GIBSON DUNN

IPO and Public Company Readiness: Cybersecurity

Presented by:

Andrew Fabens, Stewart McDowell, Alexander Southwell, Peter Wardle

February 28, 2017

Cybersecurity Dominated Recent Headlines

- Numerous significant data breaches at major retailers

- Cyberattacks increasingly sophisticated and beyond retail

JPMorgan Chase Hacking Affects 76 Million Households
- *New York Times*, 10/2/2014

Sony to Lose $200 Million Following Cyber Attack
- *Business Standard*, 12/23/2014

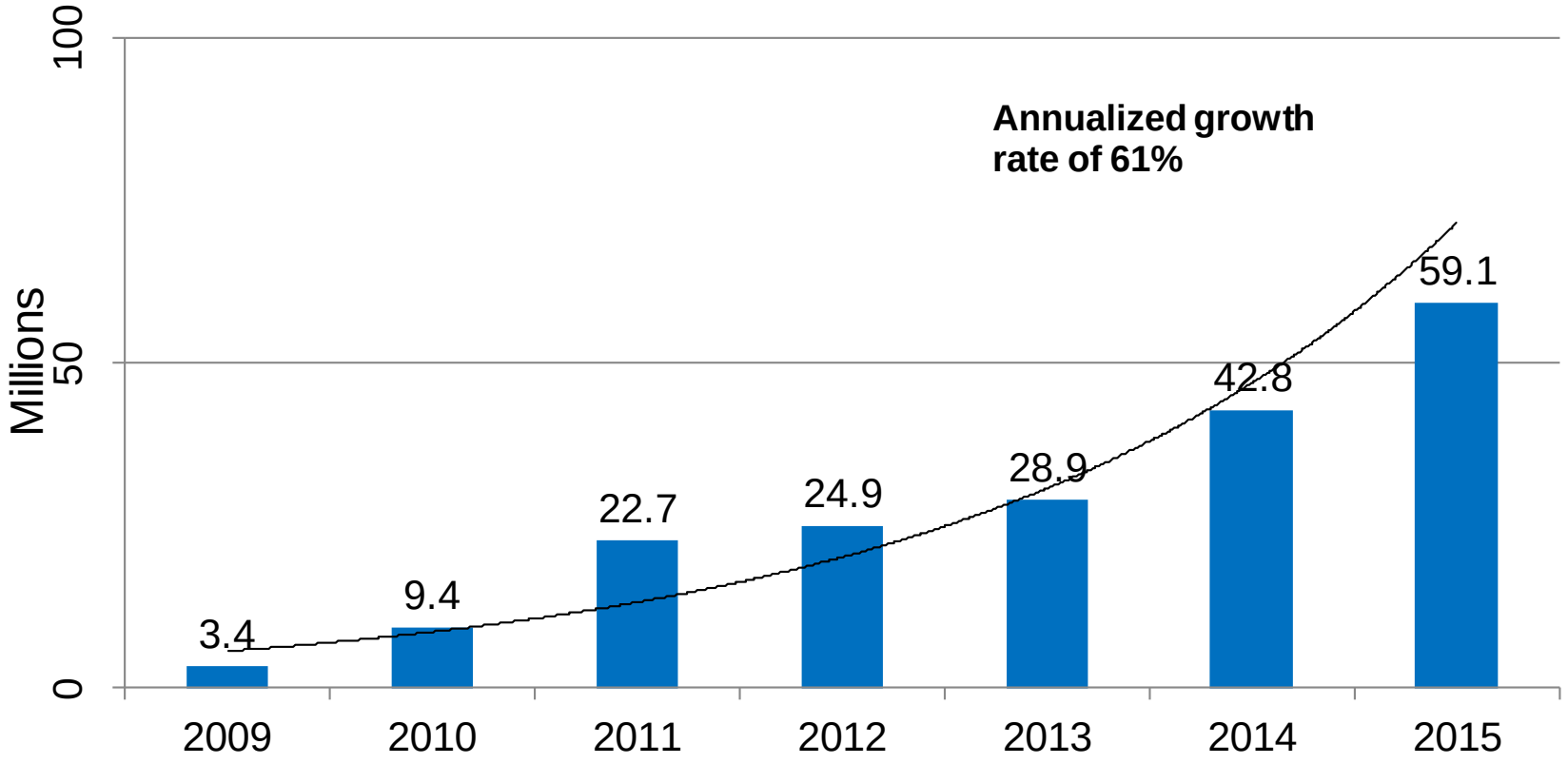
Starwood Hotels and Resorts warns of breach at 54 of its hotels
- *New York Times*, 11/20/2015

Office of Personnel Management hack compromised 22.1 million people
- *Washington Post*, 7/9/2015

Anthem warns customers regarding its huge data breach
- *Los Angeles Times*, 3/6/2015

Experian breach hit 15 million T-Mobile customers
- *Reuters*, 10/1/2015

Cybersecurity Incidents Worldwide



Source: PWC Global State of Information Security Survey 2015, Figure 2 & PWC Global State of Information Security Survey 2016, Appendix A

Categories of Cybersecurity Incidents and Sources of Risks

Incident by Attack Type Over Time

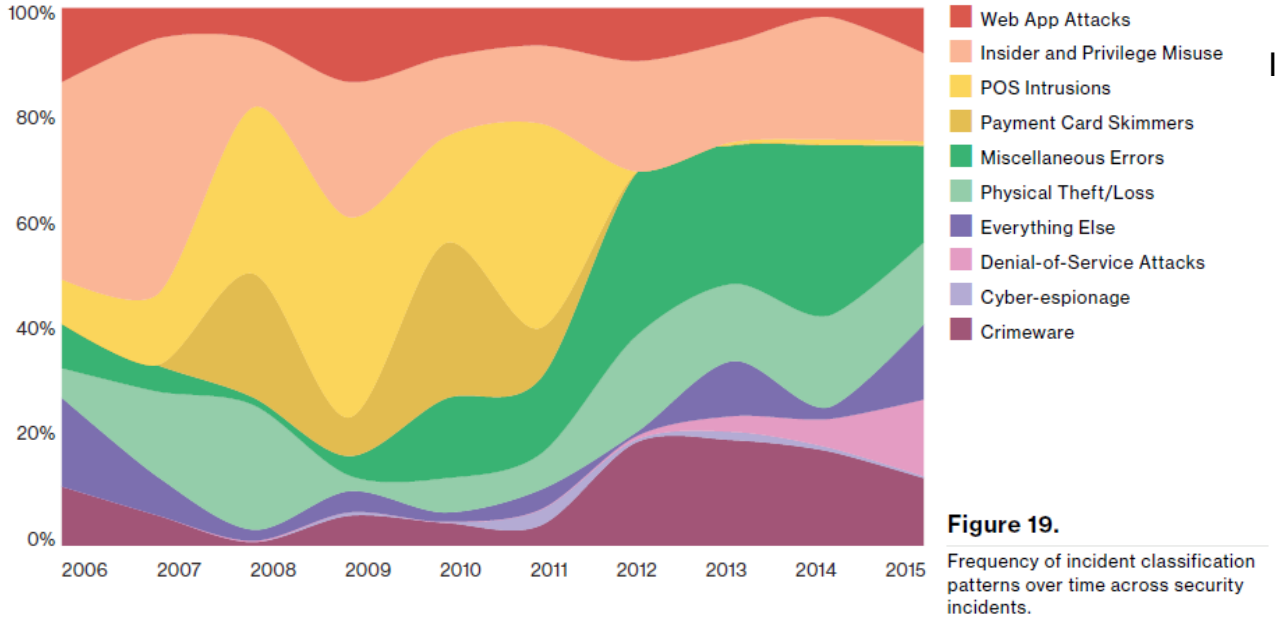
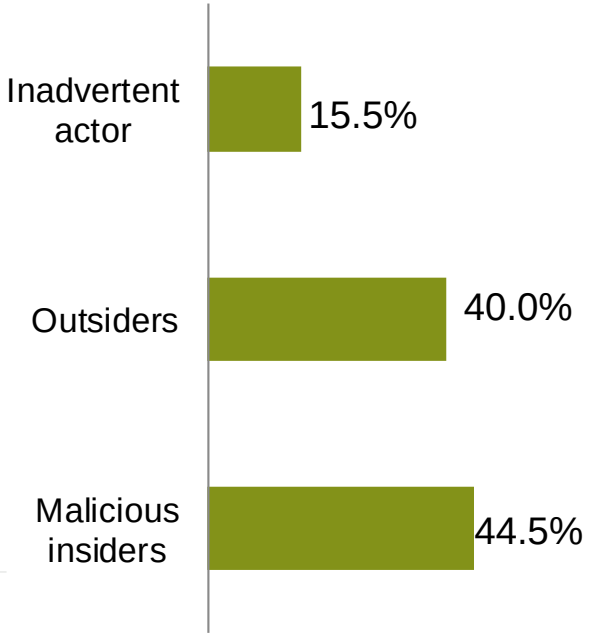


Figure 19.

Frequency of incident classification patterns over time across security incidents.

Source: Verizon 2016 Data Breach Investigations Report, Figure 19

Incidents by Attacker Type

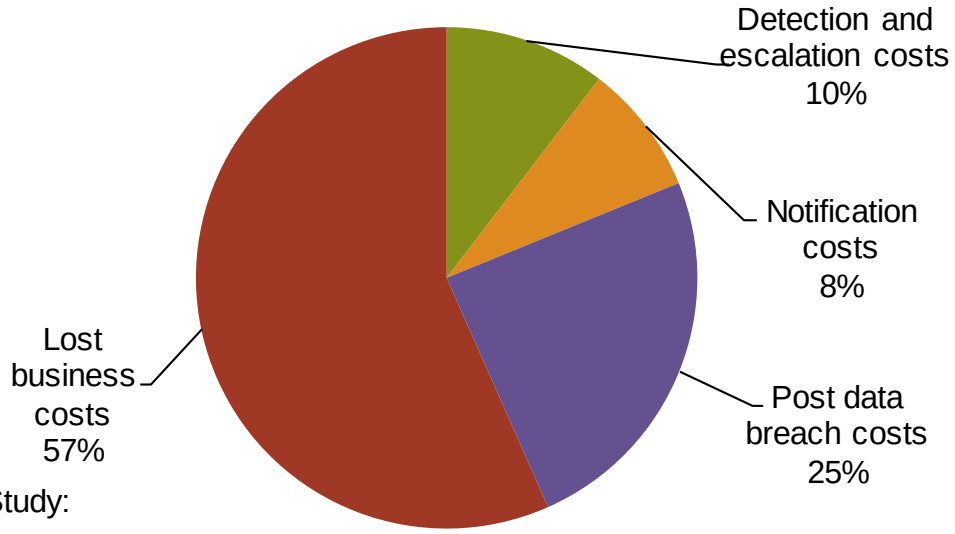


Source: IBM Cyber Security Intelligence Index 2016, Figure 4

Data Breach Costs Continue to Increase

- Average number of records breached per breach in the United States in 2016: 29,611.
- Average per capita cost of a data breach in the United States in FY 2016: $221, compared to $217 in FY 2015 and $201 in FY 2014.
- Average total organizational cost of data breach in the United States in 2016: $7.01M compared to $6.53M in 2015 and $5.85M in 2014.

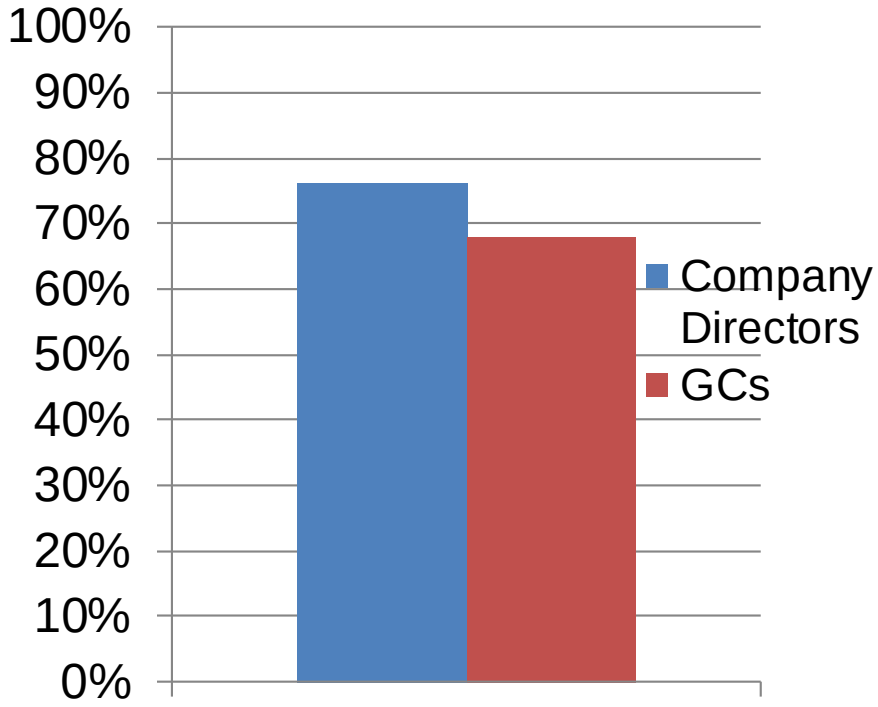
Average costs of data breaches by category



Source: Ponemon Institute - 2016 Cost of Data Breach Study: Global Analysis, Figures 1-3, 13-16

Major Concerns of GCs and Boards

GCs and directors reporting a need for better information and processes regarding IT strategy and risk



Source: Corporate Board Member – Law in the Boardroom Study (2015), Figure 3

Source: Corporate Board Member – Law in the Boardroom Study (2015), Figure 1

Risks From a Cyberattack

- Damage to Business
  - Lost Customers/Revenue
  - Damage to Reputation/Brand
  - Diverted Management and Board Focus
  - Direct Response Costs
- Litigation/Regulatory Risks
  - Law Enforcement Investigations (e.g., FBI, Secret Service)
  - Regulatory investigations (e.g., FTC, state AGs, FCC, SEC)
  - Consumer Class Actions
  - Derivative Actions
  - Shareholder Actions
- Impact to Public Company/Stock Price
  - Loss of Investor Confidence
  - Negative Financial Impact
  - Failure to Meet Guidance

Key IPO Considerations

- Disclosure
  - Registration statement/prospectus must appropriately disclose material risks of cybersecurity
- Underwriters due diligence
  - Underwriters seeking to establish due diligence defense by conducting reasonable diligence
- Public attention
  - Publicity around IPO/being a public company may attract higher level of attack/scrutiny

Scrutiny Turns Internal

While law enforcement focuses on prosecution of hackers, regulators, investors and plaintiffs analyze behavior of victim companies.

- Scrutiny on:
  - Did company adequately plan/prepare for possible breach?
  - How quickly and efficiently did company discover the intrusion?
  - How did company respond, including securing the breach, remediation efforts, notice to consumers, etc.?
  - Were the company's disclosures adequate?
- Standards for what is deemed "reasonable" in the cybersecurity arena continue to evolve

Securities Fraud and Derivative Litigation: New Areas of Potential Exposure

- New area of focus for plaintiffs' attorneys
- Possibility of Section 11, Section 12 and Rule 10b-5 lawsuits if significant stock drop
  - Focus on misrepresentations or omissions concerning safeguards, disclosures of breaches, response to cyberattacks
- Derivative lawsuits against Directors and Officers
  - Alleging breaches of fiduciary duties, mismanagement, abuse of control, and corporate waste relating to oversight of Company's policies and procedures concerning cybersecurity, disclosures, and response to cyberattacks
  - At least 6 lawsuits filed since 2009, with two lawsuits filed in 2014 and one each in 2015, 2016, and 2017

Assessing Exposure

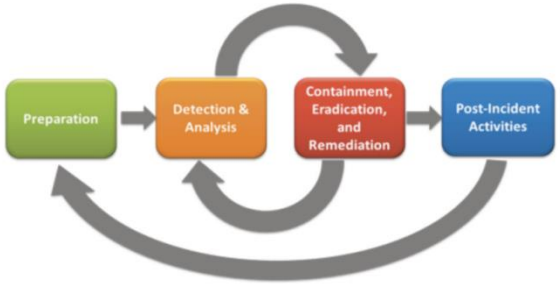
- Data identification and prioritization
  - What types of data do we store? Where? What is most sensitive?
- Enterprise Risk Management (ERM)
  - Does an ERM framework exist? Does it cover data security? Business continuity? Disaster recovery?
  - Formal cybersecurity Incident Response Plan (IRP)?
- Corporate governance issues
  - C-suite level executive responsible for cybersecurity
  - Board committee focused on cybersecurity

Assessing Exposure

- Consider the sector
  - Is the company's market attractive to hackers?
  - Are there regulatory rules or guidance from self-regulatory bodies regarding cybersecurity?
- Consider prior data security incidents
  - Has the company been breached before? If so, how did the company respond?
- Review the company's IT infrastructure and vendors
  - What functions does the target outsource?
  - Do vendors have adequate security protocols?
- Review the company's policies, procedures, and corporate governance
  - Do they demonstrate that the company takes cybersecurity seriously?
  - Are they commensurate with the risk?

Responding to the Risks: Preparedness

- Incident Response Plan (IRP)
  - Critical elements
    - Pre-selected, multidisciplinary Incident Response Team (IRT)
    - Clear delegation of authority
    - Clear escalation procedures
    - Incident severity classification system
    - Key outside contacts identified – computer security, forensics, outside counsel, public/media relations, law enforcement
    - Post-incident feedback loop to improve response capabilities



Responding to the Risks: Preparedness

- Regular employee training
- Formal policies
- Asset management
- Technical best practices
  - Encryption
  - Access control / ID management
  - Secure destruction
  - Intrusion detection systems
  - Data loss prevention software

Responding to the Risks: Testing Preparedness

- Penetration testing
  - Hire “white hat” hackers to find vulnerabilities
- Stress testing
  - Learn your IT system’s breaking points
  - Understand vulnerabilities to denial-of-service attacks
- Social engineering assessments
  - E.g., Internal phishing campaigns
- “Tabletop” exercises
  - Simulated cybersecurity emergency
  - Test/improve response processes

Responding to the Risks: Board Oversight

- What should Directors be asking?
  - What are our data "crown jewels"? Encrypted? What would happen if hackers got to them?
  - Who are our likely adversaries?
  - What are the most likely attack vectors?
  - Are our own Board communications secure?
  - Have we been breached before? How many times? What happened? What did we learn? How have we improved?
  - Do we conduct external security audits? What have they shown?
  - Is oversight structured in compliance with applicable regulation and guidance?

Responding to the Risks: Board Oversight

- What should Directors be asking?
  - Do we have an IRP? Do we follow it? Test it?
  - Does our IRP take into account the NIST Cybersecurity Framework?
  - Should we seek any certifications (e.g., ISO 27001)?
  - Who's on our IRT? Are they qualified?
  - How else are we protecting ourselves?
  - What else can we do that we are not doing? What are the costs/benefits?
- How should oversight be structured?

Responding to the Risks: Communicating About Preparedness

- For employees
  - Communicating about cybersecurity, computer use, social media policies
- For the Board
  - Regular meetings with committee focused on cybersecurity
  - Regular agenda items and presentations regarding cybersecurity for full Board
- For the public/investors
  - Privacy policies
  - Disclosures to the SEC, other regulators, and investors
  - Representations in advertising and marketing materials

Responding to the Risks: Evaluating Cyber Insurance

- Market expanding
  - General liability and D&O policies usually not adequate
  - Significant variations in terms and coverage
  - May mitigate disclosure obligations by reducing financial risk of cyber incident
- Common types of coverage
  - Crisis management expenses
  - Notification costs
  - Credit monitoring costs
  - Business interruption
  - Litigation / regulatory response costs
  - Network security
  - Privacy liability

Next Steps – Analysis of Cybersecurity and Data Privacy for Pre-IPO Client

- As part of the IPO preparation, Gibson Dunn analyzes client's policies, procedures and practices
- Scope of review includes
  - Review of relevant policies
  - Calls with and questions posed to client personnel
- Provides client with analysis and recommendations that can include, e.g.
  - Recommendations to build out business continuity plan by considering responses to specific types of threats, clarifying roles and responsibilities and clarifying customer notification procedures
  - Recommendations to augment data security policy with more detail regarding access controls, authentication and authorization
  - Recommendations to augment "Bring your Own Device," email and password policies for employees
  - Recommendations to augment board oversight of cybersecurity matters

GIBSON DUNN

Professional Profiles

Andrew L. Fabens

200 Park Avenue, New York, NY 10166-0193
Tel: +1 212.351.4034
AFabens@gibsondunn.com

Andrew L. Fabens is a partner in the New York office of Gibson, Dunn & Crutcher. Mr. Fabens is Co-Chair of Gibson Dunn's Capital Markets Practice Group and is a member of Gibson Dunn's Securities Regulation and Corporate Governance Practice Group.

Mr. Fabens advises companies on long-term and strategic capital planning, disclosure and reporting obligations under U.S. federal securities laws, corporate governance issues and stock exchange listing obligations. He represents issuers and underwriters in public and private corporate finance transactions, both in the United States and internationally. His experience encompasses initial public offerings, follow-on equity offerings, investment grade, high-yield and convertible debt offerings and offerings of preferred, hybrid and derivative securities. In addition, he regularly advises companies and investment banks on corporate and securities law issues, including M&A financing, spinoff transactions and liability management programs.

Mr. Fabens is ranked as a leading Capital Markets lawyer by *Chambers USA: America's Leading Lawyers for Business*, *The Legal 500 US* and *Chambers Global: The World's Leading Lawyers for Business*. He is noted as being able to "readily adapt to his client's style, understand what they need and deliver it," that he is "so amazingly even-keeled that nothing throws him," and is a "strong and knowledgeable lawyer" who is very "practical in terms of assessing risk and moving forward."

Mr. Fabens earned his Juris Doctor from Columbia Law School in 2000. He earned a Bachelor of Arts *cum laude* from the University of Michigan in 1989.

Stewart L. McDowell

555 Mission Street, San Francisco, CA 94105-0921
Tel: +1 415.393.8200
SMcDowell@gibsondunn.com

Stewart L. McDowell is a partner in the San Francisco office of Gibson, Dunn & Crutcher. She is Co-Chair of the firm's Capital Markets Practice.

Ms. McDowell's practice involves the representation of business organizations as to capital markets transactions, mergers and acquisitions, SEC reporting, corporate governance and general corporate matters. She has significant experience representing both underwriters and issuers in a broad range of both debt and equity securities offerings. She also represents both buyers and sellers in connection with U.S. and cross-border mergers, acquisitions and strategic investments.

Ms. McDowell received her law degree from the University of Virginia School of Law in 1995 and her Bachelor of Arts degree from Princeton University in 1991.

Ms. McDowell is a member of the California State Bar and the New York Bar Association.

Alexander H. Southwell

200 Park Avenue, New York, NY 10166-0193
Tel: +1 212.351.3981
ASouthwell@gibsondunn.com

Alexander H. Southwell is a partner in Gibson, Dunn & Crutcher's New York office and is Chair of Gibson Dunn's Privacy, Cybersecurity, and Consumer Protection Practice Group. His practice focuses on counseling a variety of clients on privacy, information technology, data breach, theft of trade secrets and intellectual property, computer fraud, national security, and network and data security issues, including handling investigations, enforcement defense, and litigation. In particular, Mr. Southwell regularly advises companies victimized by cyber-crimes and counsels on issues under the Computer Fraud and Abuse Act, the Economic Espionage Act, the Electronic Communications Privacy Act, and related federal and state statutes. Mr. Southwell additionally handles a range of white-collar criminal and regulatory enforcement defense, internal investigation, compliance, and complex civil litigation matters. An experienced trial and appellate attorney, prior to joining Gibson Dunn, Mr. Southwell served as an Assistant United States Attorney in the United States Attorney's Office for the Southern District of New York.

Mr. Southwell is also an Adjunct Professor of Law at Fordham University School of Law where he teaches a seminar on cyber-crimes, covering computer misuse crimes, intellectual property offenses, the Fourth Amendment in cyber-space, computer evidence at trial, data breach and privacy issues, and information security, among other areas.

Mr. Southwell earned his undergraduate degree, *magna cum laude*, from Princeton University and his Juris Doctor, *magna cum laude*, from New York University School of Law. Following law school, Mr. Southwell was a Law Clerk for the Honorable Naomi Reice Buchwald of the United States District Court for the Southern District of New York.

Mr. Southwell was named a *Law360* "MVP" in Privacy in both 2015 and 2016 – one of five "elite attorneys" who have "distinguished themselves from their peers by securing hard-earned successes in high-stakes litigation, complex global matters and record-breaking deals," and is ranked as an up and comer in White Collar Litigation in the most recent *Chambers USA: America's Leading Lawyers for Business*. *Chambers* noted Mr. Southwell has "impeccable judgment, is very detail-oriented and is someone you can really trust with your most important matters." Mr. Southwell was selected as a Cybersecurity and Data Privacy Trailblazer in 2015 by *The National Law Journal.* Mr. Southwell is also honored in *Benchmark Litigation* as a future star and by *The Best Lawyers in America*© as a leading lawyer in the area of Criminal Defense: White-Collar.

Peter W. Wardle

333 South Grand Avenue, Los Angeles, CA 90071-3197
Tel: +1 213.229.7242
PWardle@gibsondunn.com

Peter W. Wardle is a partner in the Los Angeles office of Gibson, Dunn & Crutcher. He is Co-Chair of its Capital Markets Practice Group.

Mr. Wardle's practice includes representation of issuers and underwriters in equity and debt offerings, including IPOs and secondary public offerings, and representation of both public and private companies in mergers and acquisitions, including private equity, cross border, leveraged buy-out, distressed and going private transactions. He also advises clients on a wide variety of general corporate and securities law matters, including corporate governance issues.

Mr. Wardle earned his J.D. in 1997 from the University of California, Los Angeles, School of Law, where he was elected to the Order of the Coif and served as Business Manager of the *UCLA Law Review* and Articles Editor of the *UCLA Entertainment Law Review*. He received an A.B. degree *cum laude* in 1992 from Harvard University. Mr. Wardle is a member of the Board of Directors and Co-Chair of the Governance Committee for The Colburn School. He is a member of the firm's Compensation Committee, National Pro Bono Committee and chair of the Community Affairs Committee, and serves as one of the Pro Bono Partners for the Los Angeles area offices.

Our Offices

Beijing
Unit 1301, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025, P.R.C.
+86 10 6502 8500

Brussels
Avenue Louise 480
1050 Brussels
Belgium
+32 2 554 70 00

Century City
2029 Century Park East
Los Angeles, CA 90067-3026
+1 310.552.8500

Dallas
2100 McKinney Avenue
Suite 1100
Dallas, TX 75201-6912
+1 214.698.3100

Denver
1801 California Street
Suite 4200
Denver, CO 80202-2642
+1 303.298.5700

Dubai
Building 5, Level 4
Dubai International Financial Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 318 4600

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt
Germany
+49 69 247 411 500

Hong Kong
32/F Gloucester Tower, The Landmark
15 Queen's Road Central
Hong Kong
+852 2214 3700

Houston
1221 McKinney Street
Houston, TX 77010

London
Telephone House
2-4 Temple Avenue
London EC4Y 0HB
England
+44 (0) 20 7071 4000

Los Angeles
333 South Grand Avenue
Los Angeles, CA 90071-3197
+1 213.229.7000

Munich
Hofgarten Palais
Marstallstrasse 11
80539 Munich
Germany
+49 89 189 33-0

New York
200 Park Avenue
New York, NY 10166-0193
+1 212.351.4000

Orange County
3161 Michelson Drive
Irvine, CA 92612-4412
+1 949.451.3800

Palo Alto
1881 Page Mill Road
Palo Alto, CA 94304-1125
+1 650.849.5300

Paris
166, rue du faubourg Saint Honoré
75008 Paris
France
+33 (0) 1 56 43 13 00

San Francisco
555 Mission Street
San Francisco, CA 94105-0921
+1 415.393.8200

São Paulo
Rua Funchal, 418, 35°andar
São Paulo 04551-060
Brazil
+55 (11) 3521.7160

Singapore
One Raffles Quay
Level #37-01, North Tower
Singapore 048583
+65.6507.3600

Washington, D.C.
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306
+1 202.955.8500