EFiled: Jun 15 2015 03:09PM EDT
Transaction ID 57405408
Case No. 11122-VCP

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

CORA FROHMAN, Plaintiff, v. THE HOME DEPOT, INC., Defendant.	C.A. No. 11122-VCP PBLIC VERSION FILED: June 15, 2015

VERIFIED COMPLAINT PURSUANT TO 8 DEL. C. § 220 TO COMPEL INSPECTION OF BOOKS AND RECORDS

Plaintiff Cora Frohman ("Plaintiff"), by her undersigned attorneys, on behalf of herself and all others similarly situated, alleges upon information and belief, including the investigation of counsel, and a review of publicly-available information, except for her own acts, which are alleged on personal knowledge as follows:

NATURE OF THE ACTION

1. In this action, Plaintiff seeks to enforce her right to inspect certain book and records of defendant The Home Depot, Inc. ("Home Depot" or the "Company"), a Delaware corporation, pursuant to 8 Del C. § 220 ("Section 220"). Plaintiff seeks to inspect these documents to (a)

investigate potential wrongdoing, mismanagement, and breaches of fiduciary duties by the members of the Company's management and certain directors of the Board or others in connection with the events, circumstances, and transactions described herein; (b) assess the ability of the Board to impartially consider a demand for action (including a request for permission to file a derivative lawsuit on the Company's behalf) related to the items described in this demand including the scope of such demand; (c) determine whether the current directors are fit to continue serving on the board of directors; and (d) take appropriate action in the event the members of the Company's management and certain directors did not properly discharge their fiduciary duties, including the preparation and filing of a stockholder derivative lawsuit, if warranted.

2. As explained below, sensitive financial data including customers' names, credit and debit cards numbers, card expiration dates and card verification values of 56 million Home Depot customers were compromised as a result of Home Depot's failure to adequately secure payment information on its data systems. It is believed to be the largest data security breach in U.S. history, yet Home Depot's security was so deficient that the breach continued for more than four months without Home Depot

even detecting it. According to Home Depot's latest Form 10-Q filed with the Securities and Exchange Commission ("SEC"), the Company faces at least 57 civil actions that have been filed in courts in the U.S. and Canada. Furthermore, several state and federal agencies, including State Attorneys General, are investigating events related to the data beach, including how it occurred, its consequences and the Company's responses. It has been estimated that the total cost of the breach may exceed $10 billion.[1]

3. The Home Depot breach involved substantially the same techniques as those used in other significant data breaches which have occurred over the last few years. Despite knowledge that such breaches were occurring throughout the retail industry, Home Depot failed to properly protect the sensitive card information from what is now a widely known preventable method of cyber-attack. There is a credible basis to believe that officers and directors of Home Depot were aware of the risks that the Company faced from a cyber-attack but in breach of their fiduciary duties

[1] *See* Trefis Team, Home Depot: Will The Impact Of The Data Breach Be Significant? http://www.forbes.com/sites/greatspeculations/2015/03/30/home-depot-will-the-impact-of-the-data-breach-be-significant/ (last visited June 3, 2015).

the Board has failed in its responsibilities to implement systems and internal controls to properly protect the Company from this threat.

4. On November 17, 2014, Home Depot began its production on a rolling basis and completed its production on May 8, 2015 (the "Document Production"), approximately six months after receiving Plaintiff's September 30, 2014 demand for books and records pursuant to Section 220 (the "Demand"). The entire production encompassed 510 pages, is incomplete, inconsistent, duplicative and inappropriately redacts information necessary and essential to Plaintiff's stated purpose, in large part, on the basis of security concerns, despite the fact the Plaintiff signed a Confidentiality and Non-Disclosure Agreement Governing the Inspection of Books and Records ("NDA") and Plaintiff's counsel agreed to be jointly and severely liable for any damages suffered as a result of unauthorized dissemination of the Document Production.[2]

[2] The NDA provides in pertinent part that "Frohman and each Advisor must hold all Inspection Information in confidence, and may not disclose, publish, disseminate, or communicate the Inspection Information (or the content thereof) to anyone, either directly or indirectly, except as provided in this Agreement. Frohman's counsel agrees that it will be jointly and severally responsible and liable to The Home Depot for any breach by any Advisor of this Agreement or of any Advisor Undertaking in the form attached hereto as

5. Plaintiff respectfully requests that her Section 220 Demand be deemed proper and enforceable and that Home Depot be directed to produce unredacted copies of all books and records sought by Plaintiff in her Section 220 Demand immediately.

PARTIES

6. Plaintiff is a stockholder of defendant Home Depot and has been a stockholder of the Company since at least June 2005.

7. Defendant Home Depot is a Delaware corporation with its principal executive offices located at 2455 Paces Ferry Road N.W., Atlanta, Georgia 30339. Home Depot is the world's largest home improvement retailer based on Net Sales for the fiscal year ended February 1, 2015. The Home Depot stores sell a wide assortment of building materials, home improvement products and lawn and garden products and provide a number of services.

FACTUAL BACKGROUND

8. On September 2, 2014, Brian Krebs originally reported a potential breach of Home Depot's payment data systems on his blog "Krebs

---

Exhibit B executed by such Advisor."

on Security".[3] On September 8, 2014, Home Depot publicly confirmed the breach and stated that it had begun an investigation on September 2 into a possible data breach into its payment systems after receiving reports from its banking partners and law enforcement. Home Depot believes that the malware used in the breach was present between April and September 2014. The breach affected Home Depot's stores in the U.S. and Canada. On September 18, 2014, Home Depot announced that it estimated that the breach put approximately 56 million unique payment cards at risk. The attack is being reported as the largest known breach of a retail company's computer network.

9. According to the Company's Form 8-K filed with the SEC on September 18, 2014, as a result of the data breach Home Depot decided to "provide credit monitoring services to its customers, increase call center staffing, and pay legal and professional services, all of which are expensed

[3] Brian Krebs is a former reporter for the Washington Post whose reporting on cyber security is widely considered to be among the best on the topic. http://www.nytimes.com/2014/02/17/technology/reporting-from-the-webs-underbelly.html; http://www.bloomberg.com/bw/articles/2014-01-16/brian-krebs-the-cybersecurity-blogger-hackers-love-to-hate

as incurred in a gross amount of approximately $62 million, partially offset by a $27 million receivable for costs the Company believes are reimbursable and probable of recovery under its insurance coverage." In addition, the Company claims that it has closed off the hackers' method of entry and eliminated the malware from the Company's systems.

10. The Company also introduced a new payment security protection system, which was completed in all U.S. stores on September 13, 2014 but was not completed in Canadian stores until early 2015. The new system "locks down payment data through enhanced encryption, which takes raw payment card information and scrambles it to make it unreadable and virtually useless to hackers." The new encryption technology was provided by Voltage Security, Inc. and the encryption project was launched in January 2014.

11. According to news sources, there were smaller breaches of Home Depot's systems in 2013. On July 25, 2013, a data stealing virus was found to have spread to eight registers in a Home Depot in Denton, Texas, and the Infostealer virus, which is known for stealing credit card data, was found in December 2013 at a Columbia, Maryland Home Depot store.

12. Following news of the breach, several news outlets interviewed

former Home Depot information security staff. The former staff members reported that managers did not take employees' concerns about the security of Home Depots' systems seriously. They also recalled that Home Depot relied on outdated antivirus software and failed to conduct full vulnerability scans every quarter, despite Payment Card Industry Data Security Standards ("PCI DSS") requirements. Moreover, Home Depot's in-store payment systems did not encrypt customer credit card data; rather, data was sent from Home Depot stores to central servers in clear text, making it vulnerable to attack. In addition, since news of the breach broke, news reports and tech bloggers have suggested that part of the reason Home Depot was vulnerable to the attack was that it continued to use Windows XP embedded as its operating system on its point of sale terminals, rather than upgrade to a more secure operating system.

13. According to former Home Depot managers interviewed by news outlets, Home Depot bought a tool from Voltage Security in January 2014 to encrypt card data, which had not been installed as of April 2014. Based upon Home Depot's announcements, it appears that the tool to which the former managers referred was the encryption technology that was installed in all U.S. stores as of September 13, 2014. It is unclear why there

was such a long gap between the purchase of the encryption technology and its installation in Home Depot stores. Although many details about the breach have yet to be disclosed, it is possible that earlier installation could have prevented or at least mitigated the effects of the data breach.

14. According to news sources, security consultants urged Home Depot between August 2013 and February 2014 to turn on an intrusion prevention feature in its software suite. FishNet Security prepared a report for Home Depot that was published around October 1, 2013, warning Home Depot that the Company left its computers vulnerable by failing to activate Symantec's Network Threat Protection firewall and relying instead on a Window's firewall.

15. The breach of Home Depot's systems is all the more troubling given the recent history of major retailers' payment systems being compromised by malware. In December 2013, Target Corp. ("Target") announced that its payment systems were breached. Until the attack that struck Home Depot, Target's data breach was reported to be the largest retail hack in U.S. history.

16. As a result of this data breach, information has come to light suggesting that Home Depot did not properly secure its customers' credit

card information, possibly in violation of several state and federal laws and Home Depot's agreements with credit card companies.

PLAINTIFF'S DEMAND LETTER AND HOME DEPOT'S DEFICIENT RESPONSE

17. In consideration of the foregoing facts, Plaintiff seeks to (a) investigate potential wrongdoing, mismanagement, and breaches of fiduciary duties by the members of the Company's management and certain directors of the Board or others in connection with the events, circumstances, and transactions described herein; (b) assess the ability of the Board to impartially consider a demand for action (including a request for permission to file a derivative lawsuit on the Company's behalf) related to the items described in the Demand including the scope of such Demand; (c) determine whether the current directors are fit to continue serving on the board of directors; and (d) take appropriate action in the event the members of the Company's management and certain directors did not properly discharge their fiduciary duties, including the preparation and filing of a stockholder derivative lawsuit, if appropriate.

18. On September 30, 2014, Plaintiff's counsel mailed the narrowly tailored Demand to the Chairman of Home Depot's Board of Directors,

demanding to inspect the books, records and documents of Home Depot relating to the various matters described herein. The Demand was accompanied by proof of ownership of Home Depot common stock and a Power of Attorney signed under oath by Plaintiff, appointing Holzer & Holzer, LLC and Faruqi & Faruqi, LLP as Plaintiff's attorney-in-fact to act on Plaintiff's behalf to make the Demand pursuant to Section 220. A copy of Plaintiff's Demand (and exhibits thereto) is attached hereto as Exhibit A and incorporated herein by reference.

19. Pursuant to the Demand, Plaintiff requested that the Company produce or allow the inspection of the following documents:[4]

> 1) All Board Materials[5] that concern, raise or discuss any of the following topics:

[4] The Demand defines "Documents" to incorporate the "term as used in Delaware Court of Chancery Rule 34(a), including all correspondence related to a given category, and all electronically created and retained directories, files, documents, spreadsheets, graphical renderings and e-mails with their attachments."

[5] The Demand defines "Board Materials" to mean all documents concerning, related to, provided at, considered at, discussed at, or prepared or disseminated in connection with any meeting of the Company's board of directors or any regular or specially created committee thereof, including all presentations, board packages, recordings, agendas, summaries, memoranda, transcripts, notes, minutes of meetings, drafts of minutes of meetings, exhibits distributed at meetings, summaries of meetings, or resolutions.

a) How Home Depot was notified of the potential breach first reported on September 2, 2014, and all steps taken subsequent to that notification, including but not limited to the identities of the source of the notification and any immediate measures taken to secure customer payment data.

b) Any discussion, analysis and/or report concerning the hackers' method of entry into Home Depot's payment security systems.

c) Any discussion, analysis and/or report concerning any prior breaches of Home Depot's systems, including but not limited to information about the data stealing virus found in July 2013 at a Home Depot in Denton, TX and the Infostealer virus found in December 2013 at a Columbia, MD Home Depot Store.

d) Any analysis and/or reports on payment data security in any of Home Depot's stores, including but not limited to information about: (i) the operating system in place at Home Depot's point-of-sale terminals, the potential security risks incurred by not upgrading to a more secure operating system, and the cost of upgrading to a more secure operating system; (ii) implementing EMV Chip-and-Pin technology in Home Depot's stores, the potential security risks incurred by not implementing such technology, the costs of implementing it in all Home Depot stores, and the rationale for implementing such technology in Canada before the U.S.; (iii) the edition of Symantec antivirus software, or other antivirus software, that Home Depot was running as of April

1, 2014, and what plans there were to update that software; (iv) whether continuous monitoring of Home Depot's network for unusual behavior was in place and the frequency with which the Company conducted full network scans; (v) knowledge about methods Home Depot could have used to defend its systems from malware and the cost of different anti-malware systems that could have been implemented; and (vi) security problems associated with self-checkout registers and the steps needed to neutralize those problems.

e) Home Depot's encryption project and the purchase of Voltage Security encryption technology, including but not limited to any analysis and/or reports on the progress of implementing that technology before and after the breach.

f) Any discussions, analysis and/or reports about why the encryption technology was installed in all U.S. stores as of September 13, 2014 but why it has not yet been installed in Canadian stores.

g) The cost of Home Depot's payment data security system in place in April 2014 and the cost of the new encryption system, which was completed in U.S. stores on September 13, 2014.

h) Any discussion, analysis and/or report concerning the 2013 and 2014 data breaches at other major retailers such as Target, including but not limited to whether Home Depot was doing enough to protect its customers' data from similar breaches.

i) Any due diligence conducted on Home Depot's former senior IT security architect, Ricky Joe Mitchell, including but not limited to information

concerning his termination from EnerVest Operating and whether he is thought to be involved in the breach.

j) The decision to hire outside security consultants in 2013 and 2014 prior to the breach, including but not limited to FishNet Security, and information about: (i) the reasons the outside security consultant was hired; (ii) the outside security consultant(s) recommendations; (iii) whether those recommendations were followed; and (iv) if any recommendations were not followed, an explanation as to why they were not followed.

k) FishNet Security's report for Home Depot that was completed on or about October 1, 2013, including but not limited to information about: (i) the reason Home Depot requested the report; (ii) FishNet Security's recommendations in the report; (iii) whether Home Depot followed those recommendations; and (iv) if Home Depot did not follow all the recommendations, an explanation as to why it did not.

l) Any analysis and/or report concerning how Home Depot estimated the cost of the breach to the company.

m) Discussions or correspondence related to employees' concerns about Home Depot's security software, handling of customer data, or requests for security training as of April 2014.

n) Any programs or policies for complying with the Payment Card Industry Data Security Standard ("PCI DSS") version 2.0 requirements 1-12, and any discussions, programs or policies about

implementing the changes required by version 3.0 of the PCI DSS, including but not limited to:

i) Home Depot's Vulnerability Management Program or similar plan in place as of April 2014, which contains information about how the Company uses and updates its anti-virus software or programs and develops and maintains secure systems and applications;

ii) Home Depot's access control measures, in place as of April 2014, including but not limited to information pertaining to the type of cardholder data that Home Depot stores and the amount of time for which it stores that information, whether each store employee with computer access has his or her own unique ID to access the computer, whether there are measures in place to restrict physical access to cardholder data, and if so, what those measures included;

iii) Home Depot's policies and programs, in place as of April 2014, to monitor and test networks, including but not limited to information concerning how the Company tracks and monitors access to network resources and cardholder data, and how frequently security systems and processes are tested; and

iv) Home Depot's information security policy or similar policy, in place as of April 2014, that addresses information security for all personnel.

o) Any post-April 2014 updates that Home Depot made to the programs or policies requested in paragraph 1(n) above.

p) The decision to retain Symantec and FishNet Security, and any other consultants, to aid Home Depot in determining whether a breach occurred and to help fix the breach, including but not limited to the cost of hiring those companies and any other consultants, and the scope of their investigation.

q) Any discussions, analysis and/or reports on the multiple lawsuits filed against Home Depot on or after September 2, 2014 alleging that the plaintiffs suffered damages as a result of the breach.

r) All Reports on Compliance that Home Depot submitted pursuant to the PCI DSS and any discussions, analysis and/or reports about the same.

s) The process by which Home Depot makes decisions about upgrading its systems, including but not limited to information concerning the input of Home Depot's IT security staff.

2) Any and all communications between and among Home Depot's directors and officers and/or management in connection with any of the items enumerated above in request 1(a)-(s).

20. The Demand enumerated the following legitimate and proper purposes for the inspection of the books, records, and documents:

(a) to investigate potential wrongdoing, mismanagement, and breaches of fiduciary duties by the members of the Company's management and certain directors of the Board or others in connection with the events, circumstances, and

transactions described herein;

(b) to assess the ability of the Board to impartially consider a demand for action (including a request for permission to file a derivative lawsuit on the Company's behalf) related to the items described in this demand including the scope of such demand;

(c) to determine whether the current directors are fit to continue serving on the board of directors; and

(d) to take appropriate action in the event the members of the Company's management and certain directors did not properly discharge their fiduciary duties, including the preparation and filing of a stockholder derivative lawsuit, if appropriate.

21. These purposes are reasonably related to Plaintiff's interest as a stockholder of the Company, and the inspection is not sought for a purpose that is in the interest of a business or object other than the business of the Company.

22. The books and records sought are narrowly tailored to serve Plaintiff's purposes in sending the Demand.

23. Shortly thereafter, counsel for Home Depot advised that they needed additional time to consider the Demand, but would agree to the production of a general set of documents related to the breach assuming that an agreement regarding confidentiality could be reached.

24. After considerable negotiations, the NDA was entered into

between Plaintiff and Home Depot on October 29, 2014.

25. On November 17, 2014, counsel for Home Depot, on Home Depot's behalf, sent a letter to Plaintiff's counsel wherein Home Depot refused to produce the document's demanded but agreed instead to produce the following:

> Board minutes and materials dated on or after January 1, 2013 from the Company's official board files concerning the following topics to the extent such documents exist:
>
> (i) The 2014 Breach, including notification of the Breach and any discussions or analysis of its materiality;
>
> (ii) The Home Depot's cybersecurity controls, processes, policies and procedures, including materials related to The Home Depot's payment data system;
>
> (iii) Outside incidents of cyberattacks (i.e. discussion of the Target breach); and
>
> (iv) Compliance with regulations concerning payment data systems.

26. Home Depot's counsel refused the Demand for the reason that the Demand "greatly exceeds the scope of inspection permitted under Delaware law."

27. On March 18, 2015 Home Depot's counsel indicated that it had completed its document production "pursuant to the parameters set forth in

[his] letter dated November 17, 2014." Counsel's letter also notes that it redacted responsive, non-privileged materials that fell within the Company's own agreed up production parameters (the "Redacted Documents").[6]

28. The Redacted Documents reflect the Board's involvement and consideration of cybersecurity-related issues between February 2013 and August 2014.

29. Home Depot's counsel further indicated in his March 18, 2015 letter that the production of these documents "is not necessary and essential to addressing [plaintiff's] stated purpose."

30. According to Home Depot's counsel's March 18, 2015 letter the Redacted Documents purportedly "reflect in great detail the internal audits performed on the Company's cybersecurity processes, the results of those audits, and in some instances, the actions taken in response to the audit results." Nothing could be more essential to Plaintiff's stated purposes.

[6] According to Counsel's letter the following documents were redacted for security reasons: FROHMAN__000009-28 (dated 2/28/13), THD-FROHMAN__000050-52(dated 5/22/13), THD-FROHMAN__000150-154(dated 8/20/14), THD-FROHMAN__000271-275(dated 8/20/14), THD-FROHMAN__000347 (dated 2/28/13), THD-FROHMAN__000357-358(dated 8/22/13), THD-FROHMAN__000369-373(dated 2/27/14) and THD-FROHMAN__000378(dated 5/21/14).

31. In an attempt to avoid litigation, Plaintiff sent a follow-up letter to Home Depot's counsel on April 16, 2015 noting a number of significant deficiencies in the Company's production and requesting that they rectify the deficiencies. Specifically, the letter states that:

> Further, and most important, several documents have been redacted not based on relevancy or privilege grounds but rather because Home Depot determined that "[w]hile we produced these documents to demonstrate the Board's involvement in and consideration of cybersecurity-related issues, the level of detailed sensitive information contained therein is not necessary and essential to addressing your stated purposes" of the Demand. The fact that the Board was involved in and considered cybersecurity-related issues is of no import where you concede that the documents you refuse to produce "reflect in great detail the internal audits performed on the Company's cybersecurity processes, the results of those audits, and in some instances, the actions taken in response to the audit results." Indeed, based on your own assessment, these documents probably rank as the most essential of all in providing the highly particularized information of what the Board knew about the Company's cybersecurity measures and when they knew it, the testing of those measures and results of that testing, and where there were cybersecurity issues raised by the audits, what actions were taken, if any, to strengthen Home Depot's cybersecurity systems. All of the documents that you contend fall into this category pre-date the discovery of the September 2014 data breach and thus, go to the very heart of

> what the Board knew and what it was doing if anything about the specifics of the Company's cybersecurity-related issues.[7]

The letter also raises concerns with redactions, a lack of documents responsive to some of the requests made in the Demand, missing documents, incomplete documents[8] and the lack of a privilege log.

32. On May 8, 2015, counsel for Home Depot responded to the April 16, 2015 letter by producing four additional pages and a privilege log. In responding to Plaintiff's request for the Redacted Documents, Home

[7] The letter is attached hereto as Exhibit C.

[8] For example, the Company produced a document with the bates range of THD-FROHMAN__000302-306. The document contains the agenda and materials for the Company's November 21, 2013 Board of Directors meeting, which originally was 96 pages long. The document produced by the Company only contains only five pages (1, 75, 79, 80 and 81). According to the Company, the remaining pages were not produced because they contained "non-relevant and non-responsive material" and instead they produced only "the relevant, non-privileged material in response to your demand." Letter from Home Depot's Counsel to Plaintiff's Counsel dated May 8, 2015 at 3 (attached hereto as Exhibit D). However, the company's privilege log contradicts its counsel's statement. According to the log, page 81 (THD-FROHMAN__000306) is fully redacted except for the header and footer because the page is "non-responsive." Yet the Company states that Home Depot excluded pages from documents unless they contained "relevant, non-privileged material." Such inconsistencies call into question the accuracy of the privilege log and the production in general.

Depot stated that the Company was "open to discussing a secure way for you to view these documents without creating additional risks to the Company's security. Please advise us how you propose to review these documents in a secure manner and how you plan to maintain the security and confidentiality of these documents should we agree to share them with you at this time."

33. In response, after discussion with a consulting expert in information security, Plaintiff's counsel suggested several methods by which the Redacted Documents could be reviewed securely. On a teleconference held on May 22, 2015, Home Depot's counsel rejected these suggestions and requested that counsel review the Redacted Documents in Atlanta at the offices of Alston & Bird. Plaintiff's counsel agreed despite the costs and inconvenience associated with such an approach.

34. After the teleconference, Plaintiff's counsel emailed Home Depot's counsel on May 29, 2015, to arrange a date to view the Redacted Documents. No response was received through the date of this filing.

35. By reason of the foregoing, pursuant to Section 220, Plaintiff is entitled to inspect and make copies and extracts of the books and records of Home Depot as identified in the Demand.

PLAINTIFF'S DEMAND LETTER SETS FORTH A PROPER PURPOSE

36. Home Depot has improperly rejected Plaintiff's right to inspect the demanded books of the Company.

37. As discussed above, the allegations of lax cyber security at the Company, the pending government investigations, together with numerous lawsuits claiming misconduct at Home Depot, provide a credible basis from which mismanagement at the Company can be inferred.

38. Investigations of potential wrongdoing, mismanagement, and breaches of fiduciary duties by the members of the Company's management and certain directors of the Board or others are entirely proper purposes for a Section 220 demand, and the Court of Chancery encourages their use by concerned shareholders.

39. As such, Plaintiff has met the required burden and the Court should find that Plaintiff is entitled to inspect all of the books and records of Home Depot, in unredacted form, as set forth in the Demand letter.

PLAINTIFF'S REQUESTS ARE ESSENTIAL TO ACCOMPLISHMENT OF PLAINTIFF'S ARTICULATEDPURPOSE

40. Home Depot's assertion that the documents requested pursuant to the Demand exceed the items that could properly be the subject of a stockholder demand is misplaced. Each of the requests set forth in Plaintiff's Demand is tailored to an investigation to the books and records of Home Depot for Plaintiff's stated purposes.

41. Home Depot has violated its statutory obligation to permit Plaintiff to inspect the books and records demanded by Plaintiff. As a result, Plaintiff now seeks court intervention to ensure that Home Depot complies with Plaintiff's Demand.

42. By reason of the foregoing, pursuant to Section 220, Plaintiff is entitled to inspect and make copies and extracts of the books and records of Home Depot as identified in the Demand.

COUNT I
(Demand for Inspection Pursuant to 8 *Del. C.* § 220)

43. Plaintiff repeats and realleges all of the preceding allegations as if fully set forth herein.

44. On September 30, 2014, Plaintiff made written demand upon

Home Depot for the inspection of books, records and documents set forth in the Demand letter.

45. Plaintiff has complied fully with all requirements under Section 220 of the DGCL respecting the form and manner a demand for inspections of the books, records and documents set forth in the Demand.

46. Plaintiff's demand for inspection is for proper purposes. Moreover, the documents identified in the Demand are essential to those purposes.

47. More than five business days have passed since Home Depot received the Demand, and the Company has refused to permit the inspection sought by Plaintiff by improperly denying access to unredacted copies of all of the books and records identified in the Demand.

48. By reason of the foregoing and pursuant to 8 *Del. C.* § 220, Plaintiff is entitled to an order permitting it to inspect and make copies of the books and records set forth in the Demand.

49. Plaintiff has no adequate remedy at law.

WHEREFORE, Plaintiff demands judgment as follows:

A. An Order compelling Home Depot, its officers, directors, employees, and/or agents immediately to permit Plaintiff, her

attorneys and/or agents to inspect and make copies and extracts of the books and records of Home Depot identified in the Demand immediately;

B. An Order requiring Home Depot to pay Plaintiff's costs and expenses, including reasonable attorneys' fees, incurred in the prosecution of this action; and

C. Granting such other and further relief as the Court deems just and proper.

Dated: June 8, 2015

Respectfully submitted,

By: /s/ James R. Banko
James R. Banko (#4518)
FARUQI & FARUQI, LLP
20 Montchanin Road, Suite 145
Wilmington, DE 19807
Telephone: (302) 482-3182
Facsimile: (302) 482-3612
Attorney for Plaintiff

OF COUNSEL:

Stuart J. Guber
Timothy J. Peter
FARUQI & FARUQI, LLP
101 Greenwood Avenue, Suite 600
Jenkintown, PA 19046
Telephone: (215) 277-5770
Facsimile: (215) 277-5771

-and-

Nadeem Faruqi
Nina Varindani
FARUQI & FARUQI, LLP
369 Lexington Avenue, 10th Floor
New York, NY 10017
Telephone: (212) 983-9330
Facsimile: (212) 983-9331

-and-

Corey D. Holzer
Marshall P. Dees
HOLZER & HOLZER, LLC
1200 Ashwood Parkway, Suite 410
Atlanta, GA 30338
Telephone: (770) 392-0090
Facsimile: (770) 392-0029