DORSEY
DORSEY & WHITNEY LLP

MSBA Minnesota State Bar Association

Advising the Board of Directors on Privacy and Data Security

Melissa Krasnow,
Dorsey & Whitney LLP
Certified Information Privacy Professional/US
krasnow.melissa@dorsey.com

This presentation was created by Dorsey & Whitney LLP, 50 South Sixth Street, Suite 1500, Minneapolis, MN 55402. This presentation is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances. An attorney-client relationship is not created or continued by sending and/or receiving this presentation. Members of Dorsey & Whitney will be pleased to provide further information regarding the matters discussed in this presentation.

LESSONS LEARNED FROM DIRECTORS AND OFFICERS LITIGATION INVOLVING BREACHES

- **Wyndham**

  Caremark requires that a corporation's "directors utterly failed to implement any reporting or information system ... [or] consciously failed to monitor or oversee its operations thus disabling themselves from being informed." Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006). Yet Plaintiff concedes that security measures existed when the first breach occurred, and admits the Board addressed such concerns numerous times. (Compl. ¶¶ 46, 62, 63). The Board was free to consider such potential weaknesses when assessing the lawsuit. Palkon v. Holmes, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014)

- **Target and Home Depot directors and officers litigation**
- **Director cybersecurity expertise or experience**

EXAMPLES OF DIRECTOR QUESTIONS ABOUT PRIVACY AND DATA SECURITY

- **National Association of Corporate Directors (NACD), Cyber-Risk Oversight Handbook (June 10, 2014) https://www.nacdonline.org**
- **Information Systems Audit and Control Association (ISACA), The Cyberresilient Enterprise: What the Board of Directors Needs to Ask (August 20, 2015) http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/the-cyberresilient-enterprise-what-the-board-of-directors-needs-to-ask.aspx**

PRIVACY AND DATA SECURITY AND CORPORATE GOVERNANCE RESOURCES

- **International Association of Privacy Professionals https://iapp.org**
- **Bloomberg BNA Privacy & Data Security Law Resource Center http://www.bna.com**
- **National Association of Corporate Directors https://www.nacdonline.org**
- **Harvard Law School Forum on Corporate Governance and Financial Regulation http://corpgov.law.harvard.edu/**

INCIDENT RESPONSE

- **Does the organization have an incident response plan and / or business continuity / disaster recovery plan?**
- **When was the last time each was tested or updated?**
- **How frequently is each tested or updated?**
- **What was the situation that was the subject of the testing?**
- **What are the results of and insights from testing or updating?**
- **Who are the members of the incident response team?**
- **Who are external team members, including service providers?**
- **What are incident response team member responsibilities?**

INCIDENT RESPONSE (con't)

- **Is there contact information for incident response team members?**
- **What are the lines of communication?**
- **What communications/disclosures/notifications are anticipated (e.g., internal and external)?**
- **Is the organization prepared to work with law enforcement, regulators, industry contacts and business partners?**
- **Is any cybersecurity or related training or awareness provided for employees, etc.?**

INCIDENT RESPONSE RESOURCES

- **Guidance for Incident Response Plans**
  http://www.irmi.com/articles/expert-commentary/guidance-for-incident-response-plans
- **Cybersecurity incident response: Planning is just the beginning**
  http://www.grantthornton.com/issues/library/whitepapers/advisory/2015/cybersecurity-incident-response-report.aspx#sthash.ehQeDARn.dpuf
- **Best Practices for Victim Response and Reporting of Cyber Incidents**
  http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf