
Cyber Threats in the Real Estate Sector: Practical Remediation Steps

Jan 2020



Jonathan Fairtlough
Managing Director
Kroll



Ross Prindle
Managing Director
Duff & Phelps



Alope Chakravarty
Partner
Snell & Wilmer

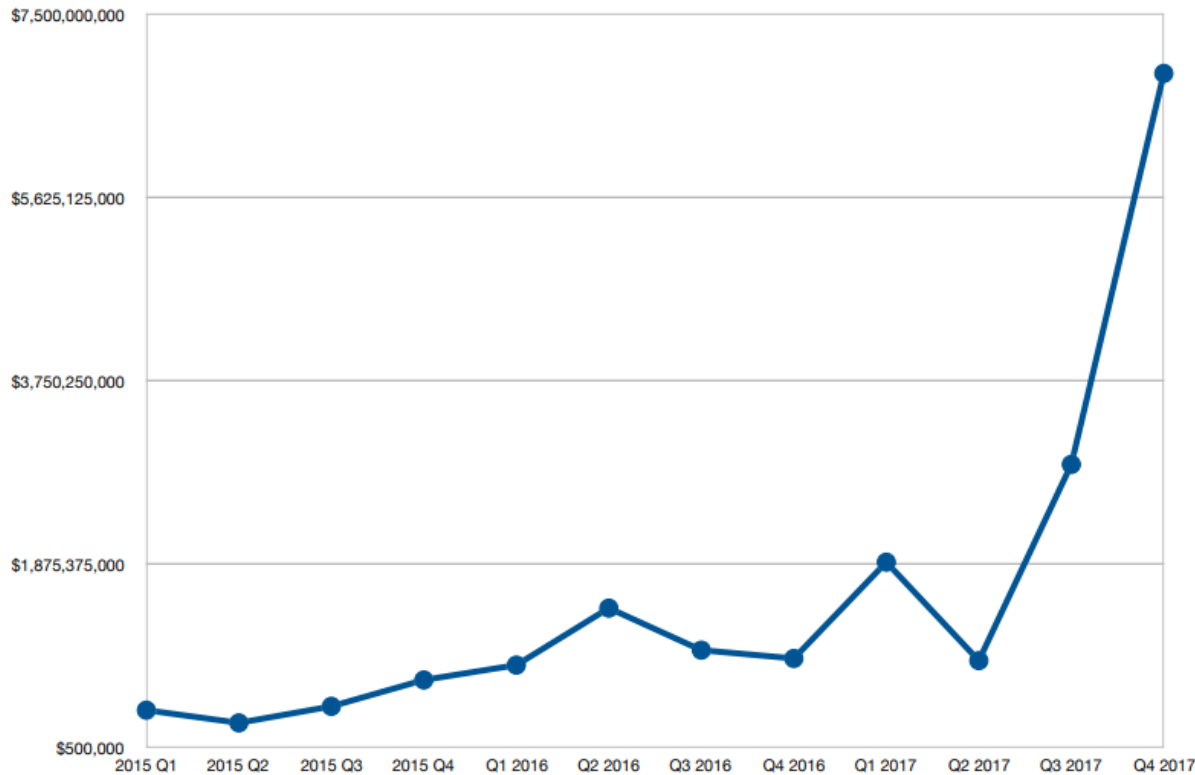
Disclaimer

Any positions presented in this session are those of the panelists and do not represent the official position of Duff & Phelps, LLC. This material is offered for educational purposes with the understanding that neither the authors nor Duff & Phelps, LLC or its affiliates are engaged in rendering legal, accounting or any other professional service through presentation of this material.

The information presented in this session has been obtained with the greatest of care from sources believed to be reliable, but is not guaranteed to be complete, accurate or timely. The authors and Duff & Phelps, LLC or its affiliates expressly disclaim any liability, including incidental or consequential damages, arising from the use of this material or any errors or omissions that may be contained in it.

©2020 All rights reserved. Notice: As part of our effort to inform you of changes in the law, Snell & Wilmer provides legal updates and presentations regarding general legal issues. Please be aware that these presentations are provided as a courtesy and will not establish or reestablish an attorney-client relationship or assumption of responsibility by Snell & Wilmer to take any action with respect to your legal matters. The purpose of the presentations is to provide seminar attendees general information about recent changes in the law that may impact their business. The presentations should not be considered legal advice or opinion because their individual contents may not apply to the specific facts of a particular case.

Three Year Timeline: Venture Capital Investments in Real Estate Tech



\$12.6B

Global investment
in PropTech, 2017

Cyber Attacks Grow Exponentially

24%

GROWTH IN ATTACK
TRAFFIC AGAINST IOT
DEVICES

204M

GLOBAL RANSOMWARE
ATTACKS IN 2018

\$26.2B

IN BUSINESS EMAIL
COMPROMISE LOSSES
REPORTED 2016-2019

AGENDA

1. How cyber criminals are monetizing attacks against real estate and construction companies
2. The growing vulnerability posed by third parties
3. Reputational and financial risks of inadequate data privacy policies
4. Key steps your organization's legal, compliance, and IT departments should take today



1

Cyber Crime Monetization

Business Email Compromise (BEC)

Indiscriminate attacks, growing sophistication



Executive scammed out of nearly \$1m in the process of buying property in Belize

- The exec had already communicated back and forth twice with the seller's attorney, paying a portion of the \$1,020,000 purchase price as a deposit. When she got a third email from the lawyer with instructions for sending the remaining \$918,000, she wired it to what she thought was a bank account in Belize. In fact, it went to a Citizens Bank in Boston.
- “The lengthy email which S.K. received included lawyerly verbiage that gave it the appearance it was from the attorney in Belize,” [the complaint says](#). “The author included information about Belize-specific regulations on the purchase of property by a foreign company. The email included the standard confidentiality notice and legal disclaimers that are commonly part of emails from attorneys. Lastly, it included a professional signature block with the attorney's name and contact information.”
- <https://qz.com/1752282/how-compromised-emails-enable-cybercrime-and-real-estate-scams/>

Business Email Compromise (BEC)

Indiscriminate attacks, growing sophistication



- The exec **had already communicated back and forth twice with the seller's attorney**, paying a portion of the \$1,020,000 purchase price as a deposit. When she got a third email from the lawyer with instructions for sending the remaining \$918,000, she wired it to what she thought was a bank account in Belize. In fact, it went to a Citizens Bank in Boston.
- “The lengthy email which S.K. received included lawyerly verbiage that gave it the appearance it was from the attorney in Belize,” [the complaint says](#). “The author included information about Belize-specific regulations on the purchase of property by a foreign company. The email included the standard confidentiality notice and legal disclaimers that are commonly part of emails from attorneys. Lastly, it included a professional signature block with the attorney’s name and contact information.”

Business Email Compromise (BEC)

Indiscriminate attacks, growing sophistication



- The exec had already communicated back and forth twice with the seller’s attorney, paying a portion of the \$1,020,000 purchase price as a deposit. **When she got a third email from the lawyer** with instructions for sending the remaining \$918,000, she wired it to what she thought was a bank account in Belize. In fact, it went to a Citizens Bank in Boston.
- “The lengthy email which S.K. received included lawyerly verbiage that gave it the appearance it was from the attorney in Belize,” [the complaint says](#). “The author included information about Belize-specific regulations on the purchase of property by a foreign company. The email included the standard confidentiality notice and legal disclaimers that are commonly part of emails from attorneys. Lastly, it included a professional signature block with the attorney’s name and contact information.”

Business Email Compromise (BEC)

Indiscriminate attacks, growing sophistication



- The exec had already communicated back and forth twice with the seller’s attorney, paying a portion of the \$1,020,000 purchase price as a deposit. When she got a third email from the lawyer with instructions for sending the remaining \$918,000, she wired it to what she thought was a bank account in Belize. In fact, it went to a Citizens Bank in Boston.
- **“The lengthy email which S.K. received included lawyerly verbiage that gave it the appearance it was from the attorney in Belize,”** the complaint says. **“The author included information about Belize-specific regulations on the purchase of property by a foreign company.”** The email included the standard confidentiality notice and legal disclaimers that are commonly part of emails from attorneys. Lastly, it included a professional signature block with the attorney’s name and contact information.”

Ransomware

Evolving attack vector may lead to bigger headaches



*“The ransomware attack on Baltimore city’s government computers has **shut down systems essential for completing home sales**, putting a halt to property deals”*

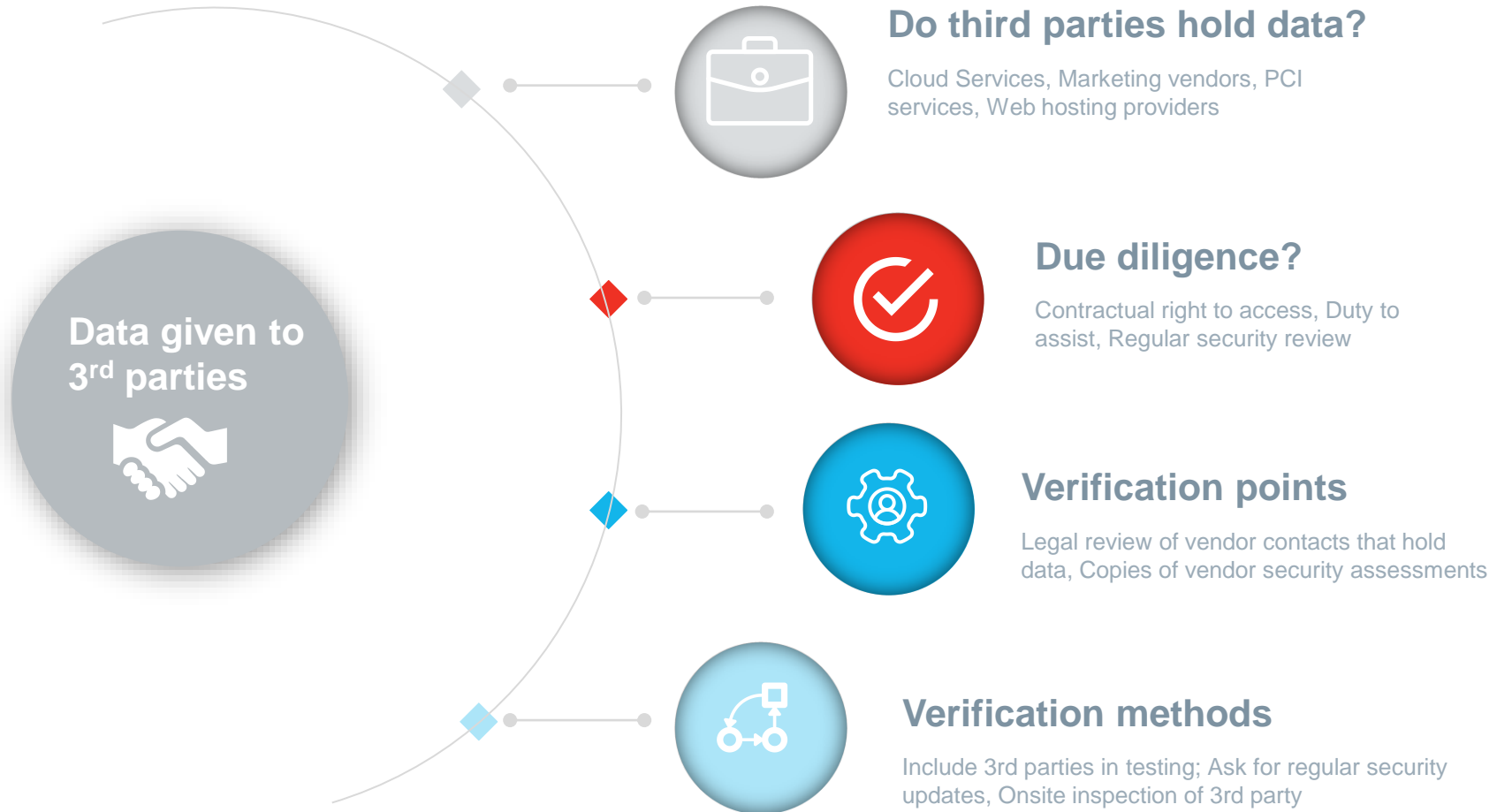
- Attackers now threaten to “dump” data publicly if ransom isn’t paid
- Exfiltration of data could lead to a privacy breach
 - Turn into costly privacy class action suits
 - Demand breach notification requirements
 - Cause press / media impact (reputational risk)



2

Third-party Risk

Preparation: Who Holds Our Data?



BOARD OVERSIGHT: Ensure that third parties meet the same security standards as the company.

Third Party Cyber Risks

Shopping Malls

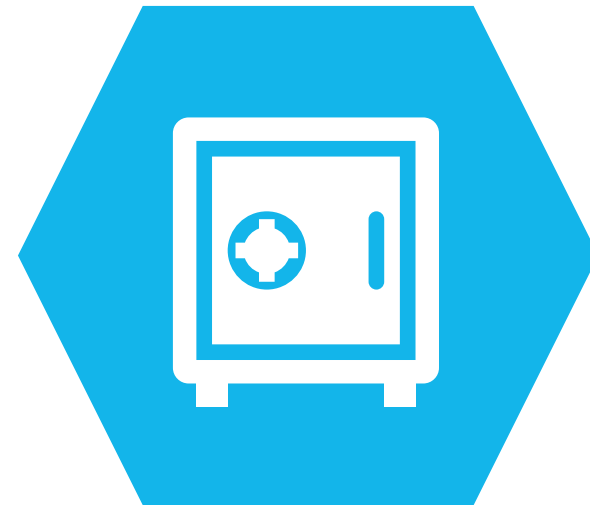


- Most major mall organizations now offer rewards cards.
- These programs, by their nature, collect PII and credit information, typically through third party vendors.
- Should this information be compromised, these companies will have widespread notification requirements.



These organizations must address the following:

- Are appropriate safeguards in place?
- Are these safeguards in place with third party vendor?
- Is there a strategy in place?



Third Party Cyber Risks

The Internet of Things



IoT presents itself throughout physical properties, via:

- Heating/cooling companies (HVAC)
- Elevator and escalator movement systems
- Air temperature monitors
- Security/alarm systems

The third-party tools used to manage these devices may leave themselves open to be accessed remotely.



Third Party Cyber Risks

Target Hack



In 2013, Target was hacked and breached. Hackers stole a reported 40 million credit card numbers.

Target has settled its breach for \$18.5 million and lost \$202 million.

This is one of the biggest data breaches in history.

Target was hacked through their HVAC vendor.



Third Party Cyber Risks

The Internet of Things



When utilizing these devices, address the following:

- Who decides when they are installed?
- Is there a risk assessment prior to installation?
 - Who can access the device?
 - How is it protected against external attack?
 - How are credentials managed- shared by vendor or issued by owner?
- What plans are in place if these devices are compromised and/or ransomed?
- **Are they part of the IT audit and review process?**

Third Party Cyber Risks

Internal Marketing Departments



Most shopping malls are not marketing machines, and often bring in **multi-tenant groups with huge marketing departments.**

These groups are usually made up of younger staff who:

- May not necessarily always communicate the technology they're using.
- Often share critical info on Slack, etc.

These attempts to become more marketing savvy may result in CCPA violations and other privacy issues.

Third Party Cyber Risks

Tracking Internal Documents



From a management perspective, internal documents like **rent and target lists** have independent commercial value, especially in areas of **declining values**, as there is **strong competition for the few commercially viable properties.**

How are these documents being maintained and protected?





3

Legal,
reputational, and
financial risk

Not Just about Data Breach

Liability from Adequate Preparations for Data Breach and Lack of Transparency



1. Personal privacy laws have made cybersecurity standards necessary even short of a cyber incident – more technical and administrative requirements
2. Increasing contractual requirements from business partners
3. Potential unfair competitive advantage – FTC and State Attorneys General
4. More information available online than ever before – and increased transparency requirements make individuals and plaintiff's firms more capable of establishing claims
5. Increased regulator scrutiny into data breaches
6. Increased liability where technical and administrative controls were inadequate

Increasing Data Privacy Regulation of Personal Information



1. European Union's General Data Protection Regulation (GDPR) drove the push to increase regulations around personal information collecting, handling and sharing
2. Far-reaching U.S. state regulations, such as the California Consumer Privacy Act (CCPA) – just went into effect, other states imminent
3. U.S. Federal Agencies trying to maximize their authority to regulate under existing laws – i.e. FTC, SEC
4. Increased State Attorneys General investigation of cyber incidents and data breaches
5. Federal legislation may come sooner than expected

Collaboration Brings Potential Third-Party Liability



1. Increasing real estate, construction management and commercial leasing requires multiple counterparties and contractors
2. Master services agreements frequently have indemnification provisions
3. Data protection agreements are increasingly included and drafted favorably to one party or another
4. Insurance does not always cover despite increasing cyber options

Whistleblower Regimes Increase Incentives



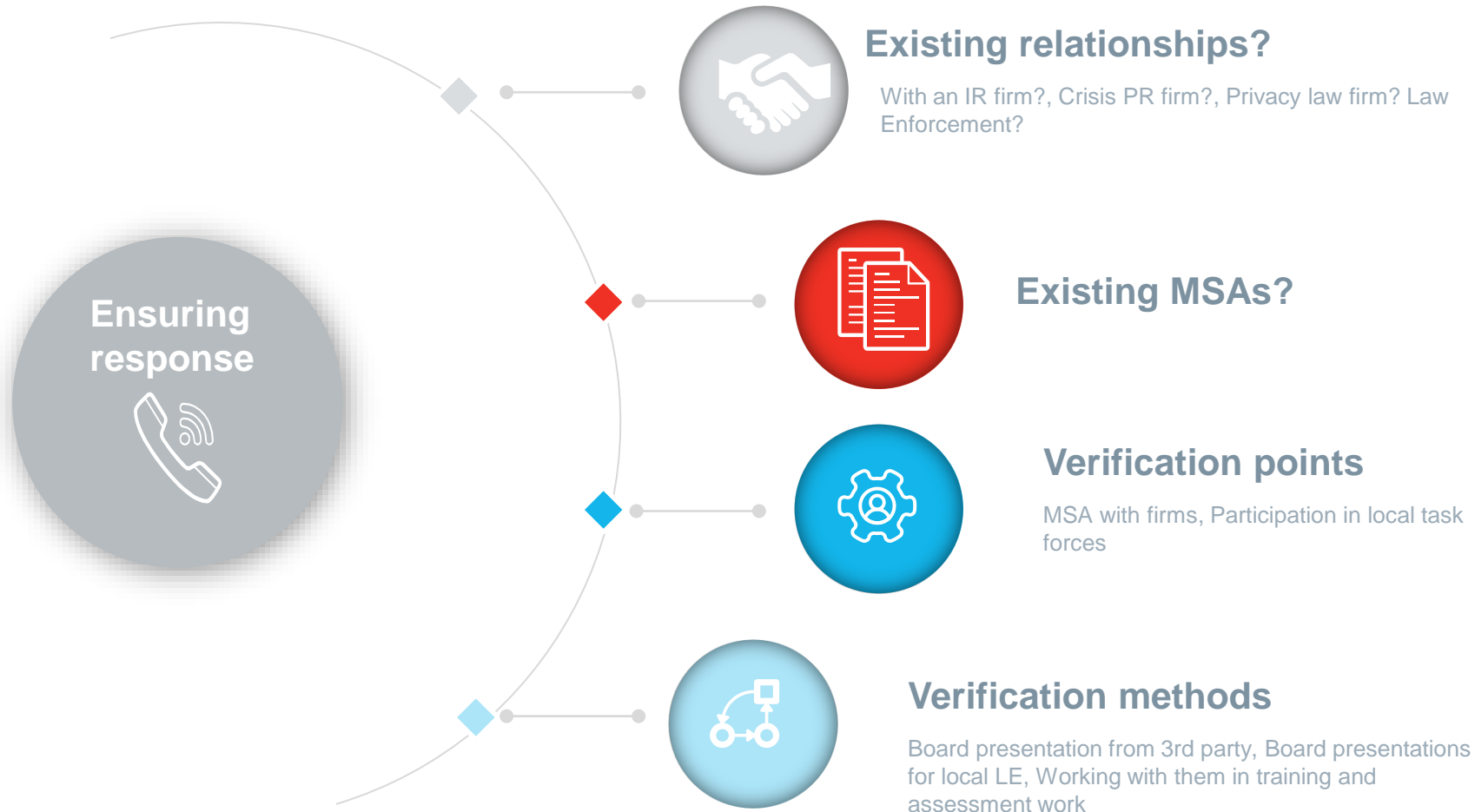
1. Increasing incentives for employee and contractor reporting to regulatory authorities or civil suits
2. Numerous federal and state regulatory schemes including Sarbanes-Oxley, SEC, state labor code, OSHA
3. For government contractors, False Claims Act and Qui Tam actions
4. Potential class action – plaintiff's incentives – reputational and financial risks – i.e. construction defects



4

Action steps

Preparation: Is Help Lined Up?



BOARD OVERSIGHT: Ensure that resources outside the company are available and compatible with the business units in case of need



1. Have an incident response plan in place
2. Ensure legal compliance measures are in place
3. Establish internal controls
4. Audit internally and partners
5. Conduct internal assessments, incident response and investigations under attorney-client privilege



Jonathan Fairtlough
Managing Director, Cyber Risk

jfairtlough@kroll.com



Ross Prindle
Managing Director and Global Head of the
Real Estate Advisory Group

ross.prindle@duffandphelps.com



Alope Chakravarty
Partner, Co-Chair of Investigations,
Government Enforcement and White
Collar Protection practice

achakravarty@swlaw.com

DUFF & PHELPS

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people.

3,500+
TOTAL PROFESSIONALS
GLOBALLY

MORE THAN
15,000
ENGAGEMENTS
PERFORMED IN 2018

7,500
CLIENTS INCLUDING NEARLY
50% OF THE
S&P 500

THE
AMERICAS

2,000+
PROFESSIONALS

EUROPE AND
MIDDLE EAST

1000+
PROFESSIONALS

ASIA
PACIFIC

500+
PROFESSIONALS

One Company

Duff & Phelps has offices in **28 COUNTRIES** worldwide with Real Estate Advisory professionals in **11** of them



THE AMERICAS

- | | | |
|----------------|---------------------|----------------------|
| Addison | Houston | Pittsburgh |
| Atlanta | Libertyville | Reston |
| Austin | Lisle | St. Louis |
| Bogota | Los Angeles | San Francisco |
| Boston | Mexico City | São Paulo |
| Buenos Aires | Miami | Seattle |
| Cayman Islands | Milwaukee | Secaucus |
| Chicago | Minneapolis | Silicon Valley |
| Dallas | Morristown | Stamford |
| Denver | Nashville | Toronto |
| Detroit | New York | Washington, DC |
| Grenada | Philadelphia | |

EUROPE AND MIDDLE EAST

- | | | |
|-----------------|-------------------|---------------|
| Abu Dhabi | Dublin | Munich |
| Agrate Brianza | Frankfurt | Padua |
| Amsterdam | Lisbon | Paris |
| Athens | London | Pesaro |
| Barcelona | Longford | Porto |
| Berlin | Luxembourg | Rome |
| Bilbao | Madrid | Turin |
| Birmingham | Manchester | Warsaw |
| Channel Islands | Milan | |
| Dubai | Moscow | |

ASIA PACIFIC

- | | |
|------------------|-----------------|
| Bangalore | Shanghai |
| Beijing | Shenzhen |
| Guangzhou | Singapore |
| Hanoi | Sydney |
| Ho Chi Minh City | Taipei |
| Hong Kong | Tokyo |
| Hyderabad | |
| Mumbai | |
| New Delhi | |

Note: Cities in red include Real Estate Advisory professionals.

DUFF & PHELPS BUSINESS UNITS

VALUATION ADVISORY

Valuation and consulting for financial reporting, tax, investment and risk management purposes

DUFF & PHELPS
Real Estate Advisory Group



CORPORATE FINANCE

Objective guidance to management teams and stakeholders throughout restructuring, financing and M&A transactions, including independent transaction opinions



GOVERNANCE, RISK, INVESTIGATIONS AND DISPUTES

Combined Duff & Phelps and Kroll disputes, investigations, cyber business intelligence, cross - border restructuring and other advisory

Kroll | A Division of
DUFF & PHELPS

Cyber Risk



PRIME CLERK

Global leader in complex business services and claims administration in the context of restructuring, business services, global corporate actions, notice media solutions and settlement administration



For more information about our global locations and services, please visit:

www.kroll.com

www.swlaw.com

www.duffandphelps.com

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com.