



SO YOU THINK YOU KNOW YOUR SAAS SECURITY AGREEMENTS?

John G. Bates, Clarity Insights

Maryjane Hall, Federal Home Loan Bank of Chicago

Helena M. Ledic, CSC

Peter T. Wakiyama, Pepper Hamilton LLP



April 24, 2019

Your Presenters



**John G.
Bates**

General Counsel / Chief
Information Security
Officer,
Clarity Insights

jbates@clarityinsights.com



**Maryjane
Hall**

Vice President Legal and
Government Affairs and
Assistant General Counsel,
Federal
Home Loan Bank of
Chicago

mjhall@fhlbc.com



**Helena M.
Ledic**

Associate General
Counsel, CSC

helena.ledic@gmail.com



**Peter T.
Wakiyama**

Partner,
Pepper Hamilton LLP

wakiyama@pepperlaw.com

Disclaimer: The views expressed by the presenters are not necessarily the views shared or endorsed by their corporations, law firm or CSC®. This presentation is for informational purposes only and does not constitute legal advice.

Our Agenda

- Due Diligence Planning
- Security Risk Assessments
- Warranties & Indemnities
- Operational Risk Assessments
- SaaS Vendor Review
- Questions

Our Agenda

- **Due Diligence Planning**
- Security Risk Assessments
- Warranties & Indemnities
- Operational Risk Assessments
- SaaS Vendor Review
- Questions

Due Diligence Planning

- Assemble Multi-Disciplinary Team including Technical, Security, Business and Legal
- Amount and scope will vary on the project
- Prepare a plan and checklist, particularly with larger projects

Technical Due Diligence – Examples

- Product demos
- Customer references
- Solution architecture review
- Technical documentation review
- Policy and procedure reviews (security, business continuity, etc.)

Security Due Diligence – Sample Questions

- How is the data protected via capabilities and policies?
- How is the application/solution protected?
- Does the vendor meet general and industry-specific security and compliance standards?
- Does the vendor meet the unique security requirements of your industry?

Business Due Diligence – Examples

- Public records searches
- Review of vendor's legal structure and ownership (public or private, sole or multiple owners, state of business formation)
- Financial performance
- Financial status

Legal Due Diligence – Examples

- Lien searches
- Litigation searches
- IP review (any patents that could prevent competitive solutions or customer from taking in-house)
- Subcontractor relationships
- Reliance on third party vendors
- Data processing and storage facility locations
- Reliance on off-shore developers

Customer Risks Not Fully Appreciated

- Insufficient scoping of implementation
- Business Continuity – no Plan B
- Access to Data Assets

Vendor Concerns

- Incomplete or incorrect sales tax analysis
- Inadequate protection of vendor IP rights; loss of IP rights (open source)
- No rights to valuable usage data, de-identified data or aggregate data

Our Agenda

- Due Diligence Planning
- **Security Risk Assessments**
- Warranties & Indemnities
- Operational Risk Assessments
- SaaS Vendor Review
- Questions

**Who in the room has
had a security incident within
the previous year?**

SaaS Security Risk Assessments



Security Control Assessments

SIG – Addresses risk controls across 16 risk area

Dashboard	Tab	% Comp
<p>The Dashboard provides you with a quick and easy reference to determine if the required sections of the SIG have been completed. As questions are answered, either directly or by being pre-filled, the Dashboard will track the completion percentage of each section.</p>	Terms Of Use	N/A
	Business Information	34%
	Documentation Request List	N/A
	SIG Lite	100%
	A. Risk Management	100%
	B. Security Policy	100%
	C. Organizational Security	100%
	D. Asset Management	100%
	E. Human Resources Security	100%
	F. Physical and Environmental	100%
	G. Communications and Operations Management	100%
	H. Access Control	100%
	I. Information Systems Application Development and Maintenance	100%
	J. Incident Event and Communications Management	100%
	K. Business Continuity and Disaster Recovery	100%
	L. Compliance	100%
	M. Mobile	100%
	P. Privacy	100%
	Q. Software Security	100%
	V. Cloud Security	100%
	Z. Additional Questions	N/A
	Glossary	N/A
	Formula Notes	N/A
	Full	N/A

Security Control Assessments

Control Frameworks

- NIST 800-53 Rev 5
- ISO 27001
- SIG
- SIG Lite
- SANS20
- PCI-DSS
- FFIEC

It's for everybody

Less technical than NIST

It's HUGE!

Less huge

A good place to start

Credit card processors

Banks

Our Agenda

- Due Diligence Planning
- Security Risk Assessments
- **Warranties & Indemnities**
- Operational Risk Assessments
- SaaS Vendor Review
- Questions

Warranties and Indemnities

WARRANTY

A promise that something is true

Implied warranties

- Not explicitly stated
- But guaranteed unless disclaimed

Express warranties

- Explicitly stated in the contract

INDEMNITY

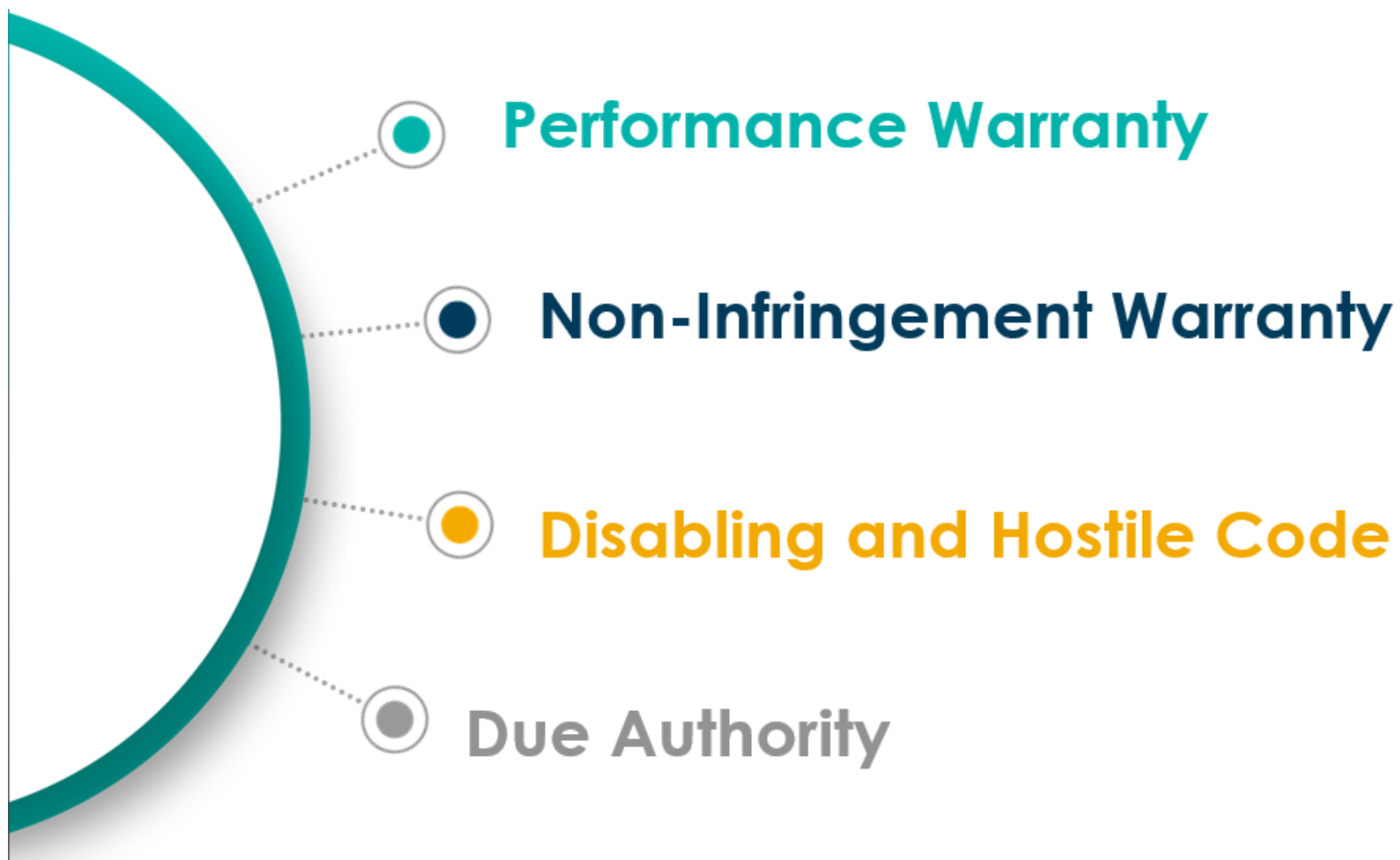
An obligation to

- Hold the customer harmless, and
- Remediate failure of essential purpose

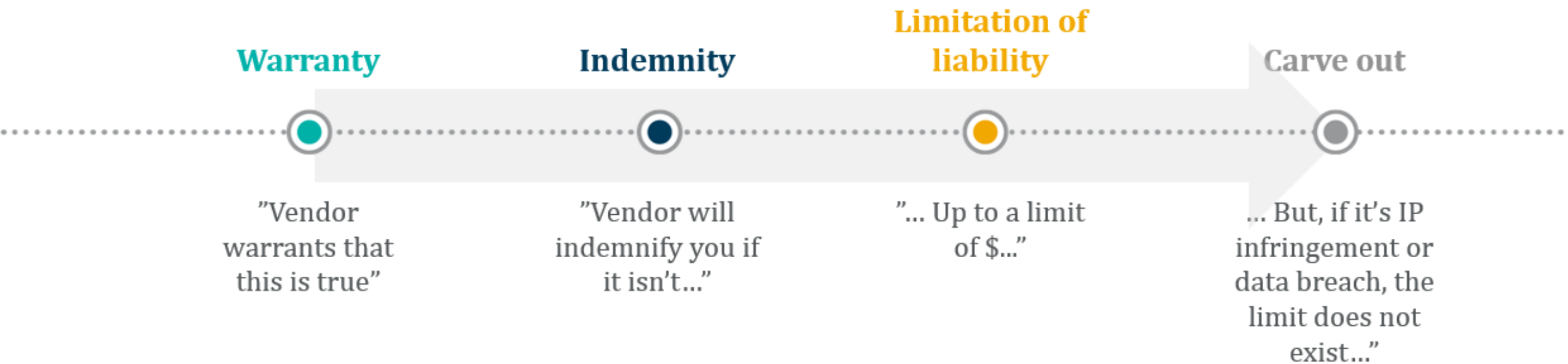
In the case of infringement

- Procure the right to use the service
- Modify or replace

Standard Warranties



Risk management through Warranty, Indemnity, Limitation of Liability, & Carve-Outs



Indemnities

An indemnity is based on the idea that the indemnifying party is responsible for

- Its own wrongdoing
- Liability that rightfully should be assumed by the indemnifying party because it is in the best position to prevent or guard against it

Standard Indemnities

- Breach of warranty - Including non-infringement
- Breach of confidentiality
- Negligent acts, omissions or intentional wrongdoing of vendor

Breach of Contract

Requires a breach of contract due to failure to deliver, or delivery rejected or revoked

Actual damages for **economic loss**

- Arise from the failure to perform as expected
- Quantified and proven
- Breach of a duty
- Actual proximate cause, and
- Reliance
- Includes costs of performance and preparation minus costs that would have been incurred anyway

Duty to mitigate

Warranty

Requires a breach of contract discovered after acceptance

Must prove actual, quantifiable loss with reasonable certainty.

Direct damages

- **Difference in value of the product** as delivered vs the value of the product as warranted
- Incidental damages (expenses and costs) incurred responding to an alleged breach of warranty
- Cost to obtain the right to use, modify or replace

No duty to mitigate

Indemnity

Does not requires a breach of contract

Damages may include

- **Losses** arising out of the action of a third party (e.g., patent troll or 3rd party IP owner)
- Compensation for **costs and expenses** regardless of economic loss
- Cost to obtain the right to use, modify or replace

No duty to mitigate

Common Carve-outs from Liability

- Customer modifications
- Use inconsistent with the authorized use
- Combination with software or other technology not provided by the licensor
 - **NOT RECOMMENDED**

Use in combination with products not provided by the vendor

Limit this carve-out to

- Exclude claims resulting from use with products **reasonably necessary for the intended use** or contemplated in the vendor's documentation, or
- Exclude claims if the other products do not perform a function in the alleged infringing activity unless the infringement could not occur but for the use of the product in combination or use with the vendor's software

Our Agenda

- Due Diligence Planning
- Security Risk Assessments
- Warranties & Indemnities
- **Operational Risk Assessments**
- SaaS Vendor Review
- Questions

Operational Risk Assessments – Vendor Risks

CATEGORY	EXAMPLES	
Information Technology / Security	Privacy breach	Identity fraud
	Intellectual property theft	Data corruption
	Denial/Loss of service	Data loss
Financial/Credit	Vendor bankruptcy	Transaction / Reporting Fraud
	Price / Exchange rate instability	Collateral mismanagement
	Unrealized return on investment	Collateral valuation errors
Operational	Business continuity / DR	Safety / OSHA/ EPA incident
	Poor quality / Performance	Poor customer service/ Reputational risk
	Damage to assets	Late delivery / Theft
Legal	Contract liability	Human Resources incident
	Contract dispute	Labor dispute/grievance
	Regulatory action	International law conflict
Brand/reputation	Brand damage	Communication crisis
	Customer dissatisfaction	Loss of investor confidence
	Competitive pressure	Loss of employee confidence

Operational Risk Assessments – Operations & Technology Risk Questions



Is the annual spend on the vendor is greater than \$__ _MM?

Is the vendor a necessary part of the company's disaster recovery or business continuity plans?

Is the company dependent on

- Vendor technology
- Vendor outsourced business services (e.g., payroll, HR, IT)

Is the company dependent on the vendor for services to third parties (agency risk)?

Does the vendor have access (physical or logical) to PII/NPI/PHI or sensitive non-public information? [Consider physical records, network access to records or vendor stored records]

How long will it take to get up and running with a replacement vendor?

Operational Risk Assessments

Credit Risk Questions

Would the company or any of its affiliates or investors suffer a **credit loss** if the vendor or its service provider failed to provide its services?

What is the risk on **non-payment** of advanced funds or high volumes of product to the vendor?

- Risks associated with cash management and credit, and managing risk mitigates such as collateral and other pledged assets.
- Risk associated with vendor's failure to perform.
- Risks associated with replacing transactions with new transactions to meet business goals.

Does the vendor provide services related to **assets or collateral servicing**, transfer, settlement, safekeeping, or reporting for the company or its affiliates or investors?

Operational Risk Assessment Examples

Financial Reporting Risk

- **Financial statements** and supporting ledgers are insufficiently detailed or do not accurately represent the financial condition of the vendor
- Regulatory reporting, financial filings, GAAP and other **compliance risks**
- Risk of unauthorized acquisition, use or **disposition of assets**

Fraud Risk

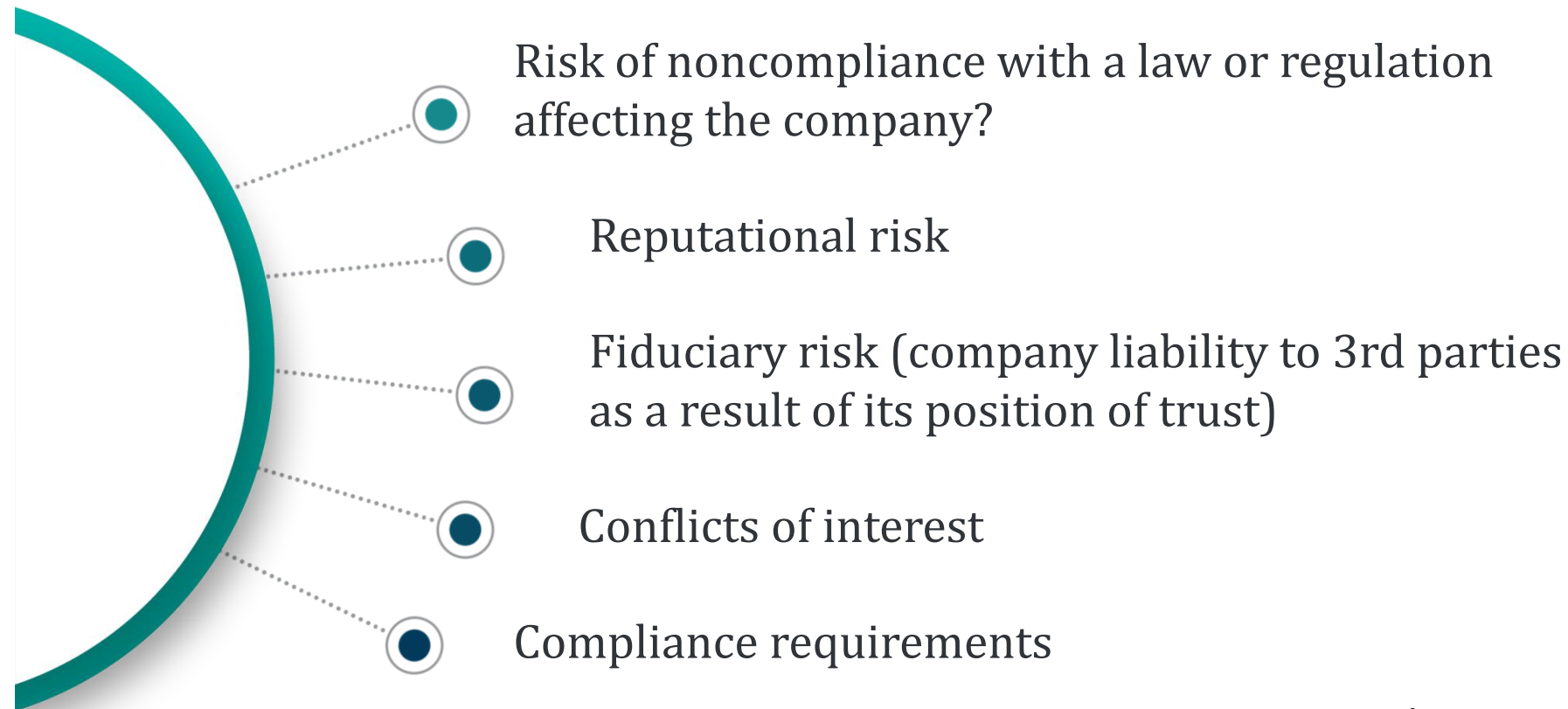
- **Misrepresentation** of financial results and records
- **Misappropriation** of assets /fraudulent expenses
- **Misuse** / theft of third party assets
- **Hiring** practices and policies

Operational Risk Assessments

Strategy & Governance Risk

- Is the vendor a **strategic partner**?
- Risks from the vendor **changing strategies** or failing to do so
- Risk to company's business strategies, product plans, shareholder expectations due to **disengagement**
- Risks related to vendor's **management** policies and processes
 - Management style and strategy
 - Sufficiency of management skill
 - Risk attitude of management
 - Conflicts of interest
 - Tone at the top of the corporate culture

Operational Risk Assessments – Legal & Compliance Risk Examples



Our Agenda


- Due Diligence Planning
- Security Risk Assessments
- Warranties & Indemnities
- Operational Risk Assessments
- **SaaS Vendor Review**
- Questions

SaaS Vendor Reviews

Quick Litmus Tests

- Do you encrypt in transit and in rest? Are all corporate laptops encrypted?
- Are development, production, test environments completely separate from one another?
- Is multifactor authentication (MFA) utilized by the entire company?
- Does everyone have Single Sign On (SSO)?
- How difficult are your passwords and how frequently do they need to be changed?
- Is a full-time employee in charge of Data Security?
- If you have multiple servers in various locations, how are all the different systems patched? How long does it take to push a patch across the entire enterprise?
- Have you had any security incidents or data breaches in the last five years?
- How do you track and/or report any security incidents?

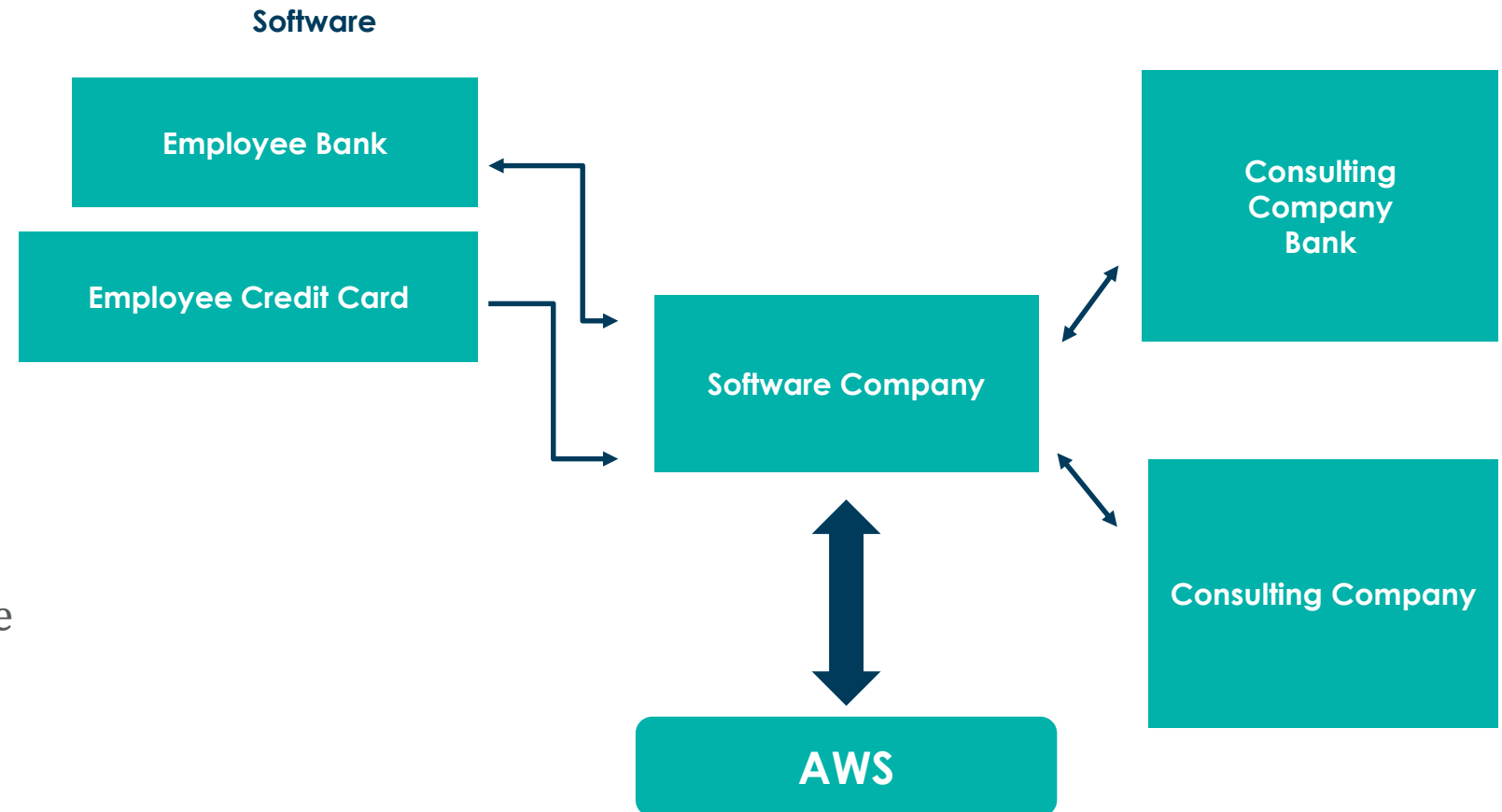
SaaS Vendor Reviews – Techniques

- 
- Follow the data, ask if any other company has access (Contractor, Third-Party software, data centers).
 - Meet with each vendor to understand whether there are underlying unknown vendors under vendors.
 - Request certifications at each level. Review them and determine if they have been gerrymandered. Scope can be unreasonably small.
 - Request meeting with individual who leads Security Program at each vendor. They may have certifications but not understand them.

SaaS Vendor Review Example #1

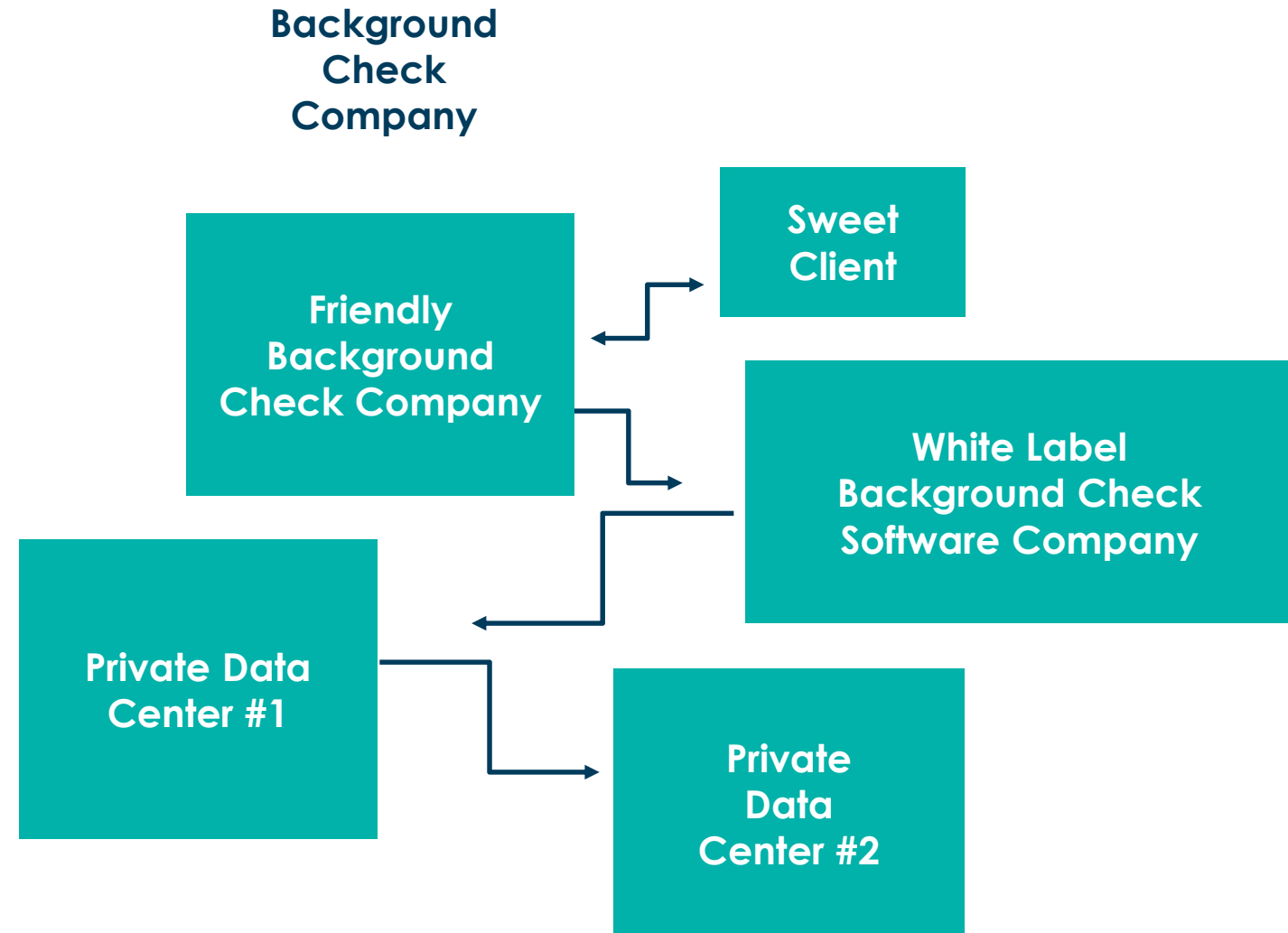


- Credit card and banking data (PCI).
- Expense Software Company PCI Certified.
- PCI Report indicated Apple laptops do not have Anti-Virus software because Macs do not suffer from viruses.



SaaS Vendor Review Example #2

- No certifications at Friendly Background Check Company.
- CEO was in charge of IT security.
- White Label Background Check Software Company not certified.
- DC #1 and DC #2 both SOC 1 certified.
- Software company data on DC #1 and #2 was unencrypted at rest.



Our Agenda

- Security Risk Assessments
- Warranties & Indemnities
- Operational Risk Assessments
- Vendor Lifecycle Management
- SaaS Vendor Review
- **Questions**

Questions?

Thank you for attending!

John G. Bates

jbates@clarityinsights.com

Maryjane Hall

mjhall@fhlbc.com

Helena M. Ledic

helena.ledic@gmail.com

Peter T. Wakiyama

wakiyama@pepperlaw.com

A reminder about the benefits of ACC membership...

- Free CLE, like the one you're attending right now
- Roundtables
- Networking meetings
- Special events
 - Spring Fling, Fall Gala, Diversity Summer Program, Golf Outing, Pro Bono clinics, Charity Softball Game & Family Fun Day, and more!
- Access to ACC resources, including:
 - ACC Newsstand (customizable updates on more than 40 practice area)
 - ACC Docket Magazine
 - InfoPAKs
 - QuickCounsel Guides
- **For more information or to refer a new member, see your hosts today or contact Chapter Administrator, Chris Stewart, at ChrisStewart@ACCglobal.com.**

