Financial Services 2024 Privacy and Cybersecurity Preview

Gregory P. Szewczyk
Partner
Privacy and Data Security
303.299.7382
szewczykg@ballardspahr.com

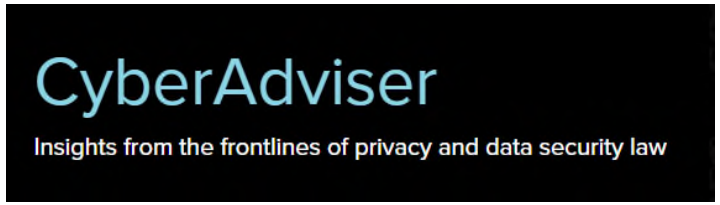
Sarah Dannecker
Associate
Privacy and Data Security
612.371.6209
danneckers@ballardspahr.com

February 1, 2024

Ballard Spahr LLP

Resources

Consumer Finance Monitor
Subscribe to our ABA award-winning blog at
http://www.consumerfinancemonitor.com



CyberAdviser
Subscribe to award-winning our blog at
https://www.cyberadviserblog.com

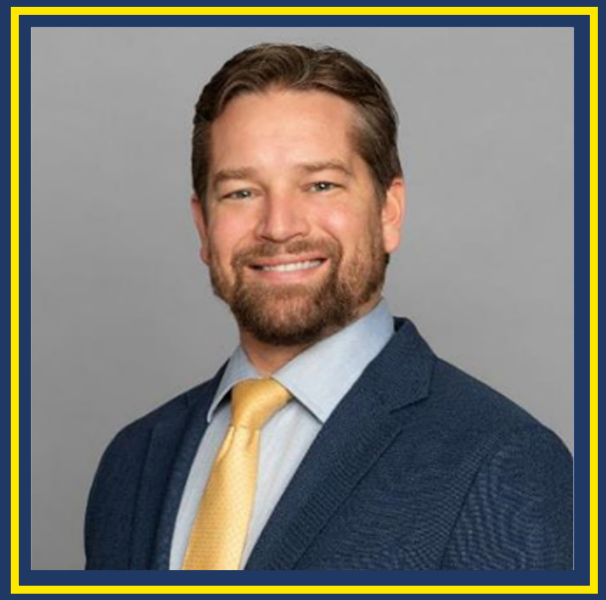
Consumer Finance Monitor Podcast
Available on ballardspahr.com, Apple iTunes, Google Play, Spotify, or your favorite podcast app. For more information, click here.

Upcoming Webinar: **The Federal Trade Commission: Looking Back at 2023 and Looking Ahead to 2024 and Beyond Feb. 28, 2024 2:00-3:00 PM ET Register Here**

Featured Podcasts: **Understanding the Federal Reserve Board Proposal to Lower Interchange Fee Cap for Debit Card Transactions Listen Here**

Will Chevron Deference Survive in the U.S. Supreme Court? An Important Discussion to Hear in Advance of the January 17th Oral Argument Listen Here

Ballard Spahr Attorneys



Gregory P. Szewczyk

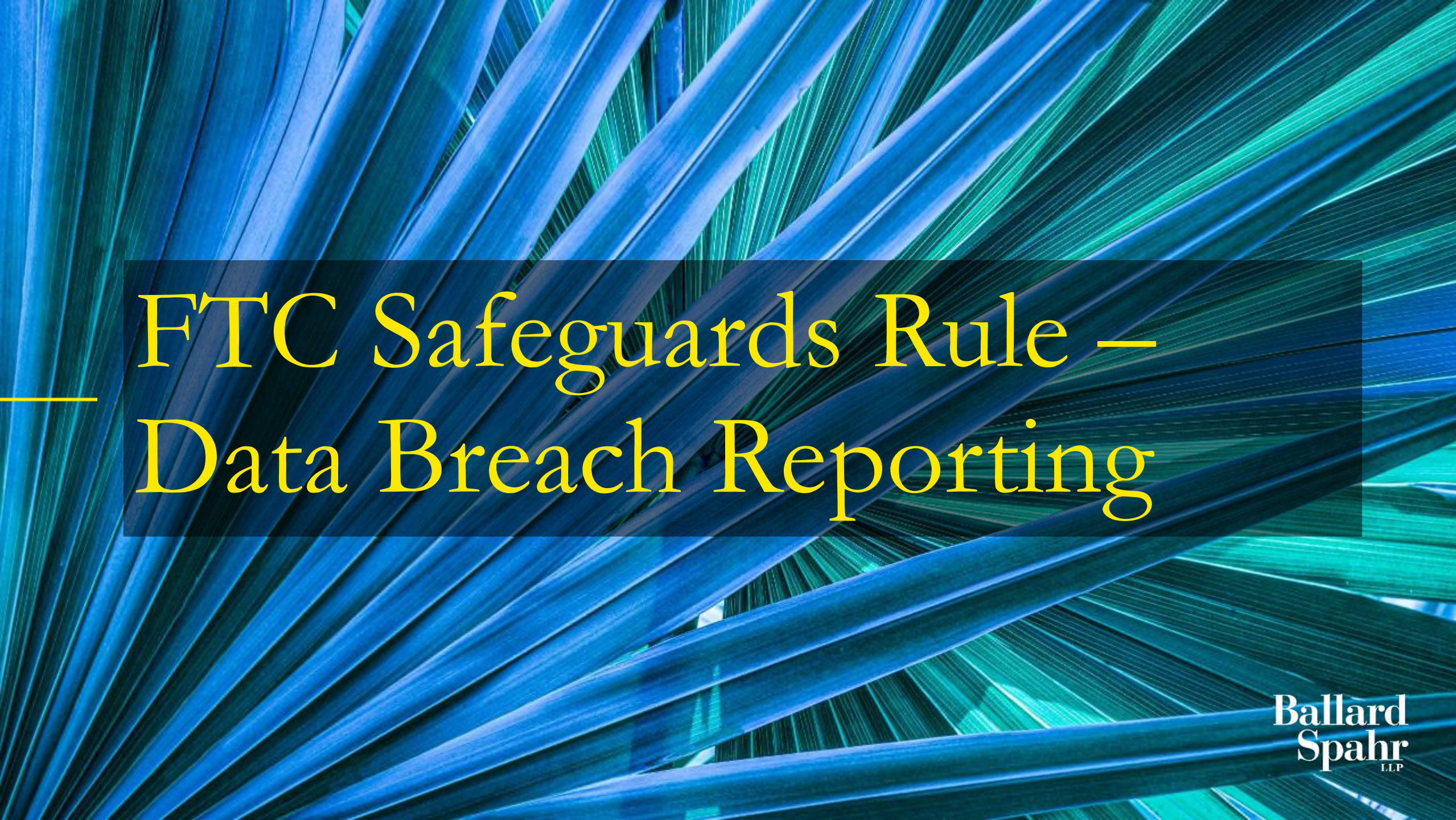
Partner

Sarah B. Dannecker

Associate

Agenda

- FTC Safeguards Rule – Data Breach Reporting
- SEC Cyber Incident Reporting
- CFPB Personal Financial Data Rights Rule
- NYDFS Cybersecurity Requirements – Financial Services Companies
- Artificial Intelligence and Cyber Policies


FTC Safeguards Rule –
Data Breach Reporting
Ballard
Spahr
LLP

Background

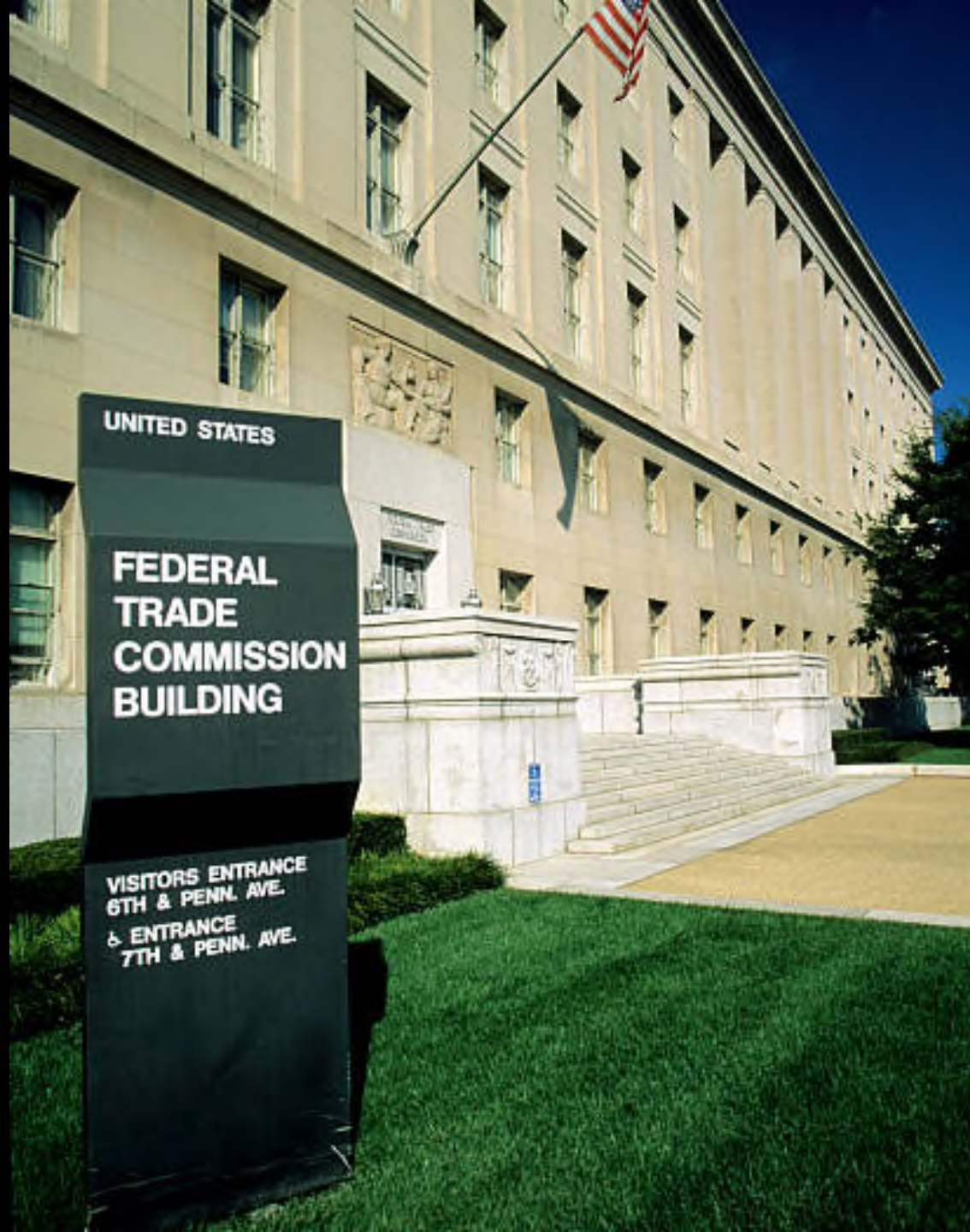
- FTC Safeguards Rule requires “financial institutions” to implement and maintain security programs to safeguard customer information

- October 2021 – FTC finalized changes to Safeguards Rule to strengthen data security requirements for financial institutions

- As part of the October 2021 changes, FTC sought comments on supplemental amendment to require data breach reporting

Amendment to FTC Safeguards Rule

- October 27, 2023 - FTC announced amendment to Safeguards Rule requiring financial institutions to report certain data breaches (effective May 13, 2024)
- Requirements:
  - ✓ Security breaches involving unencrypted data of 500 consumers or more
  - ✓ Report to FTC no later than 30 days after discovery
  - ✓ Notice must include number of consumers affected or potentially affected




SEC Cyber Incident Reporting
Ballard Spahr LLP

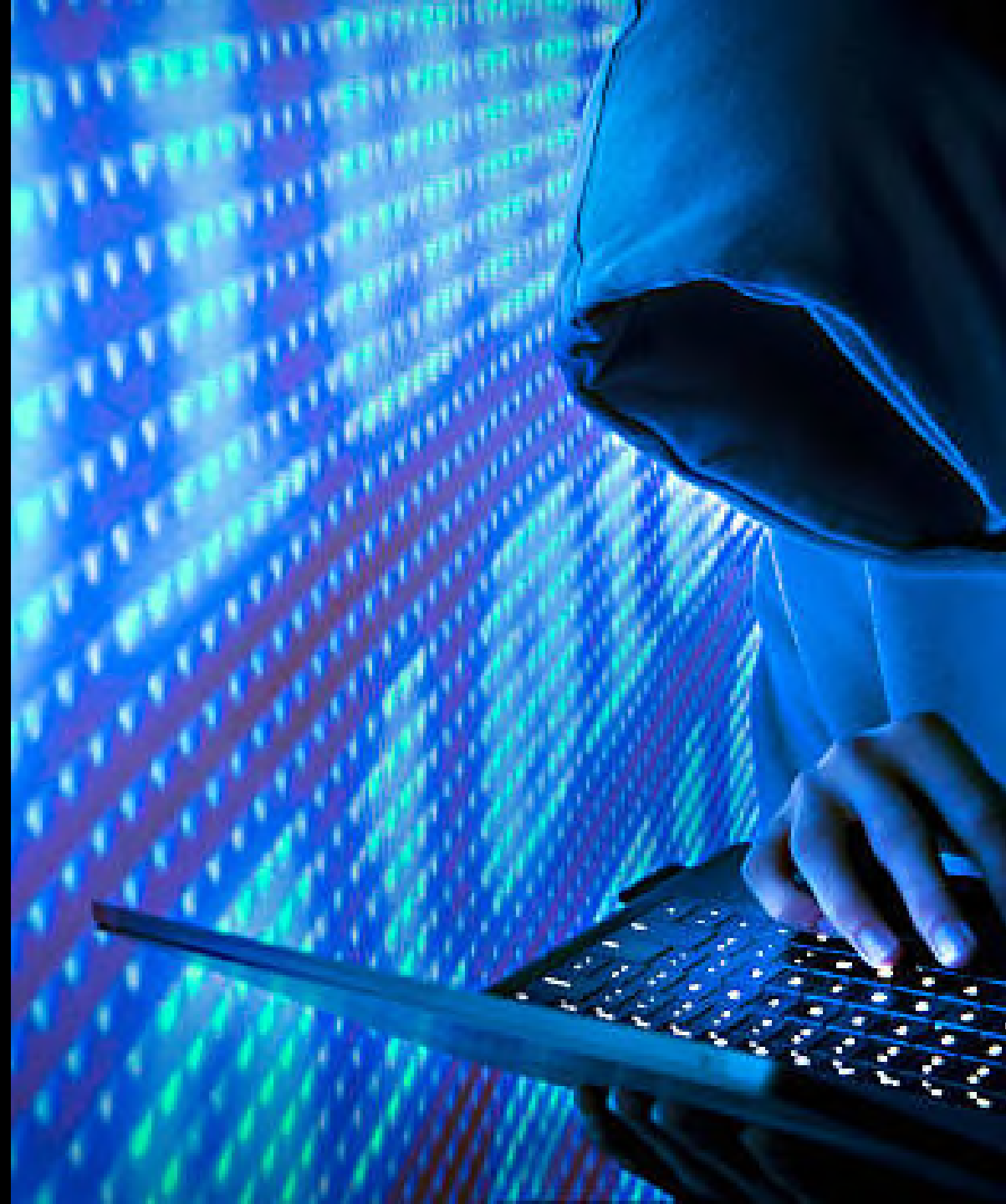
SEC Cyber Incident Reporting Rules

Public Companies

- SEC adopted final rule on July 26, 2023 requiring public disclosure of material cybersecurity incidents
- Requirements:
  - Reporting within “real time” (i.e., 4 days of materiality determination) for covered companies (Form 8-K / Form 6-K for foreign private issuers)
  - Additional cyber disclosures in annual reports (Form 10-K / Form 20-K for foreign private issuers)
    - Cyber risk management and strategy
    - Board oversight and relevant cybersecurity expertise
- Effective September 5, 2023

Unintended consequences of SEC Rule?

- MeridianLink / ALPHV/BlackCat
- Ransomware group filed complaint with SEC against its own victim, MeridianLink, for failing to disclose “significant” cybersecurity breach in Form 8-K
- MeridianLink issued statement that no user data was breached
- Weaponizing SEC rule for ransomware negotiations



CFPB Personal Financial Data Rights Rule

Ballard Spahr LLP

Scope of Proposed Rule—Covered Persons

Data Providers: Any person offering any financial produce or service that is:

1. A financial institution under Regulation E
2. Card issuers under Regulation Z
3. "Any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person"

*CFPB has indicated intent to broaden scope through future rulemaking

Third Parties: "any person or entity that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data"

- Authorized Third Party: a third party that complies with the authorization procedures in the Proposed Rule
- Data Aggregator: an entity that is retained by and provides services to the authorized third party to enable access to covered data

Summary of CFPB Proposed Rule 1033

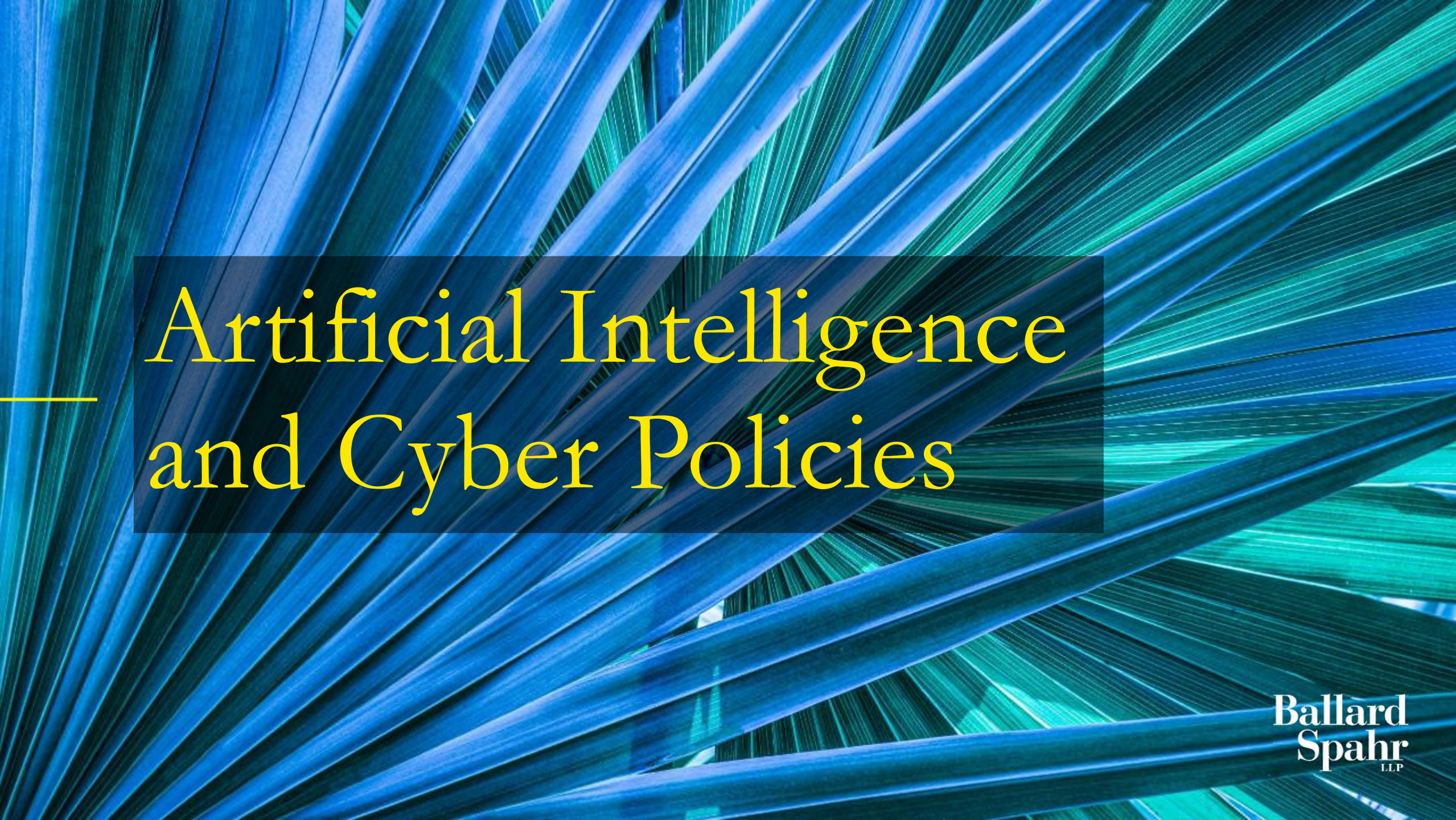
- Grants data access rights to consumers and third parties
    - Including data portability component
- Requires consumer and developer interfaces
- Limits use of covered data by third parties to what is reasonably necessary
- Expands scope of GLBA Safeguards Rule

NYDFS Cybersecurity Requirements

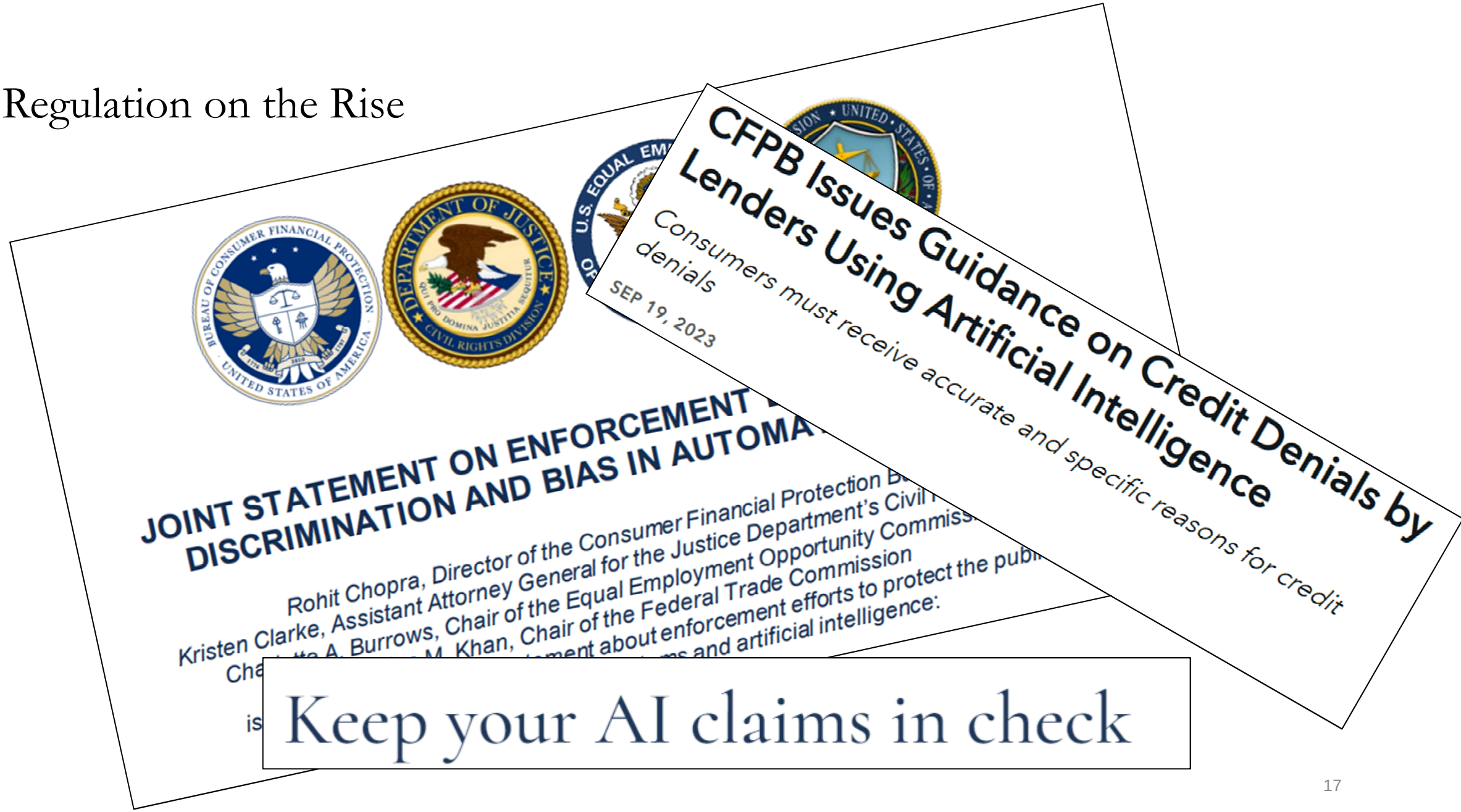
Ballard Spahr LLP

Amendment to Cybersecurity Regulation

- New classes of companies
- Expanded incident reporting requirements
- Additional security requirements
  - MFA
  - Written policies
  - Training


Artificial Intelligence
and Cyber Policies
Ballard
Spahr
LLP

Regulation on the Rise



Best Practices for Development of Use of AI

Track Regulation

- Comprehensive privacy laws covering AI
- AI specific laws
- Specific laws and regulations
- Standards

Develop AI Governance Programs

- Leverage existing Privacy & Data Security programs
- Assess risks
- Assign management responsibilities
- Ensure board reporting

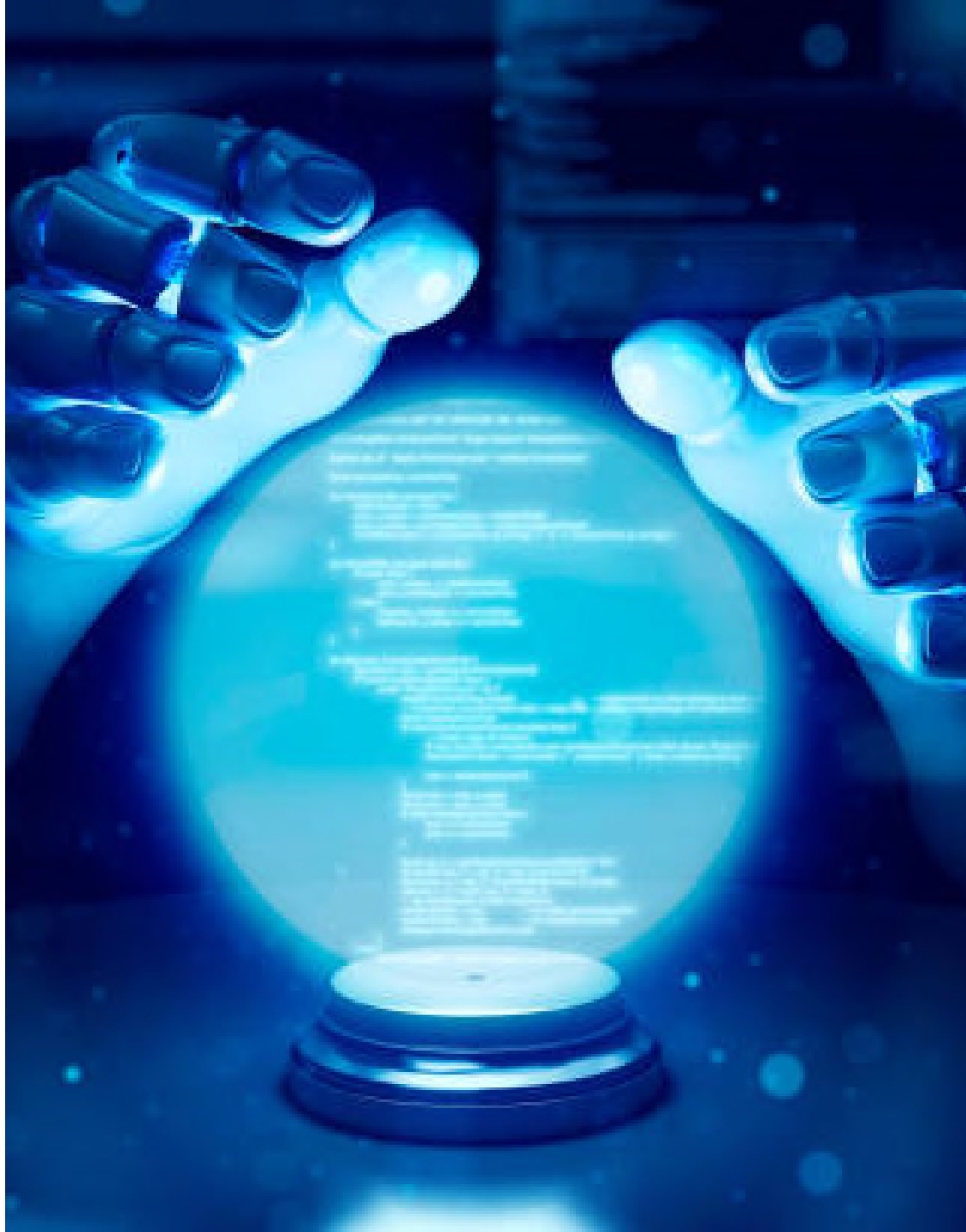
Vendor Management

- Contracting
- Cross border transfer
- Understanding data usage


Final Thoughts
Ballard
Spahr
LLP

Final Thoughts

- Predictions for the remainder of 2024 and beyond
  - State
    - Proposed revisions to CCPA regulations
  - Federal
    - Harmonized cybersecurity regulations?
    - The Office of the National Cyber Director (ONCD) seeking comments
  - AI – continuing regulatory scrutiny and compliance issues



Thank you for watching!

Gregory P. Szewczyk
Partner
Privacy and Data Security
303.299.7382
szewczykg@ballardspahr.com

Sarah Dannecker
Associate
Privacy and Data Security
612.371.6209
danneckers@ballardspahr.com

Ballard Spahr LLP

Gregory P. Szewczyk

- Greg Szewczyk is a partner in Ballard Spahr's Denver and Boulder offices and the Practice Leader of the Privacy and Data Security Group
- A lawyer who leverages over a decade of experience in high stakes litigation to help companies assess risk and comply with the ever expanding patchwork of state, federal, and international privacy and data security statutes and regulations
- Helps companies of all sizes, from Fortune 500s to start ups, build and maintain their privacy and data security programs
- He has advised hundreds of companies on various compliance issues—from the use of artificial intelligence to vendor management to routine data processing matters that arise in day-to-day business—relating to the Colorado Privacy Act (CPA), the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standards (PCI DSS), the Illinois Biometric Information Privacy Act (BIPA), the Gramm-Leach-Bliley Act (GLBA), state financial privacy laws, the Telephone Consumer Privacy Act (TCPA), and various other laws and regulations
- He advises clients in connection with corporate transactions, such as mergers, acquisitions, and partnerships. In doing so, he helps his clients assess the potential risks involved and develop creative solutions to data issues. Greg has advised clients in data breach response, including breaches impacting consumers in all 50 states and internationally. Greg also has defended companies facing data breach and privacy class actions, and has represented companies in business-to-business litigation stemming from data incidents and the alleged misuse of data, including issues involving artificial intelligence
- Accredited by the International Association of Privacy Professionals as a Certified Information Privacy Professional / United States (CIPP/US)
- Regularly quoted in periodicals such as Bloomberg. Prior to joining Ballard Spahr
- Greg was an associate at Simpson Thacher & Bartlett LLP in New York. During law school, Greg served a legal internship with the U.S. Army Judge Advocate General Corps

Sarah B. Dannecker

Sarah Dannecker is an associate in the Privacy and Data Security Department. She has experience representing clients with privacy and data security laws and regulations in areas such as the General Data Protection Regulation (GDPR), the Gramm Leach Bliley Act (GLBA), and the California Consumer Privacy Act (CCPA).

Sarah has also assisted companies with data breach investigations and responses and researches and prepares multi-state surveys and analyses relating to banking and privacy laws.

Prior to joining the firm, Sarah worked as a patent prosecution paralegal at a national intellectual property firm and as a contracts manager in the legal department for a global water and energy company.