Strafford

*Presenting a live 90-minute webinar with interactive Q&A*

# Data Privacy and Security Agreements: Defining, Allocating, and Mitigating Risks From Data Security Breaches

TUESDAY, MARCH 9, 2021

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Matthew J. Bacal, Counsel, **Davis Polk & Wardwell**, New York

Daniel F. Forester, Counsel, **Davis Polk & Wardwell**, New York

Matthew A. Kelly, Counsel, **Davis Polk & Wardwell**, New York

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

# *Tips for Optimal Quality*

FOR LIVE EVENT ONLY

*Sound Quality*

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

*Viewing Quality*

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

## *Continuing Education Credits*

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

## *Program Materials*

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

# Data Privacy and Security Agreements: Defining, Allocating, and Mitigating Risks from Data Security Breaches

Presented by:

**Matthew J. Bacal** – Intellectual Property & Technology Transactions
**Daniel F. Forester** – Intellectual Property & Technology Transactions
**Matthew A. Kelly** – Litigation

**March 9, 2021**

Davis Polk

# Agenda

1  Understanding Vendor Risk

2  Approaching the Vendor Relationship

3  Contracting with Your Vendor

4  Managing the Vendor Relationship and Dealing with Data Breaches

# Understanding Vendor Risk

Davis Polk

# Threat Landscape

**Phishing & "Malspam"**

**Over 90%**

Percentage of cybersecurity incidents that begin with a malicious email

**Data Breach**

**16 billion**

Records exposed (first 6 months of 2020)

**Business Email Compromise**

**Over $2,000,000,000**

Estimated losses due to BEC in 2019, with comparable estimates expected for 2020

**Extortion/Ransomware**

**Over $20,000,000,000**

Expected losses from extortion/ransomware in 2021

# Understanding Legal Risk from Poor Vendor Data Security

- Increasing Regulatory Requirements and Scrutiny
  - GDPR makes the data controller responsible for its vendors' handling of personal data processed on behalf of the data controller
  - Requirements under state laws in major jurisdictions, e.g., New York SHIELD Act, Massachusetts
  - CCPA litigation risk and data security as a defense
  - Long-emphasized in FTC enforcement actions
  - SEC has also prioritized vendor security
  - Other regulators and self-regulatory organizations have emphasized vendor due diligence for data security, including the OCC, FINRA, NFA, and NYDFS
- Enforcement and Civil Litigation Risk
  - CFTC fine against AMP Global Clearing LLC
  - FTC settlement with BLU Products, Inc.
  - Follow-on litigation from major vendor breaches

# Approaching the Vendor Relationship


Davis Polk

# Developing a Vendor Management Policy

- No one-size-fits-all approach to vendor management, including for diligence
- Develop a plan to understand your needs, risks from vendors, and legal obligations for data privacy and security that flow to your vendors (e.g., the GDPR, NYDFS requirements)
- Factors to consider when risk rating vendors:
  - Sensitivity of information exposed to the vendor
  - Quantity of information exposed to the vendor
  - Necessity of the vendor's services to your business
  - Fungibility of the vendor's services
- Diligence expectations/compliance requirements for each vendor risk category:
  - Data security measures
  - Privacy program
  - Audit rights
  - Cooperation rights
- Contractual obligations for each vendor risk category

# Example of Vendor Diligence Requirements: NYDFS

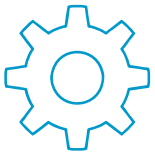
- NYDFS is a helpful measuring stick for comprehensive security practices
- NYDFS-regulated entities must have a vendor diligence program that includes:
  - Procedures to identify and assess vendor risks;
  - Policies outlining the "minimum cybersecurity practices" and cooperation obligations required of vendors;
  - Due diligence procedures to evaluate the vendor's cybersecurity practices; and
  - Procedures to complete periodic tests of the risks and cybersecurity practices of vendors.
- NYDFS requires regulated entities to consider 14 data security domains; these are similarly worth considering for vendor diligence:

| | | | | | | |
|---|---|---|---|---|---|---|
| Information security | Data governance, classification | Asset inventory, management | Access controls, ID management | Bus. continuity, disaster rec. | Systems operations, availability | Systems and network security |
| Systems and network monitoring | Application development and QC | Physical security | Customer data privacy | Vendor management | Risk assessment | Incident Response |

# Developing a Due Diligence Plan

- Diligence of vendor should be directed toward establishing that requirements of the Vendor Management Policy will be met
- Approach to diligence depends on factors such as risk, timing, availability
  - Questionnaires
  - Remote / On-site visits
  - Copies of independent reports (e.g., SOC 2)
- When is reliance on SOC 2 or trust documentation or certifications enough?
- How do you recommend varying the approach to diligence for different sized vendors (e.g., a startup analytics company versus AWS)?
- Who should conduct the due diligence?

# Developing a Due Diligence Plan: Questions to Ask



- Technical Questions
  - Data security certifications
  - Access controls and security (e.g., multi-factor authentication, encryption)
  - Location of data storage (cloud, overseas)
  - Privacy posture
  - Risk assessments, auditing, results sharing

- Policy/Governance Questions
  - Structure of the data security organization and line of contact between you and the vendor
  - Insurance
  - Employee training
  - Notice of change in operations, certifications
  - Data breach notification and cooperation
  - Audit rights

# Contracting with Your Vendor


Davis Polk

# Know Your Obligations

What are the relevant jurisdictions?

What are your legal obligations under the laws of those jurisdictions?

What promises have you made in your privacy policies or other public disclosures?

Do you have any relevant contractual obligations to third parties?

# Key Legal Regime #1: CCPA/CPRA

## AVOIDING THE "SALES" TRAP WHEN CONTRACTING WITH VENDORS

- The CCPA introduced an enhanced set of requirements around "**sales**" of personal information
  - "**Sale**" defined to include:
    - Selling, renting, releasing, disclosing . . . transferring or otherwise communicating . . . consumer personal information . . . by the business to "third parties" . . . for monetary or other valuable consideration
  - Covered businesses engaged in "sales" must provide increased disclosures and give consumers the right to "opt-out" of such sales
  - Definition of "sale" includes several exceptions (e.g., sharing with service providers, user-directed transfers, passing through opt-outs, and certain mergers and acquisitions activity)
- In order to avoid a transfer to a service provider or contractor qualifying as a "sale," a business must observe certain contracting requirements

# Key Legal Regime #1: CCPA/CPRA

## SERVICE PROVIDER EXCEPTION

- A "**service provider**" processes personal information on behalf of a business and receives consumer's personal information under a written contract
- The written contract must prohibit the service provider from:
  - Selling the personal information (or sharing the personal information except under limited circumstances)
  - Retaining, using, or disclosing the personal information for any purpose other than for the purposes specified in the contract or outside of the direct business relationship
  - Combining the personal information with personal information that the service provider receives from another person or collects from its own interaction with the consumer (except as may be permitted by the CCPA's/CPRA's implementing regulations)*

* Requirement added by CPRA

- The CCPA/CPRA imposes certain obligations directly on service providers:
  - To cooperate with and assist businesses in providing requested personal information in response to verifiable consumer requests
  - To correct or delete personal information or limit the use of sensitive personal information in response to such requests
- Subprocessing
  - There are additional requirements if a service provider engages another person to assist in processing personal information on behalf of the business
  - The service provider must notify the business of that engagement
  - The engagement must be pursuant to a written contract with the same requirements as apply to the service provider

# Key Legal Regime #1: CCPA/CPRA

## ADDITIONAL CONTRACTING REQUIREMENTS ADDED BY THE CPRA

A business that collects a consumer's personal information and sells it to or shares it with a third party, or that discloses it to a service provider or contractor for a business purpose, must enter into an agreement that:

- Specifies that the personal information is sold or disclosed by the business only for limited and specified purposes
- Obligates the third party to comply with applicable obligations under the law
- Grants the business the right to take reasonable and appropriate steps to ensure that the third party uses the personal information in a manner consistent with the business's obligations
- Requires the third party to notify the business if it makes a determination that it can no longer meet its obligations
- Grants the business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information
- For contractors, includes a certification that the contractor understands their obligations and will comply with them

# Key Legal Regime #2: GDPR

## USE OF PROCESSORS

The GDPR requires that processing by a processor be governed by a contract that is binding on the processor and requires that the processor:

- Only process personal data, or transfer personal data internationally, pursuant to documented instructions from the controller, unless required to do so by law
- Implement appropriate technical and organizational measures to ensure a level of security appropriate to protect against the risks presented by processing
- Ensure that persons authorized to process the personal data are subject to appropriate contractual or statutory obligations of confidentiality
- Immediately inform the controller if an instruction violates the GDPR or other law
- Assist the controller by appropriate technical and organizational measures in fulfilling the controller's obligation to respond to data subjects' requests
- Notify the controller without undue delay upon becoming aware of a personal data breach and cooperate in taking reasonable steps to assist in remediating such breach
- Provide reasonable assistance to the controller with any data protection impact assessments and prior consultations with supervisory authorities
- Delete or return all personal data to the controller after the end of the provision of relevant services, and delete existing copies unless otherwise required by law to be retained
- Provide the controller with all information necessary to demonstrate compliance with GDPR obligations, including information adequate to provide the controller with sufficient guarantees that processing performed by the processor will meet the requirements of the GDPR and protect data subjects' rights
- Allow for and contribute to audits conducted by the controller or another auditor mandated by the controller

# Key Legal Regime #2: GDPR

## SUBPROCESSING

With respect to subprocessing, the processor has obligations:

- Not to engage a subprocessor without prior written authorization of the controller
- To inform the controller of any intended changes concerning the addition or replacement of subprocessors, giving the controller the opportunity to object
- To impose on the subprocessor the same data protection obligations imposed on itself pursuant to the data processing agreement
- To remain fully liable to the controller for the performance of the subprocessor's obligations under the agreement

# Key Legal Regime #2: GDPR

## OTHER CONSIDERATIONS

- If cross-border transfers are contemplated, standard contractual clauses should be put in place
  - The validity and terms of the standard contractual clauses are in flux due to Schrems II and recently proposed modifications by the European Commission

- Agreements that are intended to contemplate a controller/processor relationship but do not include the terms required under the GDPR could cause the relationship to be controller/controller by default (and thus lead to certain disclosure obligations) or be viewed as violating the GDPR

# Data Processing Agreements

## KEY TERMS AND POINTS OF NEGOTIATION

- Definitions
  - Tailor the definitions based on the vendor agreement to which the DPA is attached
  - Ensure key definitions (e.g., “Personal Information”/”Personal Data”) are broad enough to cover all applicable jurisdictions
- Processing of Protected Personal Data
  - Processing only in accordance with the DPA unless otherwise required by applicable law
  - Duration of processing
  - Confidentiality and restrictions on sale, sharing, retention, transfer, and disclosure
  - Other formalities required by applicable law
- Subprocessing
  - Due diligence / approval process
  - Liability
  - Monitoring and notification of noncompliance

# Data Processing Agreements

## KEY TERMS AND POINTS OF NEGOTIATION (CONT.)

- Personal Data Breaches and Other Security Incidents
  - Notification in the event of a personal data breach or other security incident
    - Scope of covered incidents (only personal data breaches or also other security incidents)
    - Trigger for notification (actual, reasonably suspected, attempted)
    - Timing of notice
  - Third-party notification obligations
  - Assist in the investigation, notification, and remediation of a personal data breach
  - Ability to suspend service until remediation
- Data Subject Rights
  - Assist in implementation of appropriate technical and administrative measures
  - Notification of data subject requests and cooperation in responding to such requests
- Other Assistance
  - Data protection impact assessments
  - Regulatory inquiries and consultations

# Data Processing Agreements

## KEY TERMS AND POINTS OF NEGOTIATION (CONT.)

- Security
  - Minimum requirements: to maintain reasonable physical, technical and administrative measures to ensure a level of security appropriate to the risk, for example:
    - Business contingency and disaster recovery plans
    - Pseudonyimization and/or encryption
    - Ability to restore personal data in a timely manner
    - Process for regularly testing effectiveness of measures
  - Potential additional requirements:
    - Industry standards / best practices
    - Pass through of your company's own express information security requirements
- Audit Rights
  - Obligation for service provider to maintain records
  - Third-party vs. direct audits
  - Frequency
- Deletion or Return of Protected Personal Data

# Data Processing Agreements

## KEY TERMS AND POINTS OF NEGOTIATION (CONT.)

- Risk Allocation
  - Scope of indemnity
    - Contract breaches vs. absolute indemnity for processing or data breaches
    - Violations of applicable law
  - Limitation of liability
    - Negotiation of caps
    - Common exclusions: gross negligence, willful misconduct, and fraud
    - Additional exclusions: breaches of confidentiality, breaches of obligation to cooperate, indemnity
- Further Assurances
  - Updates may be needed as laws and regulations evolve

# Managing the Vendor Relationship and Dealing with Data Breaches

4

Davis Polk

# Ordinary Course Best Practices

## PERIODIC VENDOR ASSESSMENTS

- Vendor diligence doesn't end when the contract is signed
  - Legal obligations persist:
    - e.g., periodic risk assessment under NYDFS requires regulated entities to reevaluate risks from vendors
  - Business/legal risk from the vendor may change
  - Amount/type of information exposed to the vendor may change
- How frequently should reviews be undertaken?
- How to ensure effective periodic review?
  - Set expectation with vendors during diligence
  - Build in contractual requirements
  - Ensure sufficient expertise (internal/external) to conduct periodic review
- What to ask for in a periodic review?
- What red flags should you look out for?

# Dealing with a Vendor Data Breach

## Do's

- Focus on containment/recovery (at first)
  - Is intrusion/attack/breach ongoing?
  - Is intrusion/attack/breach limited to the vendor's environment?
  - Are there minimum viable assurances you need?
  - Are there risk-based limitations or restrictions that you can implement (or require)?
- Consider best means of inducing cooperation
  - Understand that vendor may have less information than you (or they) would like
  - Understand that leverage and incentives may be complicated during immediate response period
- Keep track of required notification/reporting
  - Regulatory obligations
  - Contractual obligations
  - Insurance policies
- Handle information from the vendor with care

## Don'ts

- Don't assume the root cause of an incident lies with the vendor
- Don't let arguments over liability/blame impede recovery. But also don't…
  - Waive any rights, or
  - Express views prematurely regarding responsibility/fault
- Don't assume the vendor has the full picture, even if they purport to
  - Don't expect answers to questions that the vendor probably can't answer
  - But don't shy away from asking them, either
- Don't get ahead of what vendor has said about the breach
  - Make clear where information is coming from
  - Don't express the vendor's statements as if they were based on first-hand knowledge

# SolarWinds Breach

## CASE STUDY

SolarWinds is an IT vendor that provides network management software.

- In 2020, attackers successfully penetrated SolarWinds, and tampered with routine software update files that SolarWinds then pushed to its clients.
- The updates delivered malicious toolkits that the attackers used to backdoor their way into the clients' systems, where they established persistence.
- It is estimated that approximately 18,000 clients were directly affected (with additional downstream victims yet to be determined)

- The Cybersecurity and Infrastructure Security Agency (CISA) advised all civilian agencies to disable use of Orion
  - The Department of Defense, DOJ, State Department, and Treasury Department were among the federal agencies confirmed to have been affected
- Many large corporate Orion users affected, including Cisco, Intel, Nvidia, and Deloitte
  - Affected organizations are still working to investigate the impact
  - Many have made public statements about being affected by the breach
- State-sponsored attackers likely sought:
  - emails of corporate executives
  - files about sensitive technologies under development
  - other ways to compromise more systems in the future

# SolarWinds Breach: SEC Filings

## CASE STUDY

"In the fourth quarter of 2020, we became aware of reports that an update to widely used IT infrastructure management software provided by one of our vendors, SolarWinds Corporation, had been compromised by attackers, and we are investigating these reports. To date, cybersecurity incidents have not resulted in a material adverse impact to our business or operations, but there can be no guarantee we will not experience such an impact."

"The cyberattacks uncovered in late 2020 known as "Solorigate" are an example of a supply chain attack where malware was introduced to a software provider's customers, including us, through software updates. The attackers were later able to create false credentials that appeared legitimate to certain customers' systems. We may be targets of further attacks similar to Solorigate as both a supplier and consumer of IT."

"SolarWinds' investigations into these matters are preliminary and on-going, and SolarWinds is still discerning the implications of these security incidents. During the course of these investigations, SolarWinds may become aware of new or different information. At this time, SolarWinds is unable to predict any potential financial, legal or reputational consequences to the Company resulting from this incident, including costs related thereto."

# Q&A

To ask a question from your touchtone phone, press *1.
To exit the queue, press *1 again.

You may also use the Chat function to ask questions, or email questions to **lawquestion@straffordpub.com**

CLE CODE: **TLHGJC**

*Tell us how we did!*

Look for our 'Thank You' email (which you should receive within 24 hours) for details and a link to the program survey and attendance attestation.

*Not a Passholder Yet?*

# *Try the CLE Individual Annual Pass*

- Attend unlimited live webinars in any of our legal practice areas – we produce over 750 advanced live CLE webinars each year
- Get unlimited access to hundreds of recorded webinars
- Get all your CLE credits for one price

Simply respond to the email you will receive after the program and **we will rebate the cost of this webinar from the pass price!**

---

Did you know that Strafford offers **significant discounts for group participation?**

- Add colleagues to participate with you on the same device for up to 67% off, OR
- if they'd rather attend on their own device, add additional connections/devices and get 25% off.