or
  - Less than $10 MM in year end total assets
- Covered Entities that do not deal with Information Systems or Handle NPI
- Article 70 Insurers

Full Exemptions

- Insurance Law Section 1110 – Charitable Gift Annuities
- Section 5904 Risk Retention Groups (not chartered in NY)
- 11 NYCRR 125 – Accredited/Certified Reinsurers

Smaller entities

Exempt from:

- Designating a Chief Information Security Officer (500.04),
- Conducting penetration testing and vulnerability assessments (500.05),
- Maintaining an audit trail (500.06),
- Implementing written policies relating to application security (500.08),
- Utilizing qualified cybersecurity personnel and intelligence (500.10),
- Implementing controls such as multifactor authentication (500.12),
- Conducting regular training and monitoring (500.14),
- Implementing controls such as encryption of nonpublic information (500.15), and
- Establishing annual notice and reporting requirements of cybersecurity events to Superintendent (500.16).

Must:

- Maintain a cybersecurity program (500.02),
- Implement a written cybersecurity policy (500.03),
- Limit user access privileges (500.07),
- Conduct period risk assessments (500.09),
- Implement written policies and procedures for third party service providers (500.11),
- Develop information governance policies (500.13), and
- Provide annual notice and report cybersecurity events to superintendent (500.17)

Entities with no Information Systems or NPI

Exempt from:

- Maintaining a cybersecurity program (500.02),
- Implement a written cybersecurity policy (500.03),
- Designating a Chief Information Security Officer (500.04),
- Conducting penetration testing and vulnerability assessments (500.05),
- Maintaining an audit trail (500.06),
- Limiting user access privileges (500.07),
- Implementing written policies relating to application security (500.08),
- Utilizing qualified cybersecurity personnel and intelligence (500.10),
- Implementing controls such as multifactor authentication (500.12),
- Conducting regular training and monitoring (500.14),
- Encrypting NPI, (500.15)
- Maintaining an Incident Response Plan (500.16)

Must:

- Conduct periodic risk assessments (500.09),
- Implement written policies and procedures for third party service providers (500.11),
- Develop information governance policies (500.13)

Step 1: The Path to a Cybersecurity Program (500.02)

- Identify internal and external cyber risks
- Implement defensive infrastructure and policies and procedures
- Detect Cybersecurity event
- Recover from Cybersecurity events
- Fulfill applicable regulatory reporting obligations

Step 2: Comprehensive Cybersecurity Policy (500.03)

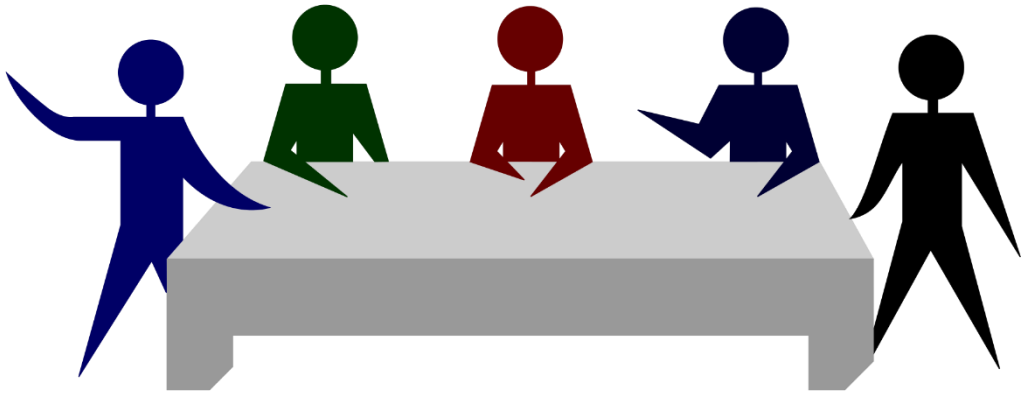
- Information security
- Data governance and classification
- Asset inventory and device management
- Access controls and identity management
- Business continuity and Disaster recovery planning and resources
- Systems and network security
- Systems and network monitoring
- Systems and application development and quality assurance
- Physical security and environmental controls
- Customer data privacy
- Vendor and Third Party Service Provider management
- Risk assessment; and
- Incident response plan

Step 3: The People (500.04, 500.10, 500.14)

- Chief Information Security Officer
  - Maintains principal responsibility for compliance
  - Issues written reports to Board (or equivalent body)
  - Can be employee or third party service provider
- Qualified Cybersecurity Personnel
- Training & Awareness for Employees

Step 4: Involving the Board (500.03, 500.04)

- Approves Comprehensive Cybersecurity Plan
- Reviews Annual CISO Report
- Reviews Risk Assessments
- Signs off on Certifications



Step 5: Technical Controls

- Network monitoring (500.05)
- Encryption of non-public Information (500.15)
- Multifactor Authentication (500.12)
- Access Privileges (500.07)
- Internal Application Security (500.08)
- Audit Trail (500.06)

Step 6: Information Governance

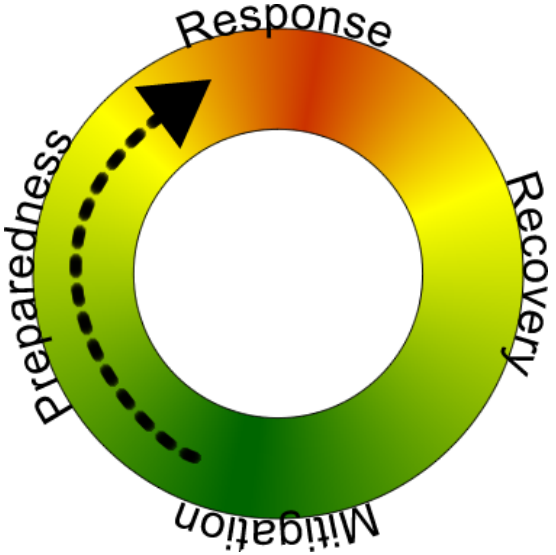
- Limitation on Data Retention
- Recordkeeping and Documentation
- Confidentiality and Information Sharing

Step 7: Vendor Management (500.11)

- External Application Security
- Third party Service Provider Security Policy
  - Covered Entities will have to evaluate vendor risks and include cybersecurity requirements in their agreements (reps and warranties and cybersecurity audit rights)

Step 8: Incident Response Plan (500.16)

- Response Planning
- Corporate Policies and Procedures
- Training and Change Management
- Tabletop Exercises
- Information Sharing Programs
- Vulnerability Reporting Programs



Step 9: Cybersecurity Event Reporting (500.17)

- Report to NYDFS Superintendent within 72 hours of determination that a Cybersecurity Event has occurred that either:
  - Impacts the covered entity of which notice is required by another government agency, or
  - Has a reasonable likelihood of materially harming any material part of the Covered Entity's normal operation

Step 10: Proactive Assessments

- Risk Assessment
- Annual Penetration Testing
- Biannual Vulnerability Assessments

Enforcement

- Enforced by the NYDFS Superintendent
- Broad remedial authority
  - Monetary penalties
  - Injunctive relief (e.g. possible revocation of a license), and
  - Orders requiring corrective action
- Superintendent can also conduct audit examinations of Covered Entities and Inspect recordkeeping
- Cybersecurity program may be a factor in license renewal

Deadlines

- August 28, 2017
  - Cybersecurity program, Cybersecurity policy, Access privileges, Incident Response Plan,
- February 15, 2018
  - First annual certification of compliance
- March 1, 2018
  - CISO report to board, Penetration testing and vulnerability assessment, Risk Assessment, Multi-factor authentication, Cyber training
- September 3, 2018
  - Encryption, Data retention policies, Policies and procedures for monitoring activity, Application security, Audit Trail
- March 1, 2019
  - Third party service provider oversight

Filing mechanics

- Cybersecurity Notices of Exemption should be filed electronically via the DFS Web Portal http://www.dfs.ny.gov/about/cybersecurity

Some areas of uncertainty

- Impact on non NYFDS affiliates, service providers
- Application of exemptions
- What will be the first targets

Bottom line – relevant for all businesses

- Know your company's data environment
- Encrypt NPI
- Engage in employee cybersecurity training
- Be aware of existing compliance obligations, especially if license renewal is approaching
- Deploy innovative products and services by thinking about privacy (and security) holistically in order to avoid reputational harm and retain consumer trust
- Rinse and Repeat

We end where we began

- Fragmented regulatory environment
- Trend toward cyber regulation
  - Numerous bills in congress
  - Likely impact on sensitive information
- Consumer Trust and Business Reputation

Learn More: DBR on Data

The Information Privacy, Security and Governance Steering Committee (IPSG), spanning multiple practice groups across the firm, provides insights about how to best harness, manage and utilize data assets. Blog posts cover developments in privacy, cybersecurity, information governance, data analytics, data breaches, state and federal security measures and many more topics, demonstrating the wide-reaching effects of data management in the global economy.

Visit us online: dbrondata.com

DrinkerBiddle

Questions?

Katherine E. Armstrong
(202) 230-5674
katherine.armstrong@dbr.com

Drinker Biddle

DFS Circular Letter No. 1 (2017) Contestable Claims

Jason P. Gosselin

Contestable Claim Process

- Policy Requirement
  - "[T]he policy shall be incontestable after being in force during the life of the insured for a period of two years from the date of issue." New York Ins. Law § 3203(a)(3).

Permissibility of Routine Contestable Investigations

- DFS has learned that some insurers “have contested numerous life insurance claims following the death of the insured during the two-year contestable period, in the absence of actual evidence of misrepresentation, and improperly have shifted the burden of proof to beneficiaries.”

Permissibility of Routine Contestable Investigations

- "Insurers are advised that ***any business practice*** by an insurer that, ***absent any evidence of a material misrepresentation,*** requires a beneficiary to furnish claim information, including medical records, so that an insurer may investigate whether an applicant made a misrepresentation when applying for life insurance, is ***not attempting to effectuate prompt, fair, and equitable settlements of claims in good faith***."

Permissibility of Routine Contestable Investigations

- *Minn. Mut. Life Ins. Co. v. Ricciardello*, No. 3:96CV2387 (AHN), 1997 WL 631027, at *2 (D. Conn. Sept. 17, 1997) ("The contestability period is a fixed span of time (here two years) after the policy issues. If death occurs within that period, the insurer may perform an investigation to determine whether the insured made a material misrepresentation on the application that might give rise to the right to contest coverage.")
- *Downs v. River City Grp., LLC*, No. 3:11-cv-00885-LRH-WGC, 2013 WL 4506141, at *3 (D. Nev. Aug. 22, 2013) ("contestability investigations are routine" and are "a customary practice in the insurance field")

Duty to Cooperate?

- "[A] beneficiary has no legal obligation to cooperate with an insurer by providing the insurer with the deceased insured's medical records."

Duty to Cooperate

- Duty of Good Faith Implied In Every Contract
  - *511 W. 232nd Owners Corp. v. Jennifer Realty Co.*, 98 N.Y.2d 144, 153 (N.Y. 2002) ("All contracts imply a covenant of good faith and fair dealing in the course of performance.")

Right to Commence Legal Action

- "While an insurer in this circumstance has the right to bring a legal action to rescind an insurance contract, an insurer may not unilaterally refuse to pay a life insurance claim unless the insurer has actual proof that the applicant made a material misrepresentation when applying for the life insurance policy."

Impact of Circular Letter

- Suspicion of misrepresentation often apparent
- Beneficiaries typically willing to cooperate
- Right to obtain information through legal process

Questions?

Jason P. Gosselin
(215) 988-3371
jason.gosselin@dbr.com