BANKING THE FINTECHS

BAAS, BANK PARTNERSHIPS, AND EMBEDDED FINANCE

MAYER|BROWN

DAVID
Beam

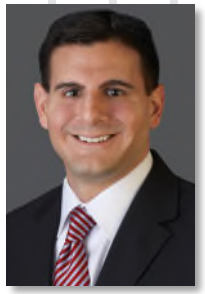
Partner
202 263 2275
dbeam@mayerbrown.com

CORINA
Cercelaru

Associate
312 701 7464
ccercelaru@mayerbrown.com

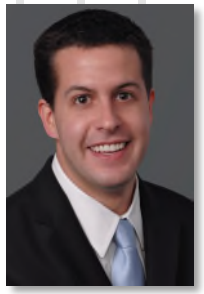
JUSTIN
Herring

Partner
212 506 2878
jherring@mayerbrown.com



THOMAS
Panoff

Partner
312 701 8821
tpanoff@mayerbrown.com



JOE
Pennell

Partner
312 701 8354
jpennell@mayerbrown.com

DOMINIQUE
Shelton Leipzig

Partner
213 229 5152
dsheltonleipzig@mayerbrown.com

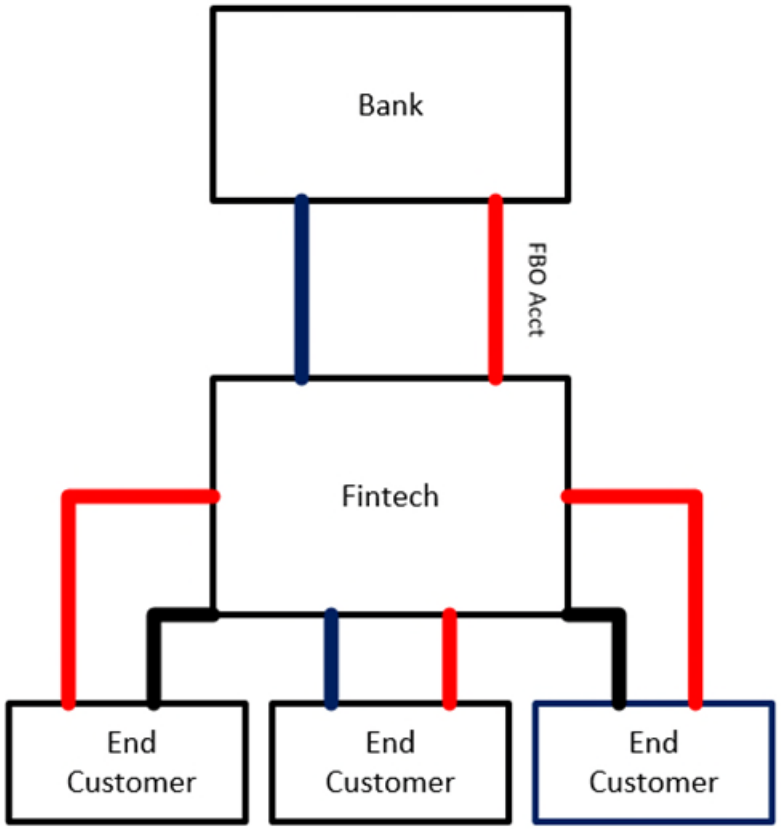
AGENDA

TIME	DURATION	TOPIC AND SPEAKER
1:00 – 1:30	**30 min**	**Overview** *David Beam*
1:30 – 1:55	**25 min**	**Privacy and Data Protection** *Dominique Shelton Leipzig*
1:55 – 2:25	**30 min**	**Key Issues in Contract Negotiations** *Joe Pennell & Corina Cercelaru*
2:25 – 2:35	**10 min**	**B R E A K**
2:35 – 3:05	**30 min**	**Allocating Responsibility for Regulatory Compliance** *David Beam*
3:05 – 3:30	**25 min**	**Litigation & Antitrust** *Thomas Panoff*
3:30 – 4:00	**30 min**	**Artificial Intelligence Contracting Issues** *Joe Pennell & Corina Cercelaru*
4:00 – 4:10	**10 min**	**B R E A K**
4:10 – 4:30	**20 min**	**Board-Level Issues (Including in relation to AI)** *Dominique Shelton Leipzig*
4:30 – 5:00	**30 min**	**Supervisory Expectations and Perspectives** *Justin Herring*

OVERVIEW

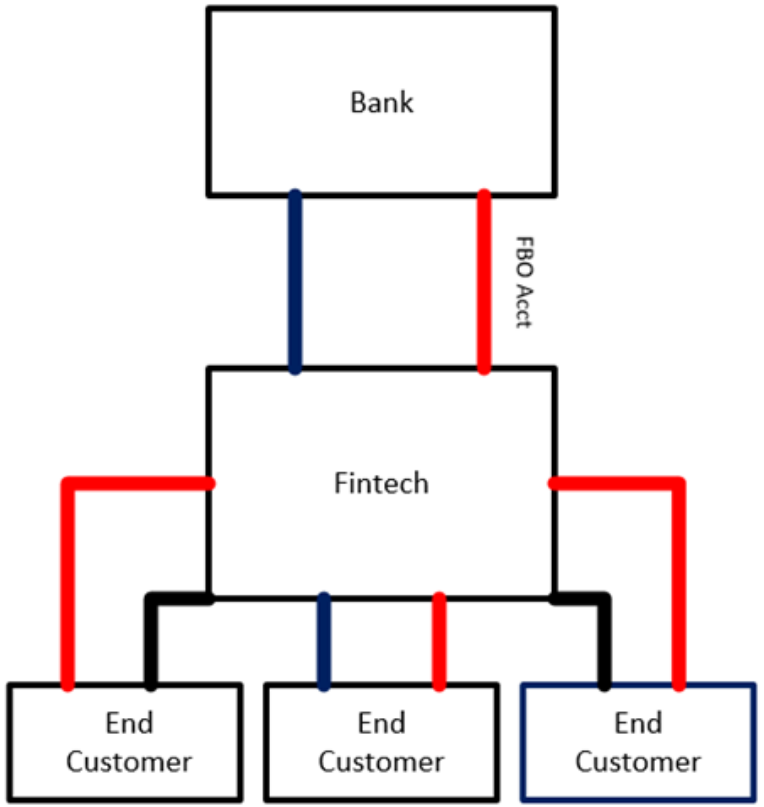
Traditional FBO Model

- Acct Title: "Fintech FBO End Customers"
- Fintech keeps all records of individual end customer balances, etc.



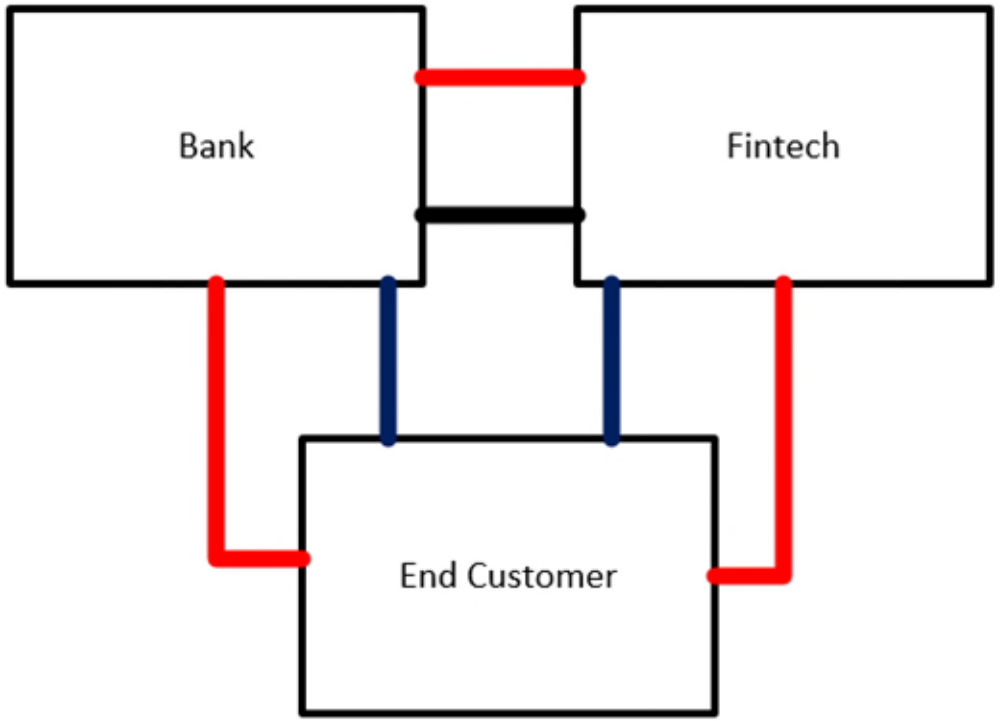
Bank FBO Fintech Model

- Acct Title: "Bank FBO Fintech"
- Fintech keeps all records of individual end customer balances, etc.

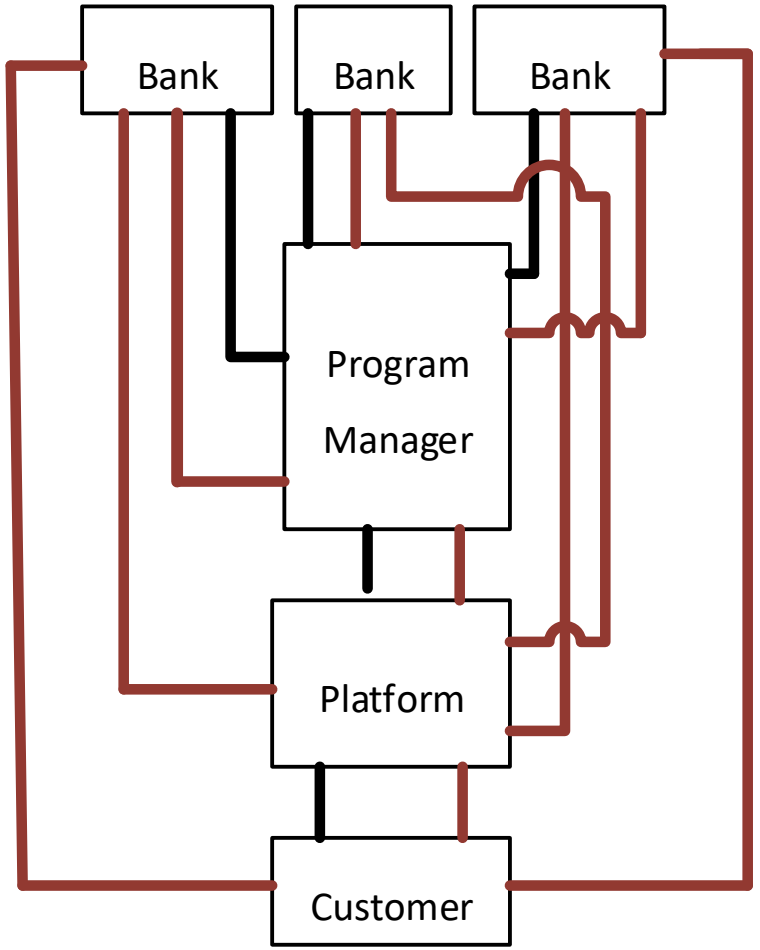


BaaS Direct Model

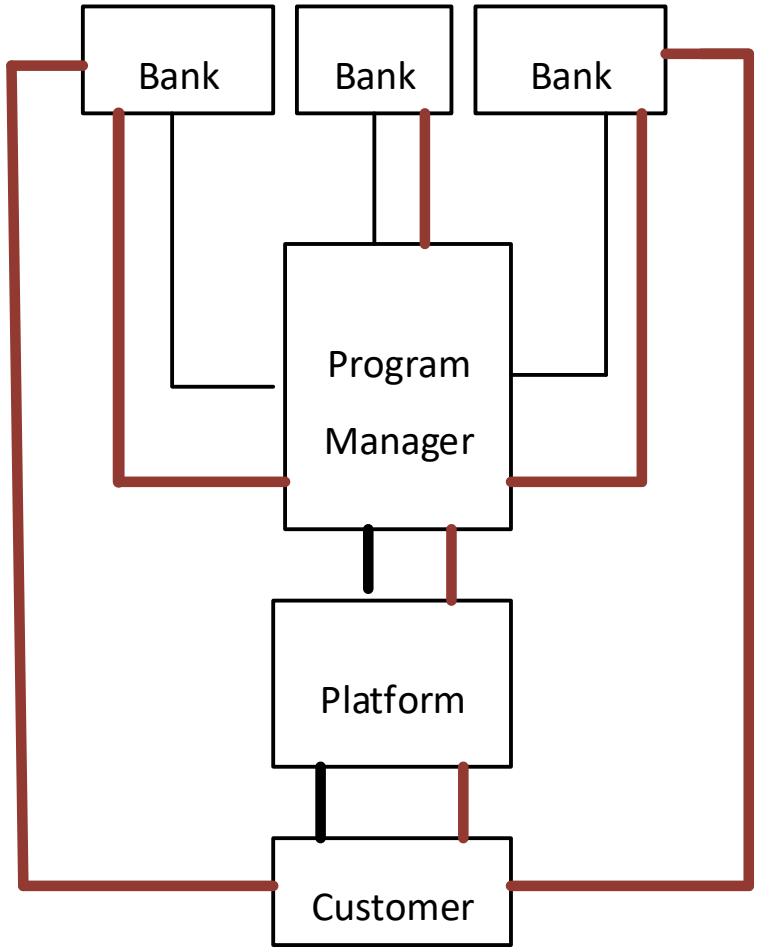
- End customer accounts may be individual DDAs or subaccounts of an FBO acct ("Bank FBO End Customers")



BaaS Program Manager Model #1



BaaS Program Manager Model #2



Related Content

MAKING SENSE OF BANKING AS A SERVICE – CONTRACTING CONSIDERATIONS

HTTPS://WWW.MAYERBROWN.COM/EN/PERSPECTIVES-EVENTS/PUBLICATIONS/2022/01/MAKING-SENSE-OF-BANKING-AS-A-SERVICE-CONTRACTING-CONSIDERATIONS

PRIVACY AND DATA PROTECTION

KEY ISSUES IN CONTRACT NEGOTIATIONS

Overview of Key Contractual Issues

- Control Over the Customer Relationship
- Data Ownership, Use and Restrictions
- End Customer Eligibility, Underwriting and Fraud
- Allocation of Intellectual Property Rights
- Service Quality
- Change Control
- Fintech Financial Issues
- Post-Termination Issues
- Other Key Contractual Issues

Control Over the Customer Relationship

WHICH PARTY CONTROLS THE END CUSTOMER RELATIONSHIP?

Commercial perspective – typically, the Fintech has the primary relationship with the End Customer (e.g., through the Fintech's platform)

Regulatory perspective – End Customers of BaaS products will always be a bank's End Customers

ALLOCATION OF CONTROL DIVIDED INTO SEVERAL CATEGORIES, INCLUDING:

- Servicing
- Exclusivity
- Cross-marketing rights
- Post-termination rights

Data Ownership

- Weak intellectual property protections for data
- Rights (and limitations) on data use are best defined by contract
- Challenges in defining the categories of data before negotiating contractual rights and obligations that apply to those categories:
  - √ Access/Login Credentials
  - √ Personal Data
  - √ Banking Data
  - √ Other Confidential Information
- Avoid getting bogged down by ownership issues

Data Use and Restrictions

- Use rights with respect to the other party's data
  - ✓ Solely to perform a party's obligations under the agreement
  - ✓ Rights to improve products and services
  - ✓ Anonymized and aggregated data
  - ✓ Rights to use overlapping data within terms of End Customer contract and applicable law
- Mitigating risk
  - ✓ Contractual obligations
  - ✓ Indemnities and limitations of liability
  - ✓ Operational mitigants

End Customer Eligibility, Underwriting and Fraud

- End Customers may not meet Bank Eligibility or Underwriting Criteria (including ESG policies)
  - ✓ Who bears the risk of claims from End Customers?
- Are the Platform's controls sufficient?
- If not, can the Platform commit to implement improved controls?
- Which party (a) has responsibility for Login Credentials and (b) bears the risk of fraud?
  - ✓ Did the Fintech comply with fraud controls?
  - ✓ Did the Bank pay out an End Customer claim when not strictly required by applicable law?

Intellectual Property (IP) Rights in BaaS Deals

Intellectual property rights in the following components:

- IT systems and data
  - ✓ Bank / Fintech proprietary systems
  - ✓ APIs
  - ✓ User interfaces / “look and feel”
- Documentation
- Know-how, insights / feedback
- Branding

IP Ownership / Licensing Trends in BaaS Deals

- Parties retain ownership of their IP
- IP licenses granted to parties by third party service providers
- Some IP (including third party IP) may be licensed by one party to the other, to enable provision of service
- IP created but specific to one party, may be assigned to that party, with cross-licensing

Joint IP Ownership

Joint ownership is best avoided because of the logistical problems and challenges it may create:

- Different default rules for jointly owned IP rights across the globe.
- Added legal and administrative costs, since ability to exploit and enforce the jointly owned IP rights otherwise must be handled contractually.
- One owner may enforce without consent and risks triggering counterclaims. In some cases, both owners must join infringement suits.
- Warranties typically require full ownership.
- Challenge for an entity's tax advisors to value jointly owned IPR.
- One co-owner may want to sell or is taken over, e.g., by a competitor.

Service Quality

- Reliability and performance of the Platform can significantly impact End Customer's satisfaction and Bank's reputation
- **Mitigating risk:**
  - ✓ Identify potential pain points
  - ✓ Investigate and align on UAT process for platform changes
  - ✓ Service level requirements
  - ✓ Termination rights

Change Control

- Changes to the financial products: establish a clear process
- Changes to the platform:
  - ✓ Concern that the Bank may have little control over development and evolution of the Platform and End Customer experience
- **Mitigating risk**:
  - ✓ Identification of key End Customer experience elements
  - ✓ Visibility into upcoming changes
  - ✓ Special treatment for critical changes
  - ✓ Participation in key partner forums
  - ✓ Termination rights

Fintech Financial and Business Stability

- The financial and business stability of the Fintech is key due to the Bank's reliance on the Platform for delivery of critical services to End Customers
- **Mitigating risk:**
  - ✓ Visibility into the Fintech's financial performance
  - ✓ Termination rights if financial metrics or credit ratings fall below defined thresholds
  - ✓ Investigate business continuity and disaster recovery plans

Post-Termination Issues

- Platform Lock-In: the Bank may become dependent on the Platform, making it difficult to switch to a different Fintech or revert to in-house operations
- Which party retains the End Customer relationship?
- **Mitigating risk**:
  - ✓ Plan for exit before entrance: robust disengagement services provisions
  - ✓ Specify procedures for sunsetting or transitioning services

Other Contractual Key Issues

- Governance of the parties' relationship
- Audit rights
- Termination rights
- Other liability provisions

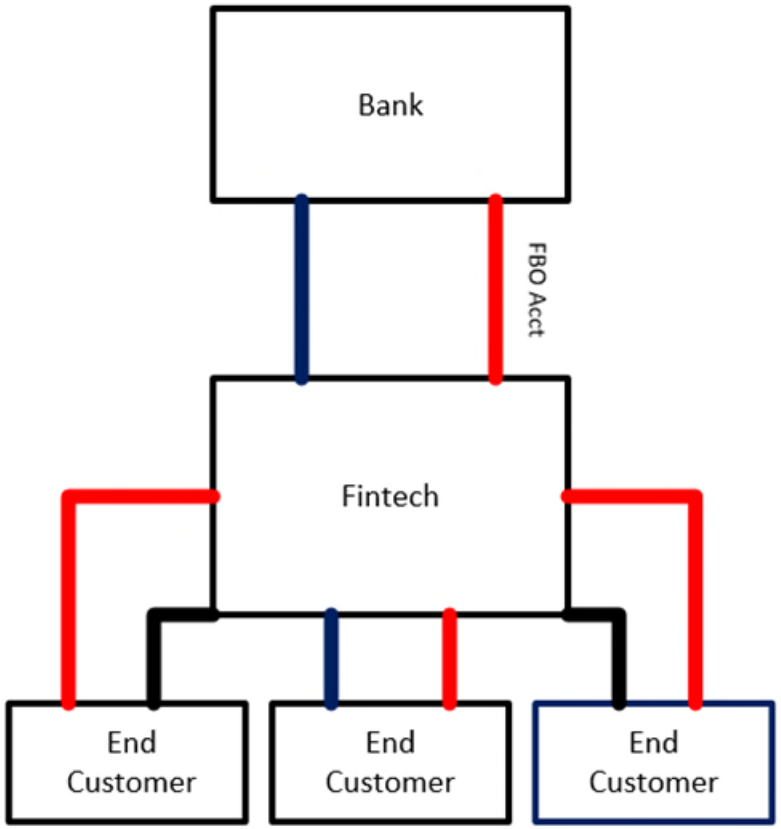
QUESTIONS?


Statistic Graph
ON
00:04:12
ON
LOREM IPSUM
EXE
00:00:12
WARNING
00:01:21
b/0

ALLOCATING RESPONSIBILITY FOR REGULATORY COMPLIANCE

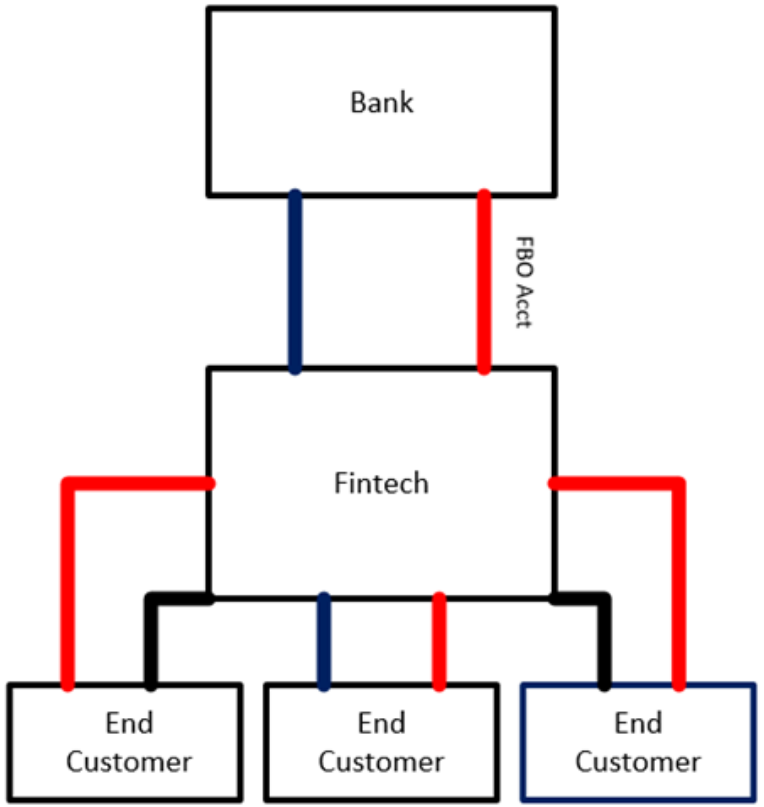
Traditional FBO Model

- Acct Title: "Fintech FBO End Customers"
- Fintech keeps all records of individual end customer balances, etc.



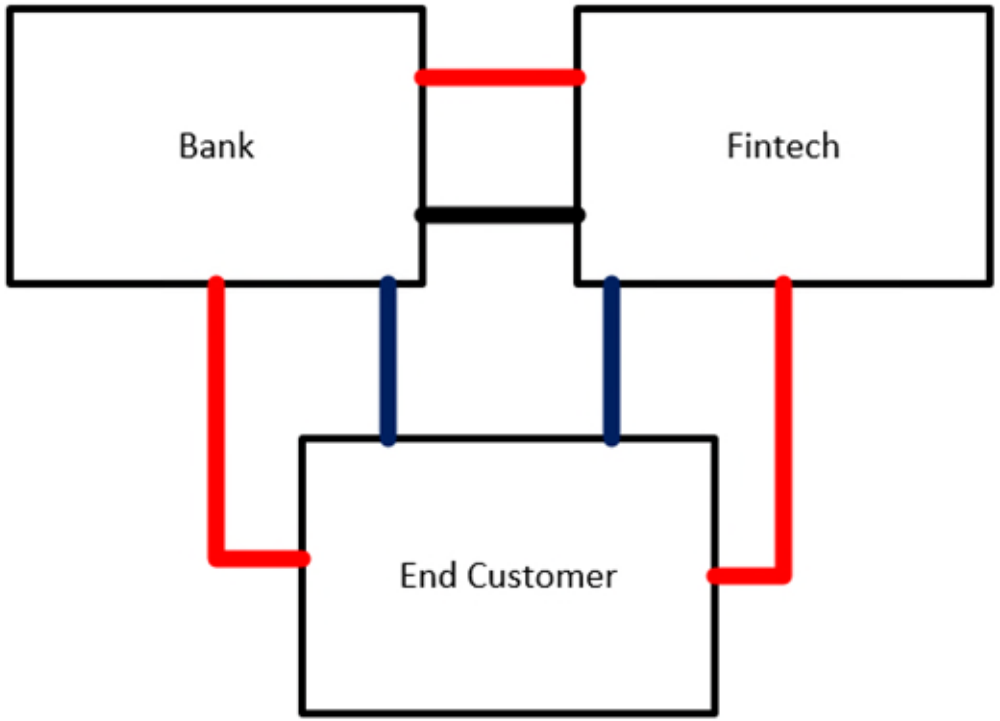
Bank FBO Fintech Model

- Acct Title: "Bank FBO Fintech"
- Fintech keeps all records of individual end customer balances, etc.

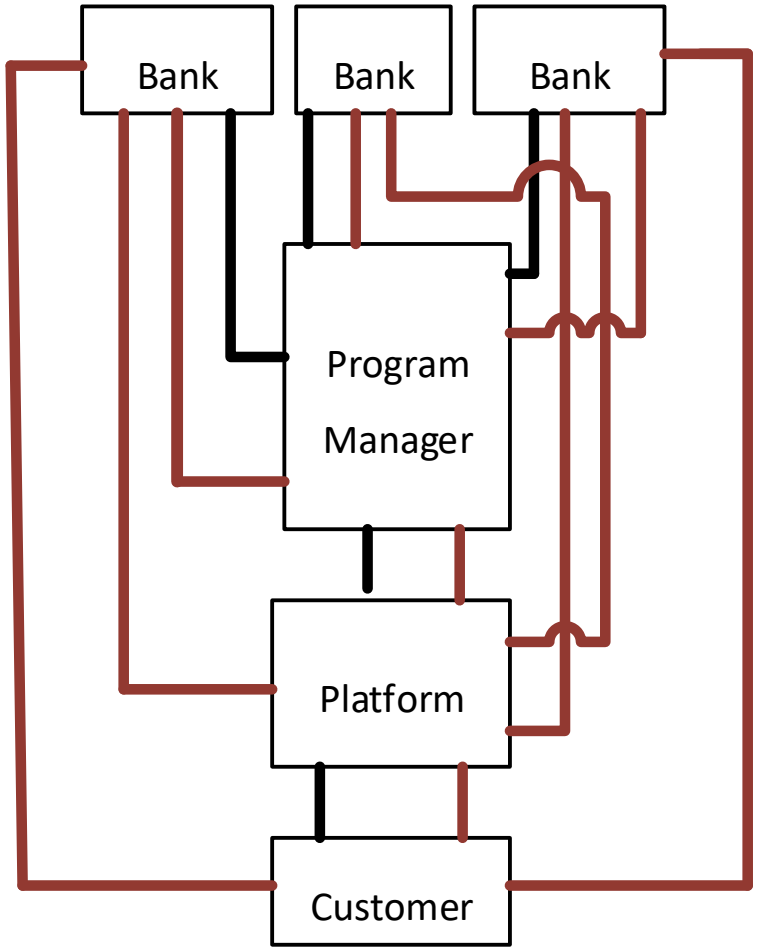


BaaS Direct Model

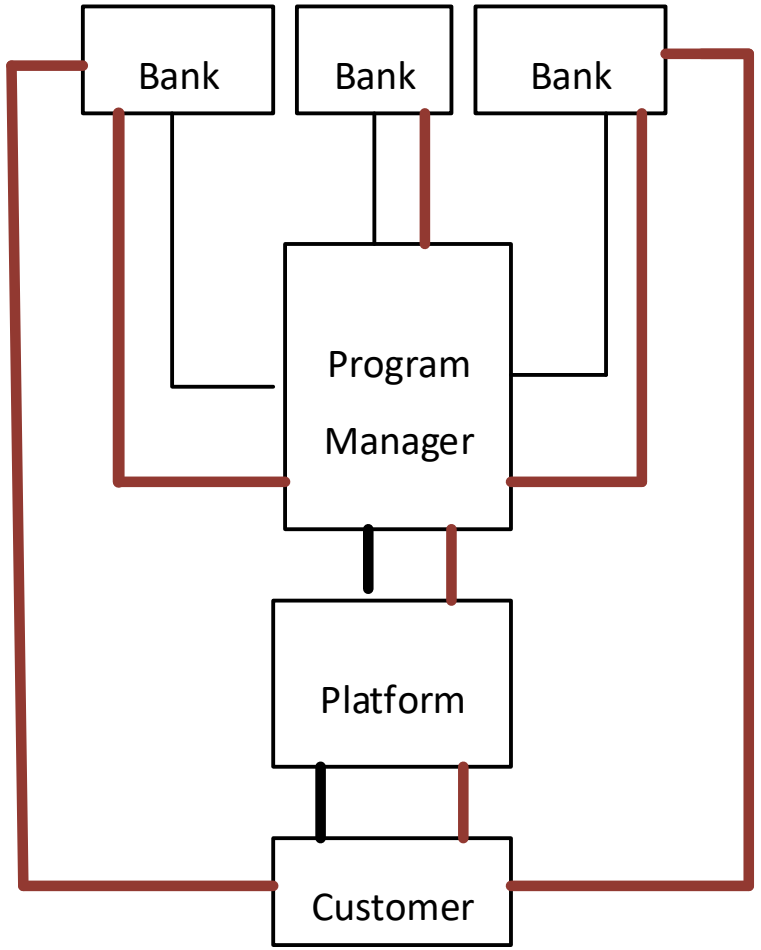
- End customer accounts may be individual DDAs or subaccounts of an FBO acct ("Bank FBO End Customers")



BaaS Program Manager Model #1



BaaS Program Manager Model #2



Related Content

US TREASURY REPORT ADDRESSES IMPACT OF FINTECH-BANK PARTNERSHIPS

HTTPS://WWW.MAYERBROWN.COM/EN/PERSPECTIVES-EVENTS/PUBLICATIONS/2022/12/US-TREASURY-REPORT-ADDRESSES-IMPACT-OF-FINTECH-BANK-PARTNERSHIPS

LITIGATION & ANTITRUST

Areas of Exposure

Litigation & Dispute Risk

- Antitrust & Competition
- Consumer Litigation / Class Actions
- Governmental / Regulatory Litigation
- Partner / B2B Disputes

Antitrust & Competition - Background

	US	EU	UK
Prohibition of restrictive agreements/ arrangements	§1 Sherman Act	Art. 101 TFEU	Ch. 1 CA98
Prohibition of abuse of a dominant position/ monopolization	§2 Sherman Act	Art. 102 TFEU	Ch. 2 CA98
Key enforcers	DOJ FTC	European Commission	CMA/ FCA

- Penalties can be both civil and criminal
- Litigation and investigations typically take years to resolve

Antitrust & Competition – Conduct at Issue

Price Fixing

Tying

Market Allocation

Bundling

Loyalty Rebates & Price Discrimination

Exclusive Dealing

Antitrust & Competition – "Newer" Enforcers & Approaches

In October 2021, the CFPB issued orders seeking 2019-2021 payment processing information from Big Tech and fintechs. CFPB: "payments businesses are network businesses and can gain tremendous scale and market power, potentially posing new risks and undermining fair competition."

Proposed revisions to 1995 Bank Merger Guidelines:
(1) broader definition of competitive effects; (2) less focus on branch divestiture remedy; and (3) increased pool of stakeholders taken into consideration

Antitrust & Competition – BaaS Potential Areas of Concern

Price Fixing / Market Allocation

Hypothetical: Bank seeks to originate loans but relies on fintech partners to secure applicants and divides market between fintechs based on geography

Exclusive Dealing

Hypothetical: Large brokerage house and bank partners only allow access to select payment apps to its cash management accountholders

"Abusive" Access to Data

Hypothetical: Big Tech company offers banking services through a bank partner (*e.g.*, deposit account, credit card, etc.) but uses account transactional data and history for marketing Big Tech's primary business lines without consent

Price Discrimination

Hypothetical: Large retailer offers financial products through bank partner and offers preferential pricing only to customers who use those financial products

Partner / B2B Litigation

Breach of Contract

- Quality and scope of services provided
- Unplanned offline or service interruption
- Pricing and payment issues

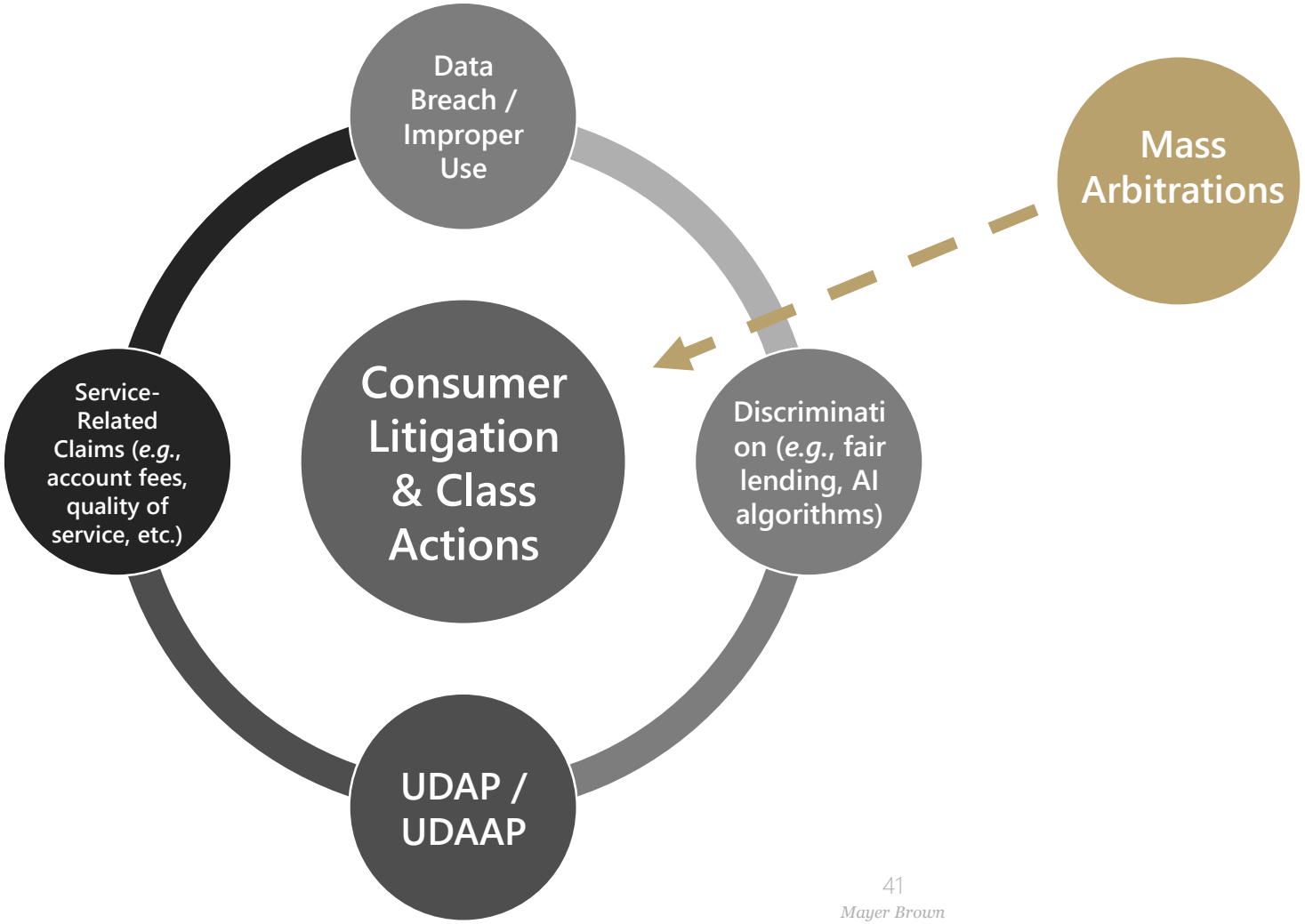
Indemnification

- Suits from end-customers or third parties
- Governmental investigations

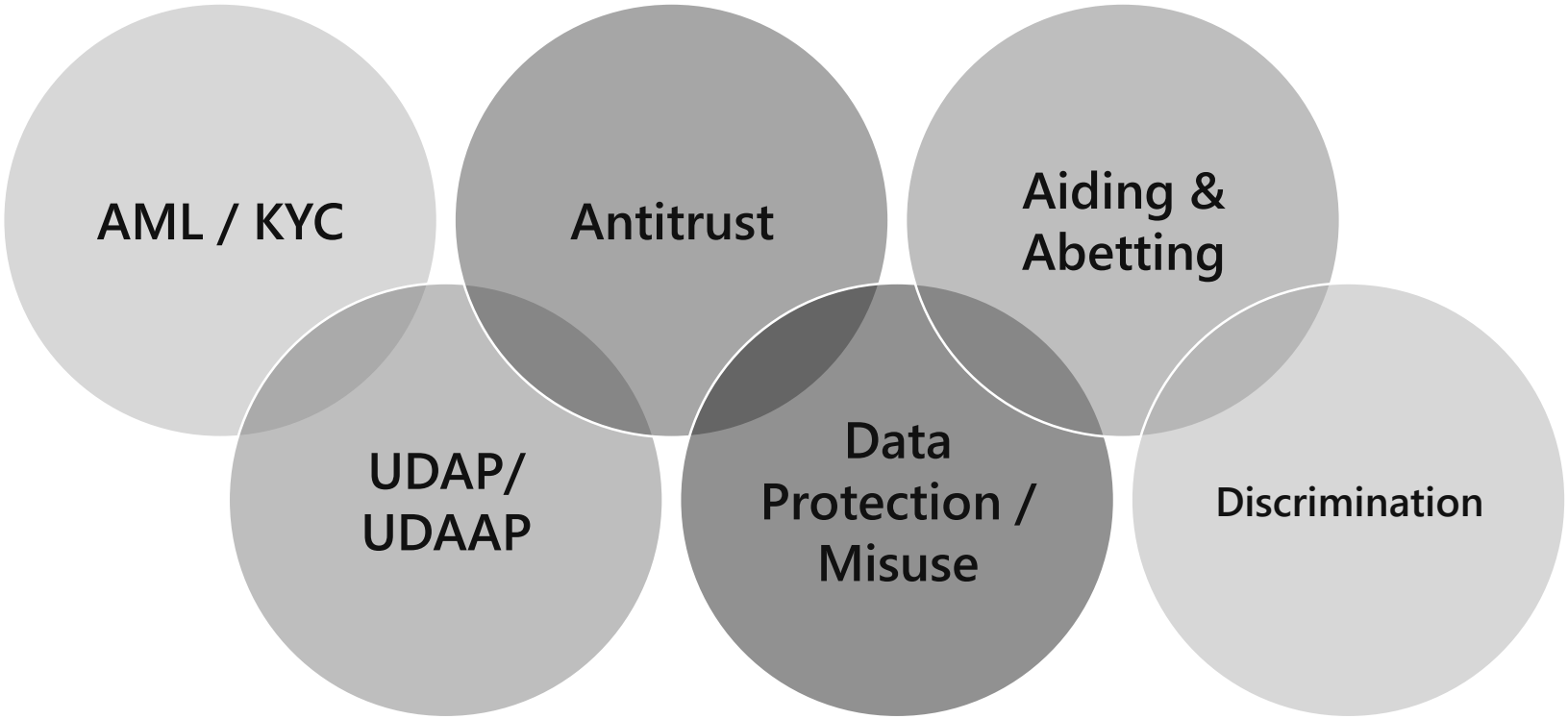
IP Dispute

- Patent / copyright / trademark
- Trade secrets

Consumer Litigation & Class Actions



Governmental / Regulatory Litigation



ARTIFICIAL INTELLIGENCE CONTRACTING ISSUES

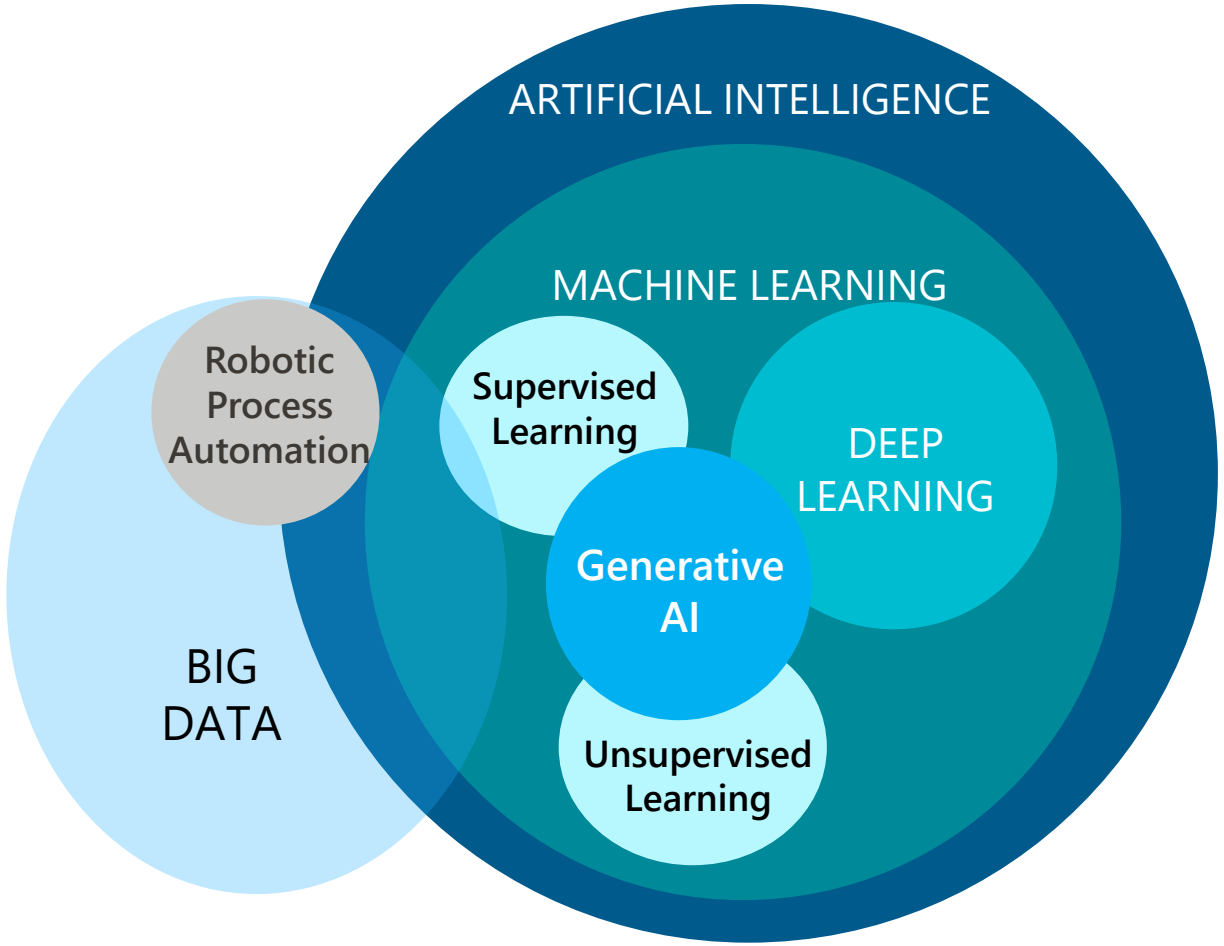
AI CAPABILITIES

What is AI?

- Definition 1: Software able to perform tasks that normally require human intelligence
- Definition 2: Use of algorithms to estimate the probability of future events based on patterns found in prior data

Examples

- Information Capture:
  - Vision recognition (e.g., recognizing a face or photo)
  - Sound recognition (e.g., transcribing spoken words)
  - Search (e.g., extracting data from unstructured documents)
  - Data analysis (e.g., identifying unusual data for human review)
- Delivering Insight from Information:
  - Natural language processing (e.g., extracting meaningful data from an email)
  - Predictions (e.g., probability that asset price will rise)
  - Recommendations (e.g., buy, sell, extend credit)
- Generating New Content



Source: Financial Stability Board

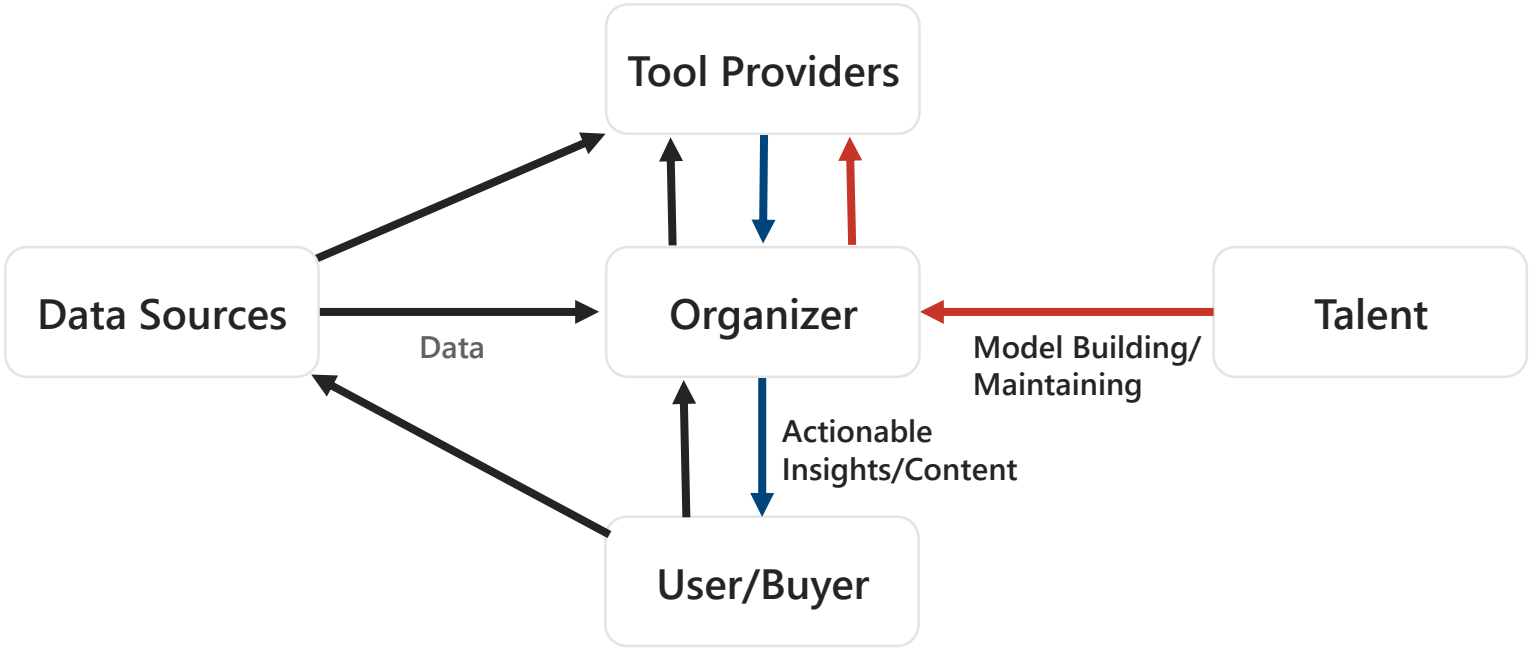
AI Contracting Overview

- Artificial intelligence and machine learning are powerful new technologies that are being rapidly adopted.
- Contracting for AI is complex because the AI ecosystem is complex.
- The result is a complex, interrelated, high-profile set of legal and contracting challenges.
- AI-savvy legal support will yield large returns as AI grows in power and value.

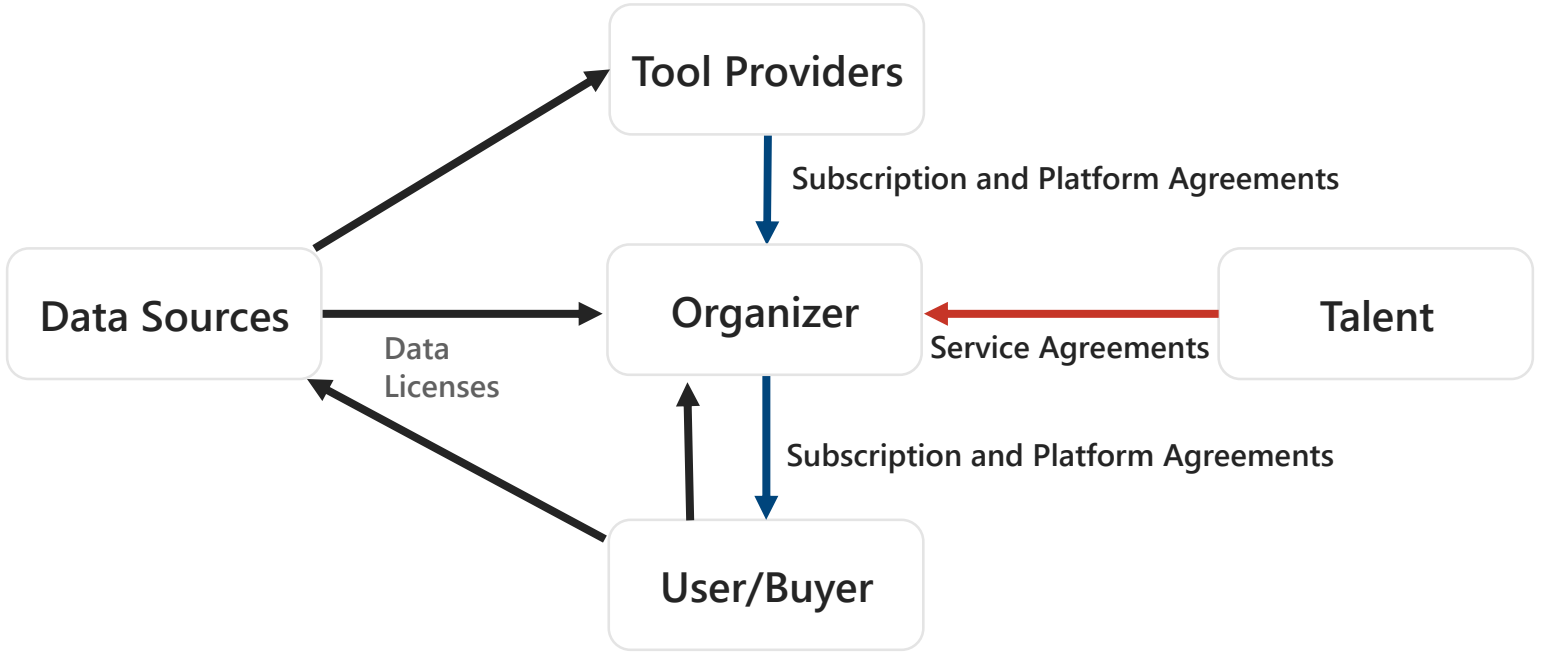
What's Different About AI and Why?

- Who does what in the AI ecosystem?
- What's new and different about contracting for AI?
- What are the critical issues for AI buyers and users?

Who Does What in the AI Ecosystem?



AI and Commercial Transactions



WHAT'S NEW AND DIFFERENT ABOUT CONTRACTING FOR AI?

Deal Structuring Challenges for AI Deals

- AI solutions involve many types of contracts, each with its own issues
- It's difficult to know what's possible, so "build to spec" is a poor fit
- Both the possible and the performance may change over time
- Inputs may bear little relationship to outputs
- Audit may be difficult or impossible
- AI organizers rely on data, tool and talent providers under contracts you cannot affect

Challenges in Defining the Key Components

AI/ML involves new concepts in people, processes, technology and data.
For example, new concepts may include:

TRAINING DATA

The data set and information used to train and test the AI Solution.

TRAINING INSTRUCTIONS

The algorithms, programs or other training processes that may be used to train and test the AI Solution.

PRODUCTION DATA

The data set entered into the AI Solution after it has been trained and is ready for production and that is used to product AI Output.

AI OUTPUT

The outcome of the AI Solution applying its logic to Production Data.

AI EVOLUTIONS

Iterations of the AI Solution that evolve during training and subsequent uses (i.e., generational refinements or improvements).

Challenges in Reviewing AI Models

- An AI/ML system cannot explain its reasoning and “explainable AI” may require designers to reduce capability.
- AI/ML systems may consider thousands of factors in opaque ways.
- AI/ML systems regenerate or recalibrate models based on new data daily or even in real time. Thus, past testing may not certify new models.

New Challenges in Non-AI Contracts

AI affects a wide range of contracts:

- Many service providers are already using AI to dramatically lower their costs without passing their savings onto customers
- Services contracts written years ago often have no barriers to the provider's use of AI to replace humans

Switching from human to AI delivery may remove the value of contractual protections and create new risks

- Service levels for humans, such as speed, lose all value
- AI systems may, however, make mistakes that no human would make

Customers need to be proactive in demanding to share in the benefits of AI innovations that are already taking place

WHAT ARE THE CRITICAL ISSUES FOR AI BUYERS AND USERS?

Initial Questions About the Project

- What predictions/probabilities/suggestions will the AI system provide?
- How will you measure success?
- Who is responsible for each AI component?
- Are you the organizer or are you contracting with an organizer?
- Will the same AI system serve customers other than you?
- Will the AI solution make or affect regulated decisions?
- Will the AI solution process personally identifiable information?
- How far along is this now?

Deal Structuring Questions

- How will the provider's performance be assessed?
- How, if at all, will the provider's compensation be linked to how well the system performs?
- Who bears the financial risk that the AI system does not perform well enough to be profitable?
- What control will the buyer/user have over how the AI system works?
- What options will each party have to terminate, and what rights will the parties have upon termination?

Key Issues in Agreements with Data Sources

- Use rights
- Functionality
- Performance
- Price
- Enabling compliance
- Term and termination
- Liability
- Provider financial condition

Key Issues in Agreements with Tool Providers, Talent and Organizers

- Use rights
- Functionality
- Performance
- Compensation
- Enabling compliance
- Term and termination
- Liability
- Provider financial condition
- Data security, data privacy and incident response
- Audits and examinations
- Personnel
- Disaster recovery and business continuity
- IP rights
- Disengagement services

Key Issues Related to Intellectual Property Rights

- Rights in AI Output
  - ✓ AI Output generally not protected under copyright or patent law because there is no human authorship
- Rights in Training Data
  - ✓ Does the AI vendor have sufficient rights in the training data used to create and refine the AI tool?
  - ✓ If the AI user is going to have the tool customized with its own data or third-party data, does the AI user have sufficient rights to license that data for training?
- Confidentiality Breaches
  - ✓ Either through day-to-day use or customized training, is the AI user jeopardizing rights in its own confidential information or that of others?

Contractual Requirements to Avoid Unauthorized Use of Data

- Use of “data lakes”
- Abide by applicable contractual requirements related to your use of data
- Internal controls on access of data
- Track what insights are derived from which data

Contractual Requirements to Protect Your AI Developments

- Adequate security measures
- Designation of data as trade secret and as Confidential Information and as “Bank Data”
- Adequate restrictions on sharing of data
- Design solutions with creative elements and have creative human input
- Review existing and new contracts for broad use rights

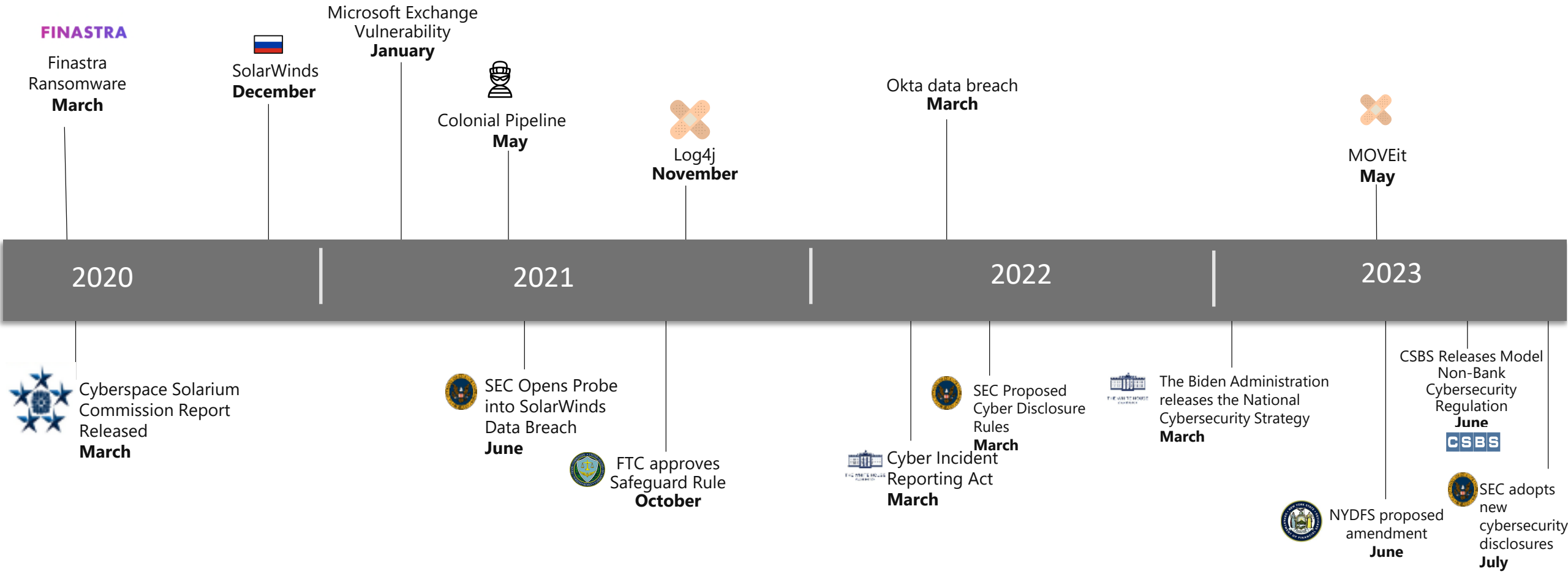
QUESTIONS?


Statistic Graph
ON
00:04:12
ON
LOREM IPSUM
EXE
00:00:12
WARNING
00:01:21
b/0

BOARD-LEVEL ISSUES (INCLUDING IN RELATION TO AI)

SUPERVISORY EXPECTATIONS AND PERSPECTIVES

Third-Party Cyber Risk Continue to Grow



Third-Party Cybersecurity Program

- Expectations set forth in NYDFS regulation, FFIEC guidance, SEC, other state regulators, etc.
- Key Components
  - ✓ Risk Assessment of Third-Parties
  - ✓ Due Diligence
  - ✓ Minimum Cybersecurity Standards
  - ✓ Contractual Assurances
  - ✓ Ongoing Diligence and Monitoring

Assessing Vendor Risk

- Sensitive Data
  - ✓ Consumer Data
    - Privacy: disclosure, consent, opt-out, etc.
    - Cybersecurity
  - ✓ Other Confidential Data
- Network Access
  - IT Infrastructure
  - Systems or database integration
- Transaction Monitoring/KYC
  - Crypto

CFPB Proposed Data Rights Rule

- October 19: Personal Financial Data Rights Rule
  - Would require covered financial institutions to provide consumers and authorized third parties with access and portability options for their financial data.
  - Intended to ensure that consumers have a legal right to share their data with the provider of choice
  - Open for comment until December 23, 2023

<u>Banks and other data providers</u>

- Create an interface to share data at no charge
- Develop a security program for the interface
- May deny access if the third party does not present evidence of adequate data security practices

<u>Third Parties</u>

- Implement a data security program per GLBA
- Consumer consent and disclosure
- Limitations on further sharing the consumer data

Regulatory Expectations & Enforcement: Your Vendor, Your Problem

- Duty to supervise third parties
- Underlying responsibility stays with the regulated company for compliance with on cyber, privacy, consumer protection, transaction monitoring, etc.
- Enforcement trends

CLE RELATED CONTENT FOR:
"PRIVACY AND DATA PROTECTION"
AND
"BOARD-LEVEL ISSUES"
PANELS

AI Regulatory Challenges

FAIRNESS/BIAS

- EU Draft Artificial Intelligence Act - *pending*
- CFPB Targets Unfair Discrimination in Consumer Finance (March 2022)
- New York City, Automated Employment Decision tools (2021)
- Colorado, Protecting Consumers from Unfair Discrimination in Insurance Practices (SB21-169) (2021)
- California, Automated Decision Tool (AB 331) – *bill pending*

BOARD OVERSIGHT MANDATED

- NYDFS Proposed Cybersecurity Rule Amendments (2022)- *pending*
- EU - Digital Operational Resilience Act (DORA) (adopted-effective 2025)

AI Governance Developments

QUESTIONS THE BOARD AND CEO SHOULD ASK:

How are we using AI?

Is customer personal/or IP protected information used to train the model?

Has the AI tool been tested for accuracy/fairness prior to deploying?

Does the company have a regular cadence for monitoring the AI to ensure accuracy?

Do we have governance policies in place for the AI?

Do we have a "human" in the middle of decision making?

Has the training been in accordance with White House AI Bill of Rights tech specifications?

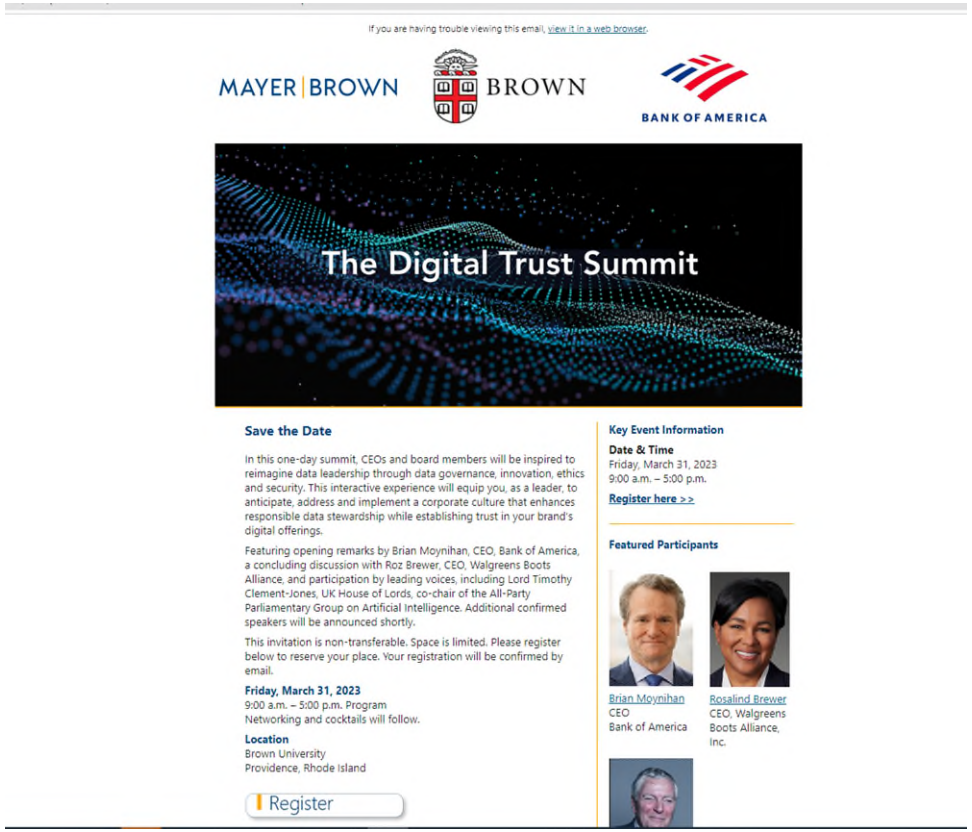
The Global Landscape on Data Has Changed

- DATA PROTECTION IS A GLOBAL ISSUE THAT IS IMPACTING TECHNOLOGIES AROUND THE WORLD.
- 160 + COUNTRIES HAVE DATA PROTECTION LAWS
- ORGANIZATION AND SYNERGY IS NEEDED TO ACHIEVE DATA LEADERSHIP AND TRUST
- HOW ATTENTION TO PRIVACY WILL STABILIZE OUR MARKETS (WORLD ECONOMIC FORUM MAY 25, 2022).

160

Countries with data protection laws located in regions where BaaS occurring

Digital Trust Summit



If you are having trouble viewing this email, view it in a web browser.

MAYER | BROWN BROWN BANK OF AMERICA

The Digital Trust Summit

Save the Date

In this one-day summit, CEOs and board members will be inspired to reimagine data leadership through data governance, innovation, ethics and security. This interactive experience will equip you, as a leader, to anticipate, address and implement a corporate culture that enhances responsible data stewardship while establishing trust in your brand's digital offerings.

Featuring opening remarks by Brian Moynihan, CEO, Bank of America, a concluding discussion with Roz Brewer, CEO, Walgreens Boots Alliance, and participation by leading voices, including Lord Timothy Clement-Jones, UK House of Lords, co-chair of the All-Party Parliamentary Group on Artificial Intelligence. Additional confirmed speakers will be announced shortly.

This invitation is non-transferable. Space is limited. Please register below to reserve your place. Your registration will be confirmed by email.

Friday, March 31, 2023
9:00 a.m. – 5:00 p.m. Program
Networking and cocktails will follow.

Location
Brown University
Providence, Rhode Island

Register

Key Event Information

Date & Time
Friday, March 31, 2023
9:00 a.m. – 5:00 p.m.

Register here >>

Featured Participants

Brian Moynihan
CEO
Bank of America

Rosalind Brewer
CEO, Walgreens Boots Alliance, Inc.

Digital Trust Summit

LED BY BANK OF AMERICA CEO BRIAN MOYNIHAN, 60 CEOS AND BOARD MEMBERS MET ON MARCH 31, 2023, AT THE WATSON INSTITUTE AT BROWN UNIVERSITY TO DISCUSS GENERATIVE AI, PRIVACY, CYBER AND DATA LEADERSHIP ACHIEVED BY ENHANCING TRUST.

REVIEW DIGITAL TRUST WEBSITE

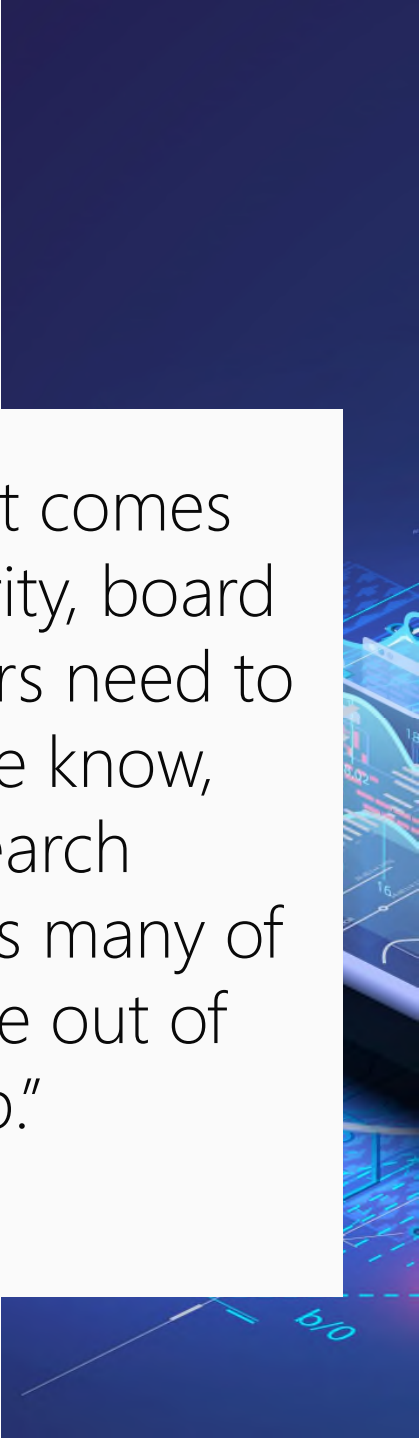
REGULATORY FOCUS ON THE BOARD'S DUTY OF CARE AND OVERSIGHT HAS HEIGHTENED OVER THE PAST YEAR

Recent Developments: FTC April 8, 2021 Report

CORPORATE BOARDS: DON'T UNDERESTIMATE YOUR ROLE IN DATA SECURITY OVERSIGHT

- April 8, 2021, the FTC published *Corporate boards: Don't underestimate your role in data security oversight*.
- In that document, the FTC called for boards to "build a team of stakeholders" who can "...bring a different perspective to the issues."
- The FTC called for the team that reports to the board to include nontechnical leaders such as the CEO, CFO and legal counsel.
- FTC also encouraged boards to review their committee structure to ensure that board oversight over cybersecurity occurs either at the audit committee level or via a standalone committee devoted to cybersecurity
- The FTC called for regular briefings to include privacy and cyber

"When it comes to security, board members need to be in the know, but research suggests many of them are out of the loop."



Privacy Has Cost Companies Trillions in Market Cap

IN 2022, BECAUSE 85% CONSUMERS OPTED OUT OF MOBILE TRACKING DUE TO PRIVACY, NASDAQ LISTED COMPANIES LOST $1.4 TRILLION IN MARKET CAP. SEE, DATA PRIVACY: A BUSINESS IMPERATIVE FOR BOARDS & LEADERS THAT MAY CONTRIBUTE TO MARKET RECOVERY (NASDAQ, 2022);

GDPR FINES NOW LEVIED AGAINST 1186 COMPANIES TOTALING €2,040,213,207, INCLUDING:

- An American multinational technology company focusing on e-commerce, cloud computing, online advertising, digital streaming, and artificial intelligence had the largest GDPR fine of €746,000,000;
- A global social network was fined €405,000,000;
- A global cloud provider was fined €90,000,000

FTC HAS FINED A MAJOR MICRO BLOGGING COMPANY $150 MILLION IN 2022

Privacy Issues Have Resulted in Over $1.4 Trillion Losses for NASDAQ Listed Companies

Boards and CEOs of Privately Held Companies Must Focus on Data Leadership

- INVESTORS SEND PRIVACY/DATA SECURITY MATURITY QUESTIONNAIRES PRIOR TO INVESTING.
- SIGNIFICANT INVESTORS HAVE ENGAGED WITH COMPANIES AROUND CYBER AND PRIVACY
  BLACKROCK.COM | INVESTMENT STEWARDSHIP REPORT: AMERICAS Q1 2018
- STOCK EXCHANGES ARE FOCUSING ON DATA PRIVACY AND SECURITY.

Recent Developments: NY DFS July 29, 2022 Proposal

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

- NY DFS' proposed rule would require board approval of cybersecurity policies that cover (at a minimum): "(a) information **security**; (b) **data governance** and classification; and…customer **privacy**."
- "The board or an appropriate committee of **the board shall have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge**, to exercise effective oversight of cyber risk and a committee or subcommittee assigned responsibility for cybersecurity."

Recent Developments: SEC Feb. 9, 2022 Proposed Rule

CYBERSECURITY RISK MANAGEMENT FOR INVESTMENT ADVISERS, REGISTERED INVESTMENT COMPANIES, AND BUSINESS DEVELOPMENT COMPANIES

- "Proposed rule 38a-2 would require a fund's **board of directors**, including a majority of its independent directors, initially to **approve the fund's cybersecurity policies and procedures**, as well as to review the written report on cybersecurity incidents and material changes to the fund's cybersecurity policies and procedures that…would be required to be prepared at least annually"
- The required written reports… would provide fund directors with **information necessary to ask questions and seek relevant information regarding the effectiveness of the program and its implementation**, and whether the fund has adequate resources with respect to cybersecurity matters, including access to cybersecurity expertise. **We anticipate that a fund's board's review of the written reports would naturally involve inquiries about cybersecurity risks** arising from the program and any incidents that have occurred

"Board oversight should not be a passive activity."

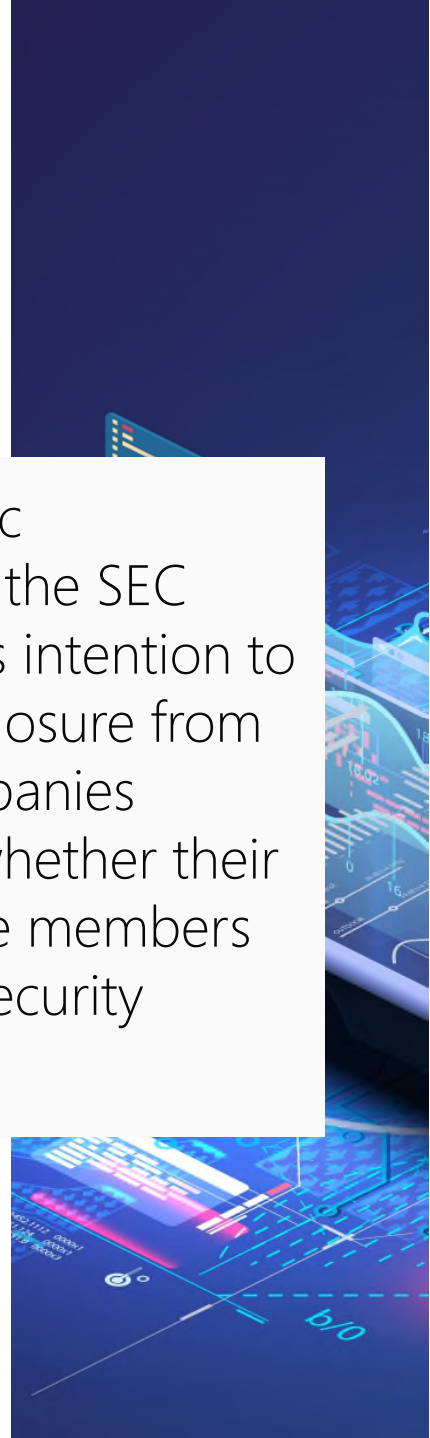
- SEC February 9, 2022 Report

Recent Developments: SEC March 2022 Proposed Rule

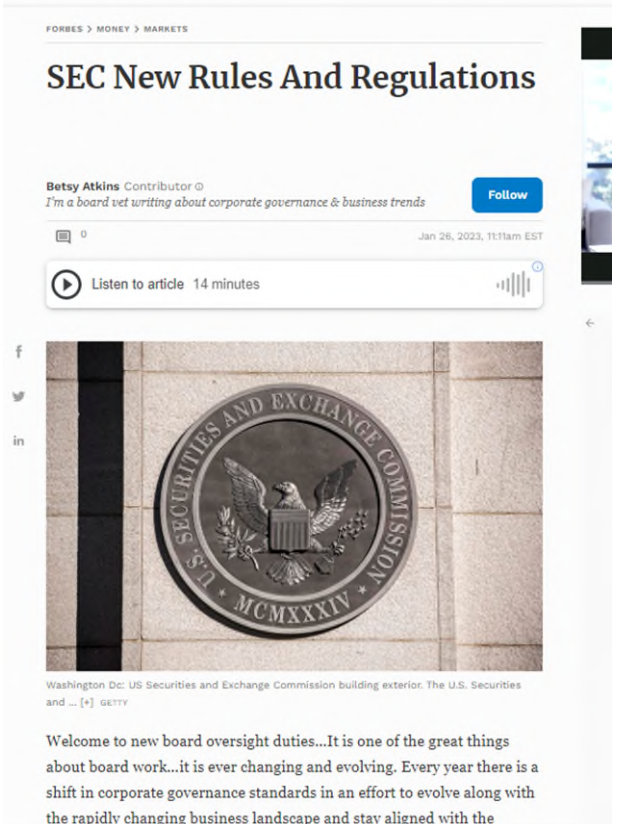
CYBERSECURITY RISK MANAGEMENT, STRATEGY, GOVERNANCE, AND INCIDENT DISCLOSURE

"Cybersecurity is already among the top priorities of many boards of directors [citation omitted] and cybersecurity incidents and other risks are considered one of the largest threats to companies.[Citation omitted] **Accordingly, investors may find disclosure of whether any board members have cybersecurity expertise to be important as they consider their investment in the registrant as well as their votes on the election of directors of the registrant**."

For all public companies, the SEC describes its intention to require disclosure from public companies regarding whether their boards have members with cybersecurity experience.



New Cybersecurity Rules Expected April 2023



FORBES > MONEY > MARKETS

SEC New Rules And Regulations

Betsy Atkins Contributor
I'm a board vet writing about corporate governance & business trends

Follow

0

Jan 26, 2023, 11:11am EST

Listen to article 14 minutes

Washington Dc: US Securities and Exchange Commission building exterior. The U.S. Securities and ... [+] GETTY

Welcome to new board oversight duties...It is one of the great things about board work...it is ever changing and evolving. Every year there is a shift in corporate governance standards in an effort to evolve along with the rapidly changing business landscape and stay aligned with the

Proposed Action: Focus on Financial Metrics

BOARD REPORTS SHOULD HIGHLIGHT THE FINANCIAL EXPOSURE ATTRIBUTED TO THE ORGANIZATION'S CYBER RISK LEVERAGING THE SAME ANALYTICS USED BY LEADERS WITHIN THE CYBER INSURANCE INDUSTRY. THE BOARD REPORTS SHOULD INCLUDE:

- An organization's overall financial exposure to cyber risks and cyber-attacks,
- A view of the cyber threats most likely to cause financial losses to a business,
- Insights on the cyber controls/investments most effective in mitigating financial losses, and
- Insights on cyber risk transfer/cyber insurance, including "stress testing" existing policies across a range of potential cyber incidents.

NACD®

Website Link

NACD Cyber Risk Reporting Standard

Shareholder Derivative Actions Naming BoD Re Privacy & Cyber are on the Rise – Over 75 Actions filed

CPO MAGAZINE HOME NEWS INSIGHTS RESOURCES

In recent months, a trend has begun to emerge among plaintiffs' lawyers seeking to file cybersecurity incident-related shareholder derivative lawsuits – attorneys are increasingly now filing claims specifically based on failures surrounding duty of oversight. In November of 2021, a shareholder derivative lawsuit was filed against T-Mobile USA's board of directors, pointing to a lack of monitoring and acting upon obvious red flags. Kevin M. Lacroix excellently outlines this trend in The D&O Diary. Directors should take notice.

Mayer Brown has identified over 75+ shareholder derivative actions pertaining to privacy and cyber.

Triggering Conduct for BoD liability

UNITED STATES

1. FAILURE TO STAY INFORMED
2. LACK OF A BOARD COMMITTEE WITH DATA PRIVACY AND SECURITY OVERSIGHT
3. LACK OF QUALIFIED OFFICERS
4. FAILURE TO SAFEGUARD PERSONAL DATA
5. FAILURE TO RESPOND TO KNOWN CYBER THREATS
6. FAILING TO CONDUCT ADEQUATE DUE DILIGENCE
7. FALSE SEC FILINGS AND OTHER PUBLIC STATEMENTS
8. LACK OF TRANSPARENCY
9. INSUFFICIENT OVERSIGHT OF VENDORS AND THIRD PARTIES
10. FAILURE TO PROVIDE TIMELY AND ADEQUATE NOTICES
11. COMPLIANCE WITH LAWS

DOJ's New Stance on Corporate Enforcement

THE WALL STREET JOURNAL.

English Edition | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business Tech Markets Opinion Books & Arts Real Estate Life & Work Style Sports

TAKE A SURVEY We want to hear from you. Take part in this short survey to help shape The Wall Street Journal. Take Survey

SHARE

RISK & COMPLIANCE JOURNAL

DOJ Pushing Ahead With Corporate Settlement Policy That Could Make Execs Liable, Official Says

The U.S. Justice Department is charging ahead with a new policy that makes top executives certify the effectiveness of their compl program as part of corporate resolutions

CCO certifications serve as a tool for the Justice Department as it tries to hold individuals accountable for their role in corporate wrongdoing, said Alixandra Smith, the deputy chief of the criminal division at the Brooklyn U.S. attorney's office.

The Emergence of Chief Controls Officers

TIAA's Pamela Feldstein leads a new tasked with understanding and revie the firm's internal controls and proce as it aims to achieve operational excellence and hone customer exper

Salesforce's Chief Ethical Use Officer: 'People Won't Use Tec They Don't Trust'

Paula Goldman, Salesforce's first chief and humane use officer, discusses the potential benefits of applying ethics in technology management and what lead do to help.

[DOJ Pushing Ahead With Corporate Settlement Policy That Could Make Execs Liable, Official Says]

"The U.S. Justice Department isn't backing away from a policy, criticized by some in the corporate sector, of having compliance officers sign off on the effectiveness of their programs as part of settlements.
The certifications serve as a tool for the Justice Department as it tries to hold individuals accountable for their role in corporate wrongdoing, said Alixandra Smith, the deputy chief of the criminal division at the Brooklyn U.S. attorney's office."

Wall Street Journal, September 22, 2022

Global Focus on BoD Oversight of Privacy & Cyber

- **EU** DRAFT DIGITAL OPERATIONAL RESILIENCE ACT (DORA) COVERS FINANCIAL SERVICES, CRYPTO, PAYMENTS AND OTHERS. DORA STATES: "MEMBERS OF THE MANAGEMENT BODY SHALL, ON A REGULAR BASIS, FOLLOW SPECIFIC TRAINING TO GAIN AND KEEP UP TO DATE SUFFICIENT KNOWLEDGE AND SKILLS TO UNDERSTAND AND ASSESS **[INFORMATION COMMUNICATION TECHNOLOGY]** ICT RISKS AND THEIR IMPACT ON THE OPERATIONS OF THE FINANCIAL ENTITY." NIST 2 – FOCUS ON "MANAGING BODIES" ACCOUNTABILITY. DRAFT ARTIFICIAL INTELLIGENCE ACT.
- THE **UNITED KINGDOM'S** NATIONAL CYBER SECURITY CENTRE (NCSC) HAS A CYBER SECURITY TOOLKIT FOR BOARDS WEBSITE THAT CONTAINS "[R]ESOURCES DESIGNED TO ENCOURAGE ESSENTIAL CYBER SECURITY DISCUSSIONS BETWEEN THE BOARD AND THEIR TECHNICAL EXPERTS."
- **DENMARK** GUIDANCE EMPHASIZES BOD'S OVERSIGHT ROLE WHEN IT COMES TO CYBER CENTRE FOR CYBER SECURITY (CFCS) PUBLISHED A DECEMBER 2019 CYBERSECURITY GUIDANCE FOR BOARDS OF DIRECTORS.
- **AUSTRALIAN SECURITIES & INVESTMENT COMMISSION** COUNSELED BOARD MEMBERS TO ASK THEMSELVES: "**DOES THE BOARD NEED FURTHER EXPERTISE TO UNDERSTAND THE RISK?** ALTHOUGH BOARDS MAY NOT REQUIRE GENERAL TECHNOLOGY EXPERTISE, FOR MANY COMPANIES IT MAY BE ADVISABLE TO HAVE ONE OR MORE DIRECTORS WHO HAVE A STRATEGIC UNDERSTANDING OF TECHNOLOGY AND ITS ASSOCIATED RISKS, OR WHO HAVE A BACKGROUND IN CYBERSECURITY. IN SOME CIRCUMSTANCES, *THE BOARD SHOULD CONSIDER THE USE OF EXTERNAL CYBER EXPERTS TO REVIEW AND CHALLENGE THE INFORMATION PRESENTED BY SENIOR MANAGEMENT.*

BoD is the focus of regulators in the EU, MEA, and APEC.

Privacy & Cyber Are Measured Under the Governance Prong of ESG

Privacy & Cyber Are Being Rated as Part of ESG by Proxy Advisors and Investors

- INSTITUTIONAL SHAREHOLDER SERVICES ("ISS") RATES COMPANIES ON THEIR CYBER AND PRIVACY PRACTICES VIA THE GOVERNANCE PRONG OF AND ISSUES A CYBER RISK SCORE
  ISS GOVERNANCE.COM | ESG CYBER RISK SCORE™
- GLOBAL REPORTING INITIATIVE (GRI), RELIED ON FOR ESG REPORTING BY MANY COMPANIES, HAS ISSUED A SPECIFIC "CUSTOMER PRIVACY STANDARD"
- SIGNIFICANT INVESTORS HAVE ENGAGED WITH COMPANIES AROUND CYBER AND PRIVACY
  BLACKROCK.COM | INVESTMENT STEWARDSHIP REPORT: AMERICAS Q1 2018

Video

Website Link

Critical Privacy Elements in ESG Scoring

Data Privacy Considerations

CUSTOMER DATA

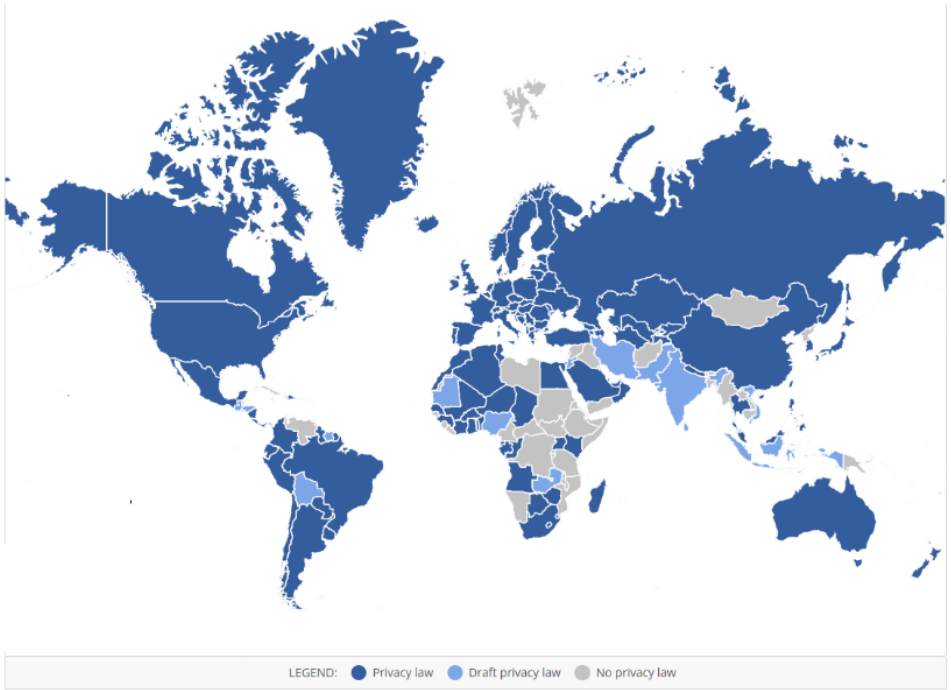
BANKING DATA

USER CREDENTIALS DATA ETC

DEVICE IDS

UNIQUE IDENTIFIERS

Can include Personal Data / PII



Things to Do

- DATA GOVERNANCE
- INVENTORY DATA
- UNDERSTAND DATA FLOWS
- INDEPENDENT USE OF DATA (BEYOND PROVIDING SERVICES FOR THE PLATFORM COMPANIES) WILL RESULT IN COMPANY BEING CONSIDERED A CONTROLLER WITH GREATER DATA PRIVACY OBLIGATIONS.
  - Using data to improve algorithms, enhance BaaS
- SECURITY IS AN ISSUE. ALWAYS.

US Privacy Laws – State Activity

COMPARING CONSUMER RIGHTS UNDER STATE PRIVACY LAWS

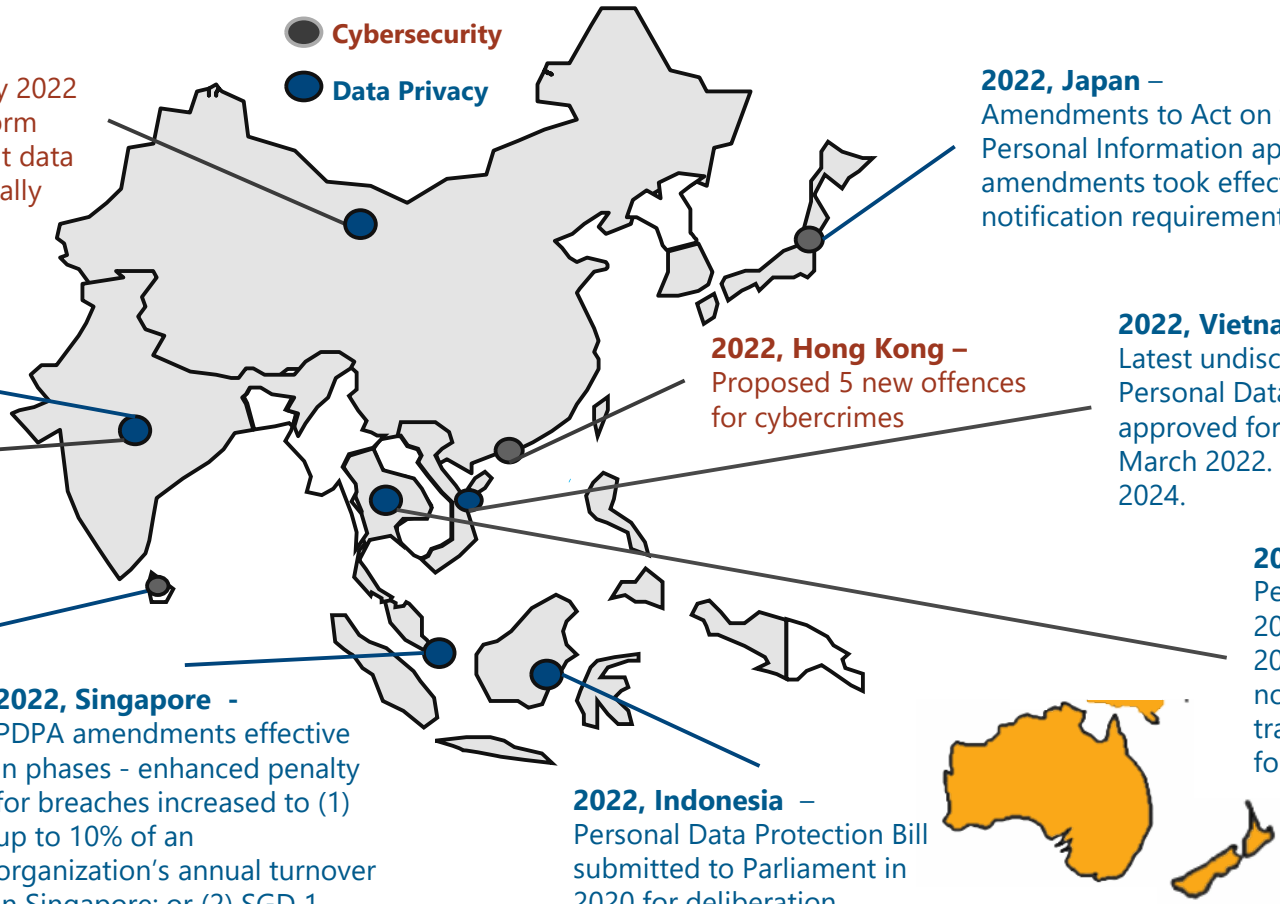
Right	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
Access	Yes	Yes	Yes	Yes	Yes	Yes
Correct	Yes	No	Yes	Yes	Yes	No
Delete	Yes (data provided by or obtained about consumer*)	Yes (data that consumer provided to controller)	Yes (personal data concerning consumer)	Yes (data provided by or obtained about consumer*)	Yes (data collected from consumer)	Yes (data collected from consumer)
Portability	Yes	Yes	Yes	Yes	Yes	Yes
Opt-out of sale	Yes	Yes	Yes	Yes	Yes	Yes
Non-discrimination	Yes	Yes	Yes	Yes	Yes	Yes
Appeals process	Yes	No	Yes	Yes	No	No

* The CTDPA authorizes businesses that collect data indirectly (about, rather than from, a consumer) to opt the consumer out of processing as an alternative or to retain (suppress) minimal data to ensure continued deletion. The VCDPA was amended on April 11, 2022, in like fashion.

DATA CONTROLLER OBLIGATIONS UNDER STATE PRIVACY LAWS

Obligation	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
Data minimization	Yes	Yes	Yes	Yes	Yes	No
Purpose limitation	Yes	Yes	Yes	Yes	Yes	Yes
Security requirements	Yes	Yes	Yes	Yes	Yes	No, but the private right of action applies to security breaches
Consent for sensitive data	Yes	No, consumers can opt-out	Yes	Yes	No, consumers can limit use to what is reasonably necessary	No
Special requirements for children's data	Yes (sale of personal information of children under 16 years)	Yes (personal data for a known child under 13 years)	Yes (personal data for a known child under 13 years)	Yes (sensitive data of children under 13 years)	Yes (sale of personal information of children under 16 years)	Yes (sale of personal information of children under 16 years)
Privacy notice	Yes	Yes	Yes	Yes	Yes	Yes
Disclose sale	Yes	Yes	Yes	Yes	Yes	Yes
Data protection assessment	Yes	No	Yes, available upon request by CO AG	Yes	Yes, risk assessments submitted to CA Privacy Protection Agency	No
Requirements for de-identified data	Yes	Yes	Yes	Yes	Yes	Yes

Regulatory Landscape in APAC



2022, China –
Measures for Cybersecurity Review effective 15 February 2022 applicable to network platform operators who may carry out data processing activities potentially affecting national security

2022, India -
Personal Data Protection Bill 2019 – Bill withdrawn, a new bill to be presented for public consultation.

2022, India -
India CERT- In Cybersecurity Directions 2022 effective 27 June 2022 mandating reporting of cybersecurity incident within 6 hours

2022, Sri Lanka -
Passed Personal Data Protection Act on 18 March 2022, to come into effect in stages 2023 onwards

2022, Singapore -
PDPA amendments effective in phases - enhanced penalty for breaches increased to (1) up to 10% of an organization's annual turnover in Singapore; or (2) SGD 1 million, whichever is higher, effective 1 Oct 2022

2022, Indonesia –
Personal Data Protection Bill submitted to Parliament in 2020 for deliberation. Expected to be signed by the House of Representatives in August 2022.

2022, Japan –
Amendments to Act on the Protection of Personal Information approved in 2020 – amendments took effect April 2022– mandatory notification requirements

2022, Hong Kong –
Proposed 5 new offences for cybercrimes

2022, Vietnam -
Latest undisclosed draft of the Personal Data Protection Decree approved for consultation in March 2022. Law expected in 2024.

2022, Thailand -
Personal Data Protection Act 2019 came into force on 1 June 2022 mandatory breach notification, cross-border transfer restrictions, right to be forgotten

The GDPR Today: Recent Trends

- **THE GDPR:**
  A UNIFORM LAW GOVERNING THE PROCESSING OF PERSONAL DATA ACROSS ALL SECTORS SINCE 2018, SUPPLEMENTED BY NATIONAL LAWS AND GUIDANCE.
- **TOUGHER ENFORCEMENT IN THE EU:**
  EVER HIGHER FINES BEING ISSUED ON A MONTHLY BASIS BY SUPERVISORY AUTHORITIES.
- **INCREASING SCRUTINY OVER INTERNATIONAL DATA TRANSFERS:**
  SCHREMS II, EDPB RECOMMENDATIONS, EUROPEAN SUPERVISORY AUTHORITY ACTION ALL RESTRICT FLOWS OF DATA OUT OF EUROPE.
- **EU & UK DIVERGENCE:**
  GDPR SPLIT INTO TWO POST-BREXIT – EU GDPR & UK GDPR. UK ANNOUNCES REFORMS THAT WILL EFFECTIVELY SOFTEN UK GDPR.

Overview of Upcoming EU Rules Relating to Data

	Digital Services Act (DSA)	Digital Markets Act (DMA)	Data Governance Act (DGA) Regulation (EU) 2022/868	Data Act (DA)
Goal	Transparency in the digital markets; Protect consumers online	Fairer competition in the digital markets	Facilitate the sharing of personal and non-personal data	Ensure a fair and innovative data economy
Applies to	Online platforms and service providers (e.g. hosting and network infrastructure providers)	Gatekeepers (large providers of core platform services, e.g. search engines, social media, cloud computing systems etc.)	Data intermediation service providers (created by this Act) and public sector	Various parties, from manufacturers of connected devices to data holders in general and public bodies
Impact	Several new obligations for online platforms and service providers relating to point of contact, content moderation and transparency reporting	Wide range of obligations for gatekeepers relating to data, advertising, e-commerce, interoperability and the commercial relationship between the service providers, customers and end users. Will require material changes to the business models of some digital platforms.	Aims to create a harmonized framework for public sector data to be reused. It stimulates data altruism and establishes the European Data Innovation Board	New rules on who can use and access data generated in the EU across all economic sectors
Status	Adopted. Waiting for publication.	Adopted. Waiting for publication. Could be in force from March 2023	Published and in force; will apply from 24 September 2023	Text under discussion

Summary: At this time, the Acts do not impose direct obligations on businesses. However, their existence, and likely adoption, signal the EU's intention to regulate data beyond "personal data". This development will likely become relevant for businesses in the mid- to long-term.

Global Focus on BoD Oversight of Privacy & Cyber

- **EU** Digital Operational Resilience Act (DORA) covers financial services, crypto, payments and others. DORA states: "Members of the management body shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess [Information Communication Technology] ICT risks and their impact on the operations of the financial entity." NIST 2 – focus on "managing bodies" accountability. Draft Artificial Intelligence Act.
- The **United Kingdom's** National Cyber Security Centre (NCSC) has a Cyber Security Toolkit for Boards website that contains "[r]esources designed to encourage essential cyber security discussions between the Board and their technical experts."
- **Denmark** guidance emphasizes BoD's oversight role when it comes to cyber Centre for Cyber Security (CFCS) published a December 2019 cybersecurity guidance for boards of directors.

Conclusion

- Given the growth of BaaS in the last few years, it is important for Banks to determine their BaaS strategy.
- While there are tremendous benefits flowing from adopting a BaaS solution, there are also a host of challenges and risks (regulatory, contractual and operational).
- It is important to think through these challenges and risks early in the process.

MAYER | BROWN