

# Information Security in Contracts and Cyber-Liability Insurance



**HCCA Indianapolis  
Regional Conference  
2018**

Nick Merker, CISSP, CPT  
Partner, Ice Miller LLP

**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## The Vendor Threat

**“At least 56% of  
respondents  
experienced a third  
party data breach in  
2017, a 7% increase  
from 2016”**

2017 Data Risk in the Third Party Ecosystem  
Study from Ponemon Institute



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Vendor Originating Threats



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Vendors as Threat Vectors

- Increasing vendor reliance for critical operations
  - Payroll, IT outsourcing, etc.
- Vendors are not "external"
  - Critical access to company infrastructure
  - Movement of data and confidential information
  - Real-time integrations with vendors
- Vendor's vendors



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Vendor Risks

- Financial risks
- Location risk
- Business continuity and time to recovery risks
- Operational risks (quality, cost, performance, capacity)



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Contract Goals

- Risk Identification



- Mitigation



- Transfer



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Diligence - Areas of Concern

- Base Controls
- Application Controls
- Cloud Security
- Infrastructure Controls
- Physical Security
- Backup & Recovery
- Electronic Transfer
- Privacy Management
- Physical Transfer
- Decommissioning & Destruction
- Physical "Paper" Management
- External Party Management

## Confidentiality

- What is Confidential Information?
- What are obligations?
- How long do obligations last?
- What are subpoena procedures?



## Key Contractual Concerns

- Vendor Business and Location
- Data Access and Segregation
- Personnel Issues
- Audit
- Data Security
- Breach Response
- Disaster Recovery and Business Continuity
- Data Sharing
- Insurance
- Laws and Regulations
- Privacy

**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Risk Identification and Assessment / Information Security Standard



Privacy Technical Assistance Center  
U.S. Department of Education



Center for  
Internet Security®



PROTECTING AMERICA'S CONSUMERS



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

# Customer Privacy Concerns

- Identify nature and categories of data
- Limit use and processing of data
- Limits on transfer of data
- Adherence to data protection laws
- Model contracts
- Flow-down provisions
- Termination



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

# Data Breach Response and Notification

- Notification requirements
- Notice requirements
- Who pays?



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Downstream Obligations (e.g. subcontractors)

- Disclosure of subcontractors
- Adhere to vendor obligations
- Vendor indemnification
- Personnel management

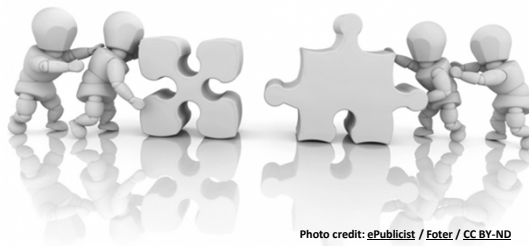


Photo credit: ePublicist / Foter / CC BY-ND

**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Termination and Data Destruction

- Transition
- Certify destruction
- Compliance concerns



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Warranties, Representation, and Indemnity

### Warranties:

- Enacted, and maintains an info. sec. program
- Confidentiality obligations
- Software and/or services are free of security defects

## Warranties, Representation, and Indemnity

### Limitations:

- 3x the contract value
- Liquidated damages



# Warranties, Representation, and Indemnity

## Indemnification:

- Data breaches
  - E.g.: Third party damages
- Breach of confidentiality obligations
- Breach of warranties

## Insurance



## Insurance

**First Party  
Insurance** **and** **Third Party  
Insurance**

## Insurance

**Cyber Security**  
**Custom Insurance Coverage Checklist - v1.1**

This coverage checklist is based on answers you provided about your business. It is for use as a guide when shopping for insurance and talking to agents. It is for informational purposes only. Please consult with your insurance agent for professional insurance advice.

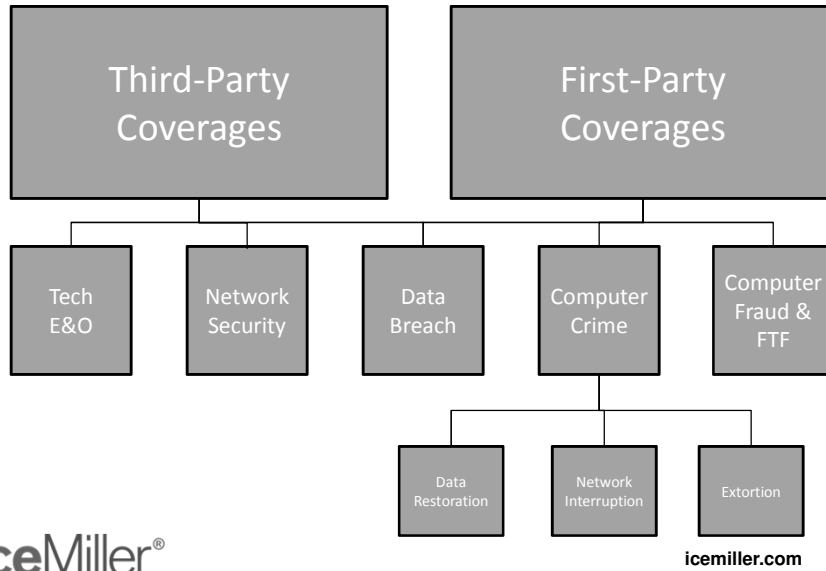
**Your Coverage Summary**

- ☒ Cyber Network, Security, and Information
- ☒ Cyber Errors, Omissions, and Wrongful Acts
- ☒ Cyber Communications and Media Liability
- ☐ Cyber Extortion Threat
- ☐ Cyber Terrorism
- ☐ Crisis Management Expenses
- ☐ Identity Theft

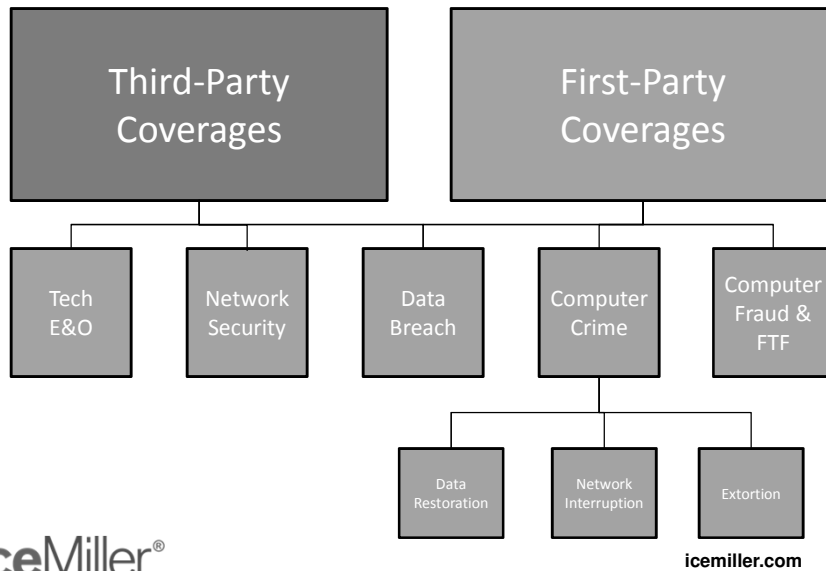
**Your Business**

- Your Business
- Your Business
- Your Business
- Your Business
- Your Business
- Your Business
- Your Business
- Your Business

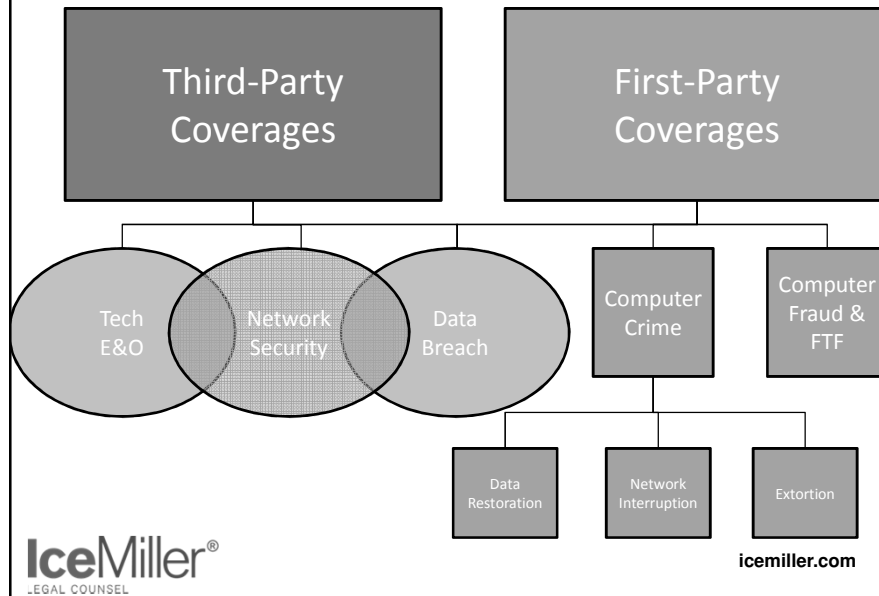
## Basic “Cyber” or “Tech” Insurance



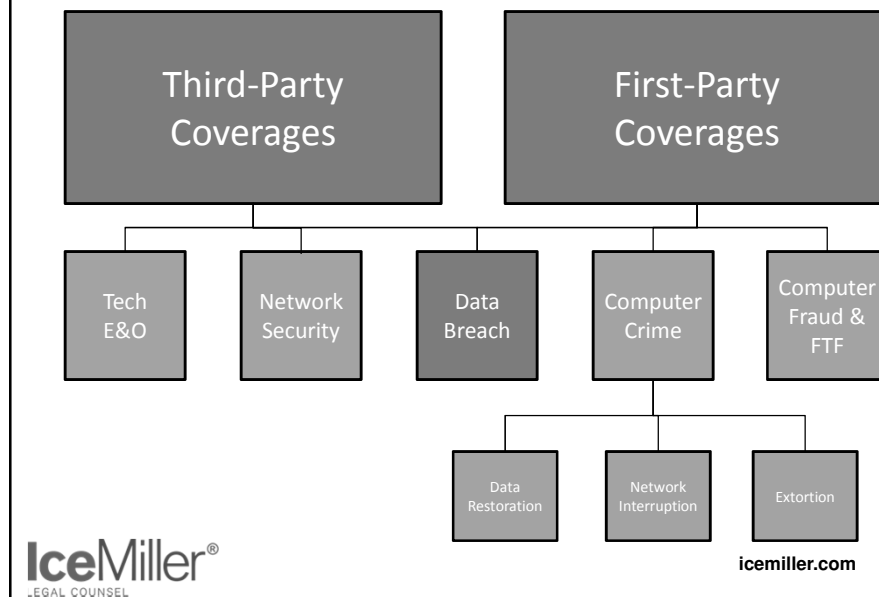
## Basic “Cyber” or “Tech” Insurance



## Basic “Cyber” or “Tech” Insurance



## Basic “Cyber” or “Tech” Insurance



## Basic “Cyber” or “Tech” Insurance

### Choosing the Right Specialty Data Breach Policy

- The types of data included in the coverage.
- Forensic Investigation Costs.
- Whether coverage is provided for data in the hands of third parties.
- Regulatory coverage.
- Business Interruption Coverage.
- Remediation coverages, including “Crisis Management,” “Credit Monitoring,” and “Public Relations Expenses.”
- Limits and control.
- Exclusions and retroactive dates.

Restoration

Interruption

Extortion

**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Basic “Cyber” or “Tech” Insurance

### Choosing the Right Specialty Data Breach Policy

- The types of data included in the coverage. ←
- Forensic Investigation Costs.
- Whether coverage is provided for data in the hands of third parties.
- Regulatory coverage.
- Business Interruption Coverage.
- Remediation coverages, including “Crisis Management,” “Credit Monitoring,” and “Public Relations Expenses.”
- Limits and control.
- Exclusions and retroactive dates.

Restoration

Interruption

Extortion

**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Basic “Cyber” or “Tech” Insurance

### Choosing the Right Specialty Data Breach Policy

- The types of data included in the coverage.
- Forensic Investigation Costs.
- Whether coverage is provided for data in the hands of third parties. ←
- Regulatory coverage.
- Business Interruption Coverage.
- Remediation coverages, including “Crisis Management,” “Credit Monitoring,” and “Public Relations Expenses.”
- Limits and control.
- Exclusions and retroactive dates.

Restoration

Interruption

Extortion

**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Basic “Cyber” or “Tech” Insurance

### Choosing the Right Specialty Data Breach Policy

- The types of data included in the coverage.
- Forensic Investigation Costs.
- Whether coverage is provided for data in the hands of third parties.
- Regulatory coverage.
- Business Interruption Coverage.
- Remediation coverages, including “Crisis Management,” “Credit Monitoring,” and “Public Relations Expenses.”
- Limits and control.
- Exclusions and retroactive dates. ←

Restoration

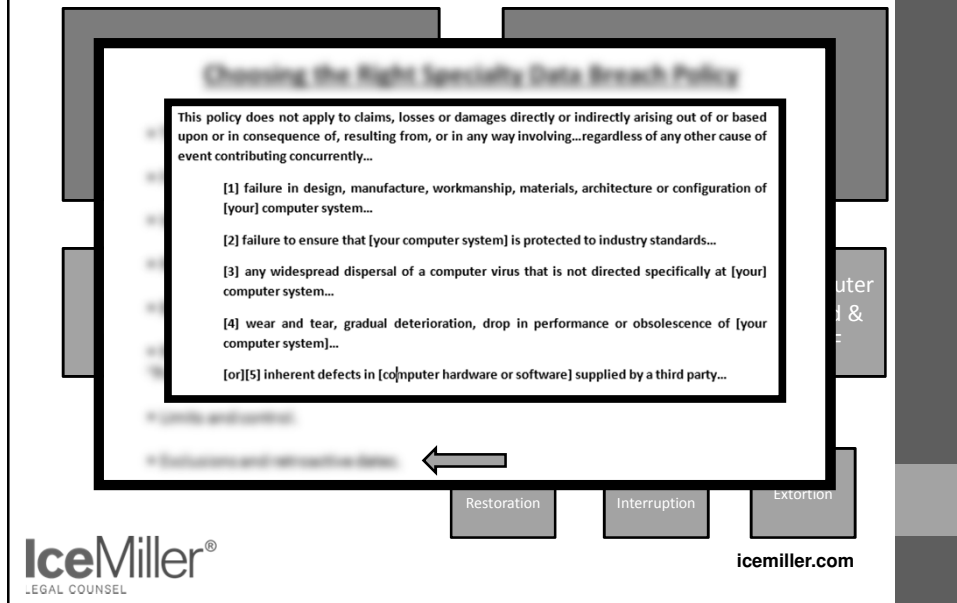
Interruption

Extortion

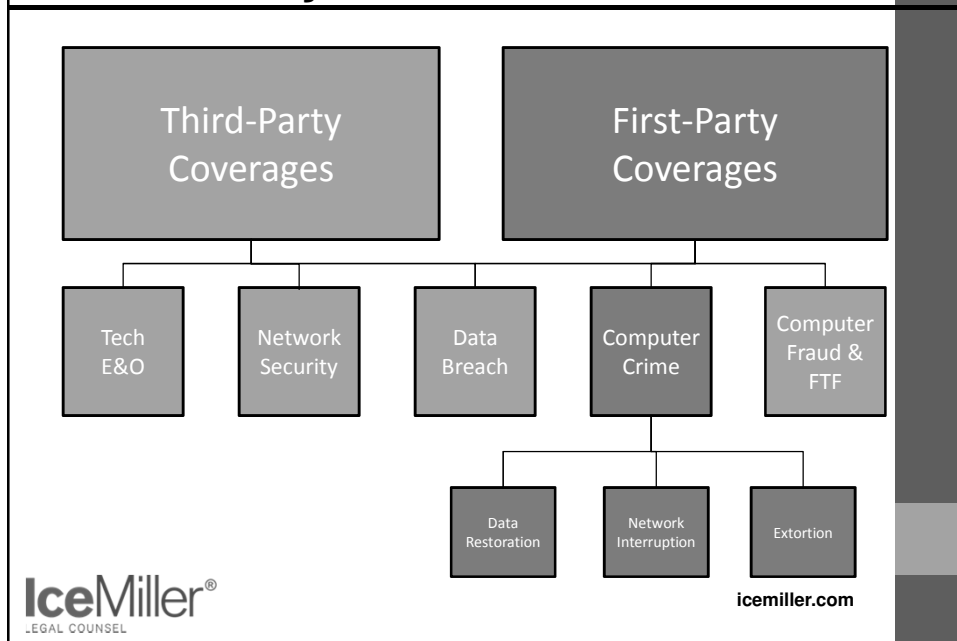
**IceMiller®**  
LEGAL COUNSEL

icemiller.com

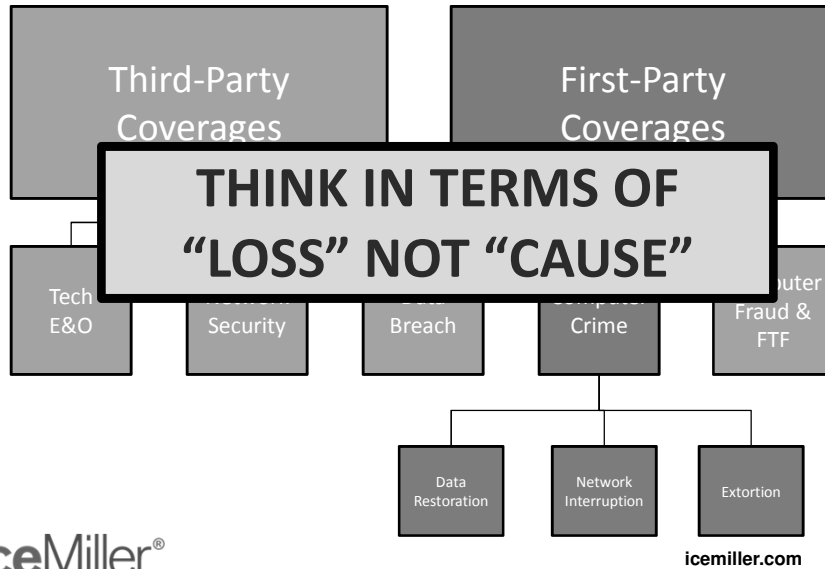
## Basic “Cyber” or “Tech” Insurance



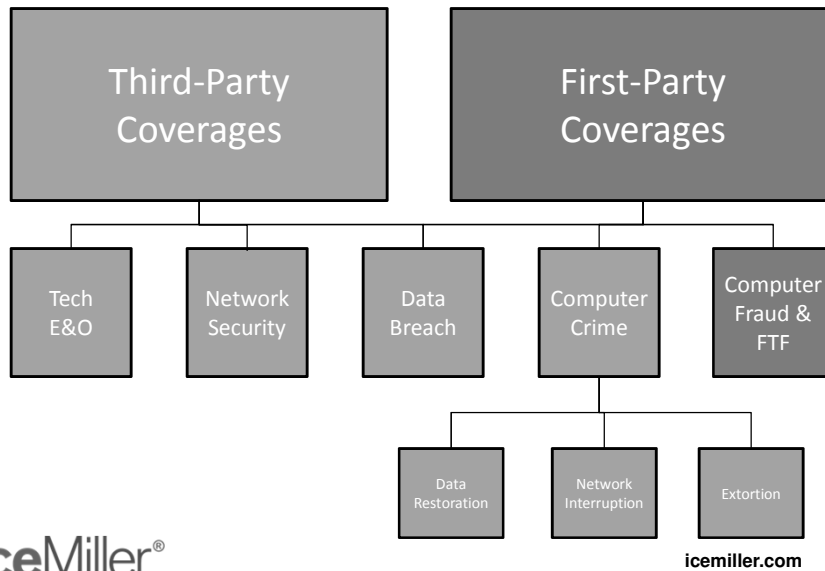
## Basic “Cyber” or “Tech” Insurance



## Basic “Cyber” or “Tech” Insurance

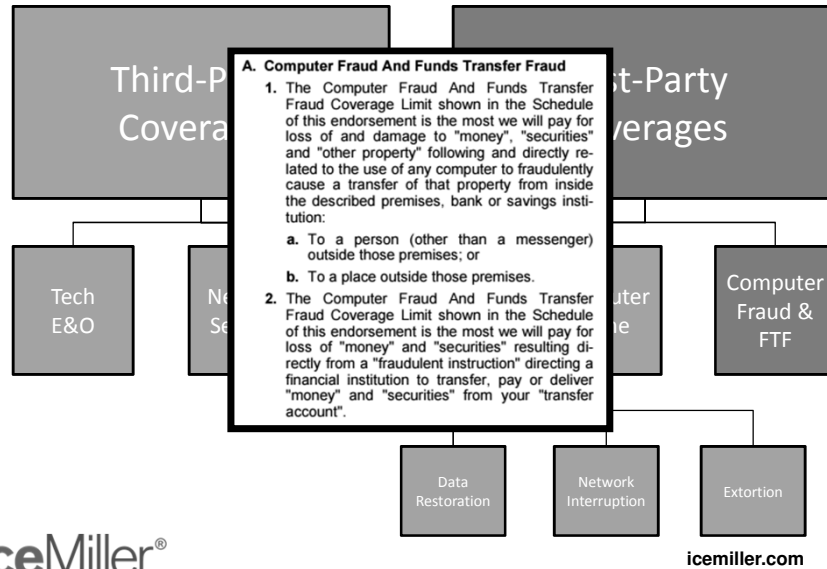


## Basic “Cyber” or “Tech” Insurance

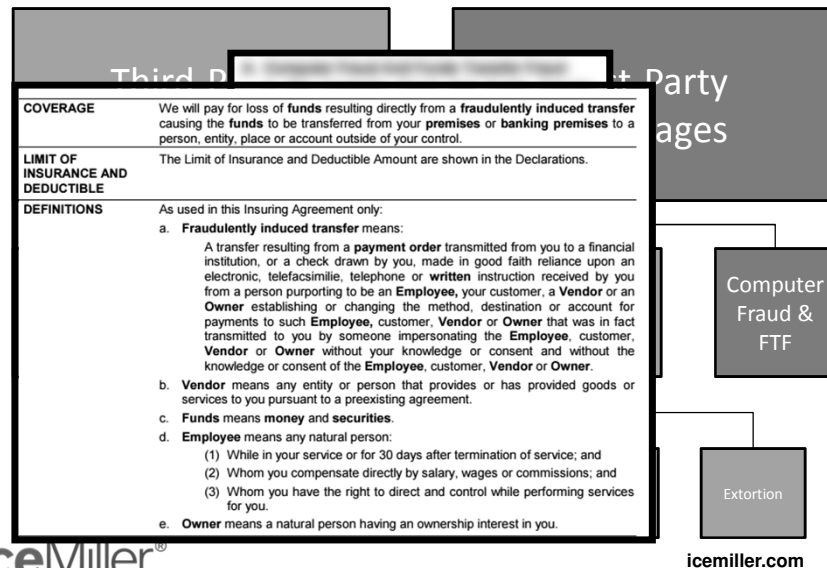




## Basic “Cyber” or “Tech” Insurance



## Basic “Cyber” or “Tech” Insurance



## Basic “Cyber” or “Tech” Insurance

Third Party Pages

|  |  |
|--|--|
| <b>COVERAGE</b>                          | We will pay for loss of funds resulting directly from a <b>fraudulently induced transfer</b> causing the <b>funds</b> to be transferred from your <b>premises</b> or <b>banking premises</b> to a person, entity, place or account outside of your control.  |
| <b>LIMIT OF INSURANCE AND DEDUCTIBLE</b> | The Limit of Insurance and Deductible Amount are shown in the Declarations.  |
| <b>DEFINITIONS</b>                       | As used in this Insuring Agreement only:   |
|  | <p>a. <b>Fraudulently induced transfer</b> means:</p> <p>A transfer resulting from a <b>payment order</b> transmitted from you to a financial institution, or a check drawn by you, made in good faith reliance upon an electronic, telefacsimile, telephone or <b>written</b> instruction received by you from a person purporting to be an <b>Employee</b>, your customer, a <b>Vendor</b> or an <b>Owner</b> establishing or changing the method, destination or account for payments to such <b>Employee</b>, customer, <b>Vendor</b> or <b>Owner</b> that was in fact transmitted to you by someone impersonating the <b>Employee</b>, customer, <b>Vendor</b> or <b>Owner</b> without your knowledge or consent and without the knowledge or consent of the <b>Employee</b>, customer, <b>Vendor</b> or <b>Owner</b>.</p> <p>b. <b>Vendor</b> means any entity or person that provides or has provided goods or services to you pursuant to a preexisting agreement.</p> <p>c. <b>Funds</b> means <b>money</b> and <b>securities</b>.</p> <p>d. <b>Employee</b> means any natural person:</p> <ol style="list-style-type: none"> <li>(1) While in your service or for 30 days after termination of service; and</li> <li>(2) Whom you compensate directly by salary, wages or commissions; and</li> <li>(3) Whom you have the right to direct and control while performing services for you.</li> </ol> <p>e. <b>Owner</b> means a natural person having an ownership interest in you.</p> |

Computer Fraud & FTF


Extortion

Social Engineering

IceMiller<sup>®</sup>  
LEGAL COUNSEL

icemiller.com

## Insurance Requirements in Contracts



IceMiller<sup>®</sup>  
LEGAL COUNSEL

icemiller.com

## Q/A



**IceMiller®**  
LEGAL COUNSEL

icemiller.com

## Thank You!

- Nick Merker
  - [Nicholas.Merker@icemiller.com](mailto:Nicholas.Merker@icemiller.com)
  - (317) 236 - 2337

**IceMiller®**  
LEGAL COUNSEL

icemiller.com