



Presentation  
Handouts

# Cyber Risk Management Facing Boards, C-Suites & General Counsel:

Prevention, Crisis Management, and  
Mitigating Personal Liability

May 10, 2017

BY PAOLO BORGHESI,  
JON RIGBY, DAVID WHITE  
AND JIM HART



# **GUARDING against cyber threats**

**In a world awash in cyber threats, partners and suppliers can be the vulnerable points that cyber criminals exploit to gain access to systems. Those challenges will get worse before they get better as supply networks become ever more complex. As a matter of urgency, business leaders must proactively balance cyber risks against opportunity, growth and profitability, starting with a clear-eyed view of the size and scale of the risks. Then it's time to set concrete expectations for suppliers. Here's a snapshot of the discussions you should be having right now.**

**N**ot too long ago, Goodwill Industries found that its customers' payments data had been breached by cyber criminals. Data from 868,000 payment card accounts was stolen. The entry point for the attack? Hackers had used malware to penetrate a third-party vendor's systems.

A year earlier, Target made news when it suffered a huge and highly publicized breach in which data from 110 million customers and 40 million payment cards was stolen. The national retailer's systems were initially breached via a connection with one of its vendors, an HVAC provider.

Goodwill and Target are by no means alone. Cyber breaches are proliferating year over year, affecting the confidentiality, integrity and availability of data; recent research by IBM indicates that just between 2014 and 2015, the number of such security incidents increased by 64%. These statistics probably reveal just the tip of the iceberg; they refer only to the security incidents that are detected and declared.

Retail and telecommunications companies are some of the most common victims of such attacks, but now, the Internet of Things (IoT) is also making manufacturing and production just as vulnerable. More broadly, ancillary sub-systems have proved alarmingly open to attack; there are well-publicized

---

*Paolo Borghesi is vice president, Cyber Security Strategy, at AlixPartners LLP. He can be reached at [pborghesi@alixpartners.com](mailto:pborghesi@alixpartners.com). Jon Rigby is director of AlixPartners' Cyber practice. He can be reached at [jrigby@alixpartners.com](mailto:jrigby@alixpartners.com). David White is director of legal services at AlixPartners. He can be reached at [dwhite@alixpartners.com](mailto:dwhite@alixpartners.com). Jim Hart can be reached at [jim\\_hart\\_99@hotmail.com](mailto:jim_hart_99@hotmail.com).*

stories of car engine-control computers being accessed by hackers via CD players and tire pressure monitors. Seemingly innocuous devices have been used in massive denial-of-service disruptions; these attacks recently wreaked havoc on Amazon, BBC, CNN, Netflix and other household-name organizations when Internet-connected devices,

## **More cyber attacks—whether inadvertent or malicious—are coming from insiders: employees, contractors, consultants, suppliers and partners.**

such as printers, cameras and baby monitors, were hacked.

At least as worrying: more of the attacks—whether inadvertent or malicious—are coming from insiders: employees, contractors, consultants, suppliers and partners. In nearly two-thirds of incident response investigations, a major component of IT support was outsourced to a third party, according to the 2013 Global Security Report from Trustwave, a security services provider. No business operates independently of partners or suppliers: A company's connections with those entities ranges from the exchange of purchase order details via e-mail or some other electronic exchange, to vendor-controlled facility management systems, to integrated design and production environments—all of which are potential security vulnerabilities. The push for greater efficiency and more innovation opportunities adds to the pressure to integrate with others in the supply chain, often without due consideration of the concomitant rise in business risk.

Of course, there is no shortage of techniques and technologies to minimize that risk. Even in the most complex businesses, it is possible to segregate information to allow for complete trust and openness with suppliers in one business process while blocking access to other information. The implementation of these safeguarding measures is not just an IT function; it requires business leaders to consider their information requirements as closely as they consider their physical pipeline, and it calls for commercial staff to write contracts that allow oversight of suppliers' information security.

It is not that business leaders aren't aware of the challenges—or aren't trying. More than two-thirds (69%) of public company board members report that their board is "more involved" with cyber security than it was 12 months earlier, according to a survey by BDO. That still isn't

enough. Despite this increase in awareness, just one-third (34%) of corporate directors report that they have documented and developed solutions to protect their business's critical digital assets. Clearly, more must be done.

In practice, business executives should adopt a risk mindset. Few of the useful risk-mitigation techniques can be truly effective if business leaders fail to balance the trust they place in partners and suppliers against the risks to their bottom line and value. They must weigh opportunity, growth and profitability against risk and make conscious investment decisions based on their business judgment. It is incumbent on executives and directors to educate themselves about cyber security and empower themselves to make informed decisions.

The obvious part of that imperative is to minimize the likelihood and thus the consequences of any data breach—regardless of where it occurs in the supply chain. For public companies, the consequences can be far-reaching: In the United States, the Securities and Exchange Commission's guidance requires that companies not only disclose material cyber security events when they occur, but also disclose material risks that could occur. For those companies that outsource functions with material risks, the guidance requires a description of those functions and how companies address the risks. But there is an upside to sound cyber security as well: Companies that truly embrace appropriately balanced cyber security measures could build capabilities that likely give them a considerable edge over their competitors.

## **The two Achilles heels of the supply chain**

Any supply chain has both internal and external cyber vulnerabilities. This article is focused on the latter, but for context, it's worthwhile to look briefly at the internal issues.

Within the four walls of the organization, systems are becoming markedly more vulnerable to cyber attacks. This is especially true in the manufacturing industry, where industrial control systems (ICSs), based on proprietary technology, have historically controlled automated production processes. Those systems were isolated from the network, meaning that to use them, factory operators had to be physically present and know how to use them.

However, over time, ICS systems (such as SCADA,

for example) began using “standard” technology (such as the Windows operating system, or SQL server as a database) and are now connected to the corporate network so they can consolidate and share information across the enterprise. This provides significant added value in that it enables companies to monitor and manage production remotely, but it also increases the chance of being subject to a cyber attack.

Additionally, there are now more ways to access industrial control systems. Once they are more broadly networked, physical access is no longer required. The system might then be accessed by malware spread across the corporate network. The malware no longer needs to be custom written for proprietary operating systems because the new systems are based on common commercial platforms. Now, a simple malware infection on a corporate IT system can easily spread to the industrial system if not properly protected.

When you move outside the four walls of the organization, the problem is just as worrisome. Most companies now manage hundreds and sometimes thousands of external, outside vendor relationships, most of which involve some level of information sharing and access. This creates significant vulnerabilities, especially when these processes are automated. Gone are the days of fortification when a

company could build a firewall around its IT perimeter and protect its information; most companies can no longer even draw a distinct line around their network perimeters, so fuzzy are the boundaries between their networks and those of their partners. Vendor integration, along with the adoption of Cloud-based computing services and employee programs such as bring-your-own-device (BYOD) and telecommuting, have nearly eliminated the corporate perimeter entirely.

Some companies are now struggling to find ways to manage and govern this problem, which is not just an IT or procurement issue. It’s a corporate-wide risk issue, which now is getting the attention of legal and compliance groups. What, then, is needed? The answer is the development of more sophisticated oversight programs.

### **Dampening external supply chain risks**

So what will it take to do that—and thus to mitigate cyber security risk in the supply chain? These days, there is no shortage of good information available to describe responses to cyber security in general. But the authors of this article have found that the following approaches are especially relevant for guarding against breaches of the external supply chain.

- **Map the data flows in the supply chain.** Most business



leaders now recognize that data is a primary asset, but fewer have a clear understanding of how data flows in and out of their companies, who they are sharing it with and how those flows are being managed and controlled—both internally and externally.

- **Plan a comprehensive risk assessment.** The organization's approach to cyber security should not be viewed in isolation from its mainstream business activities; they are too tightly interconnected. The level of protection has to be proportional to the potential impacts and likelihood of an incident. For this reason, an information security risk assessment could be the right way to assess the security of the supply chain and identify the critical areas to be addressed. The assessment will go beyond the data mapping noted above. Ideally, a third party whose independence can help ensure objectivity should conduct the assessment.

- **Align with emerging standards.** New standards have been developed as companies become aware of cyber security risks, especially with regard to the supply chain. In particular, organizations such as the Nation Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) have published frameworks and guidelines related to the management of

**Supply chain connections range from the exchange of purchase order details via e-mail or other electronic exchange, to vendor-controlled facility management systems, to integrated design and production environments—all of which are potential security vulnerabilities.**

cyber security. These frameworks, created through collaboration between government and the private sector, use a common language to address and manage cyber security risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. NIST has also produced a short animated video\* about the framework that is intended for C-suite executives as well as cyber security professionals.

Many other organizations and standards-setting communities have followed suit with their own frameworks. One of the most important features of these frameworks is their emphasis on the importance of the capabilities needed to respond to

cyber attacks. The understanding is that attacks are inevitable, so rather than just seeking to guard against them, it is crucial to build systems with the resilience to rapidly respond and ideally to minimize the damage they can cause.

- **Set clear expectations in all supply chain contracts.**

Admittedly, this is easier said than done. Yes, contractual clauses around security levels and assurances are a necessary step, but many companies are struggling to define the levels of specificity required in such clauses, and wrestling with the issues of cyber security audits and enforcement monitoring. When you have thousands of suppliers, how can you possibly audit all of their security controls? It's hard enough to audit your own. Third-party certifications and attestations are helping, but there are still plenty of gray areas about the scope of the attestation and how effective they are. Certifications are also expensive and time-consuming for vendors to achieve, and it's difficult to define the level and type of certifications they need.

Furthermore, not all certifications are equal, and companies must be alert to clever marketing by suppliers boasting of certifications for new data centers, for instance. Customers must look closely to ensure that it is the vendor's own controls that are being certified—not just that the vendor is using a third-party data center that is certified.

Simplicity is the safest approach: Organizations should ensure that all of their outsourcing contracts require their suppliers to adhere to defined maturity and audit standards; that they do this in turn with their suppliers; and

that they agree to provide access to cyber security audit results at least once a year. If a supplier cannot show such results and is reluctant to agree to such practices, then perhaps their vendor status should be reconsidered.

- **Insure, but never depend on it.** Certainly, insurance coverage can help to shift the risk, but we are now seeing that it's often not enough to cover losses. For example, Home Depot, whose massive breach made headlines around the world a few years ago, is now up to hundreds of millions of dollars in costs and still has dozens of lawsuits pending. The cap for most insurance policies designed to cover damages from cyber security breaches is usually

about \$100 million, and many such policies have a myriad of gaps in their coverage. Moreover, coverage may be denied or limited where companies do not diligently assess and manage their data-sharing relationships. The patch-

## **There is an upside to sound cyber security as well: Companies that truly embrace appropriately balanced cyber security measures could build capabilities that likely give them a considerable edge over their competitors.**

work of regulatory frameworks around security requirements, data privacy, and cross-border data transfer and data localization laws only serve to compound the problem and make governance more complex.

### **How suppliers should handle customer information**

And what obligations do suppliers have? What should be their priorities when it comes to recognizing their roles and responsibilities in guarding supply chains against cyber attacks—and building more resiliencies into their systems when cyber criminals do break in?

As a fundamental, a supplier should understand the security protections they should be offering to protect their customers' data. A prerequisite, of course, is that they acknowledge and assess the connectivity between them, and thus have a clear idea of the risks that they, as the supplier, may be introducing as a consequence of their handling of supply chain data.

At the same time, suppliers should strive for compliance with recognized security certifications. The most common among these include the U.S. Health Insurance Portability and Accountability Act (HIPAA) assessments, the American Institute of Certified Public Accountants Service Organization Control Reports (SOC 2) and the Payment Card Industry Data Security Standard (PCI-DSS). As a recommendation, suppliers should be aligned with the ISO 27001:2013 standard—the internationally applicable Information Security Management System. However, compliance with those certifications is unlikely to be enough; suppliers must seek out and work to comply with certifications specific to their industries and to their customers' needs.

Moreover, suppliers must help prevent supplier fraud—a

growing problem these days, even though it doesn't require technical expertise by the perpetrators. Their customers stand to lose a lot if the procurement or finance team is duped by a legitimate-looking e-mail from a supplier asking

to change the banking details for a big payment. To minimize the likelihood of unwittingly enabling such scams, suppliers should proactively work to establish better lines of communication with their customers—for example, agreeing on a process

that includes additional steps for further confirmation of any such change to their banking details.

### **What opportunities can cyber security create?**

So far, we have emphasized protection against the downside of cyber security breaches. But there is a more positive perspective too: the idea that high levels of supply chain data security can be used for competitive advantage. For example, promotes its ISO 27001 certification for Online Banking and Mobile Banking services on its Website.\*\*

More and more customers can be expected to look for demonstrably high levels of security. Suppliers that can show bona fide security framework certifications such as ISO 27001 could conceivably expect to be able to factor those credentials into their pricing and future contract negotiations. Furthermore, proven cyber security credentials can be used to establish differentiation—to show that one's company is more secure than others in its markets.

Clearly, the topic of supply chain cyber security is timely and fraught with challenges all its own. There are far more subtleties and interpretations to describe than can be laid out in a single article. But if there is one message that the authors hope to convey, it is that the issue is not one that can be postponed until the next meeting of the board of directors—or worse, until the next security breach. British wartime leader Winston Churchill was famous for his insistence on “action this day.” We think that is an appropriate maxim for tackling the many cyber security onslaughts of the 21st century. ☺☺

\* The NIST video can be viewed at [nist.gov/cyberframework](http://nist.gov/cyberframework)

\*\* Barclay's online certification can be viewed at [barclays.co.uk/Security/ISO27001certification/P1242561780370](http://barclays.co.uk/Security/ISO27001certification/P1242561780370)

# METROPOLITAN CORPORATE COUNSEL®

MARCH 2017

WWW.METROCORPCOUNSEL.COM

## How Counsel Can Improve Cyber-Risk Programs



## INFORMATION GOVERNANCE INSIGHTS

By **David White**

**T**he role of corporate counsel has been rapidly evolving in the past few years. The scope of responsibilities has expanded beyond legal administrative tasks to include companywide risk management, cost control, regulatory compliance and other areas that affect the company's reputation and bottom line. Data privacy and security, which used to sit squarely in the domain of the information technology department, now has the full attention of customers, shareholders and government regulators. As a result, senior management and the board are relying more and more on corporate counsel to be both the steward and the shepherd of cyber-risk governance programs.

This doesn't mean that counsel have simply inherited IT's responsibilities for managing cyber compliance. Quite the contrary. IT must still ensure that the computer systems they manage are properly secured. Counsel's role is to look beyond this hardening of IT systems to develop a more comprehensive cyber-risk governance program. Ideally, this program should consider cybersecurity from a broad perspective, and ensure that the company's statutory, contractual, regulatory and reputational liabilities are properly managed and minimized. Here are some best practices to consider to improve cyber-risk programs:

### **1 Take a top-down approach.**

Most security professionals and practitioners would agree that total prevention is not possible. However, a top-down approach that embeds cybersecurity management throughout a company's infrastructure is the most effective way to mitigate risk. This means developing a governance model that starts at the board level, and then moves down through the C-suite and line managers to ensure accountability at all levels.

Many directors may not have the technical background to make decisions on their own, so the company should line up

mechanisms to ensure that everyone has the assistance they need. These include the company deploying special cyber review or technology committees, and ensuring that other directors or advisory committee members have some technical or cyber experience as well. The committee can then perform periodic (typically quarterly) reviews and report to the board biannually. If it's not possible to create a dedicated technology committee, you should integrate the cybersecurity team into the audit or risk committee agendas for board reporting and decision-making. Determining which structure is most appropriate really hinges on the regulatory requirements, and the overall size and global footprint, of your company.

### **2 Make sure that the management team fully understands the risks.**

You should conduct a full cyber-risk assessment that considers both the likelihood of various potential scenarios and the overall impact that each would have, using in-house resources and supplementing these with external assistance, where needed. To this end, it is important that you require senior management to know who the company's primary threat actors and stakeholders are. These can differ greatly across industries and geographies, and even across internal departments. It is therefore important that management provides a road map of the actual and potential actors or perpetrators they face.

The road map should also include the data privacy and security expectations of their key stakeholders and constituents. In addition, counsel should also require management to provide a clear and comprehensive map of company information assets that are susceptible to cyberattack. It's imperative to know what key assets are, where they are stored and what their internal and external values are in order to understand the controls needed to properly protect them. You should then ask some key questions, such as "How is the company positioned to handle any one of the identified adverse scenarios?" And "Is our current approach the optimal approach?"

**AlixPartners**  
when it really  
matters

*David White is a director at AlixPartners LLP, where he advises clients on information governance, information security and electronic discovery. He can be reached at [dwhite@alixpartners.com](mailto:dwhite@alixpartners.com).*



### 3 Involve other departments.

Information assets and the risks they pose can differ greatly across the company. It is important to develop both a cross-disciplinary approach to cyber-risk management and a cross-segmental or divisional approach to cyber-risk management, including effective executive and board reporting. The information that each functional unit reports must be not only meaningful to more senior stakeholders, but also actionable.

The historic response to this challenge has been to use checklists, which are typically developed as a way for counsel to translate requirements into layman terms. Canned reports that IT professionals use to translate technological language into something others can understand and quickly review are equally common. But checklists and canned reports are unlikely on their own to give a clear picture of actual risk. This is especially true when they are just recycled metrics developed for other needs, such as the often-used common vulnerability scoring system (CVSS) reports, which were originally deployed for vulnerability response. Knowing how many vulnerabilities were reported and remediated in each quarter has very little value to a board that cannot discern if they were the right vulnerabilities or if their remediation had any impact on actual risk. (Sure, IT security closed 10,000 application vulnerabilities last period, but did that really help?)

More holistic risk reporting through a comprehensive portal that contains meaningful key performance indicators (KPIs) is essential to building an effective risk governance program. KPIs should be simple and easy to read. They should include, as a baseline, a road map that shows what your current risk profile is, where you want it to go in the future and what steps you are taking to get there.

### 4 Build cyber-risk partnerships.

Beyond leveraging internal resources, it is equally important that counsel build appropriate cyber-risk partnerships. These include actively engaging with your vendors and business partners, participating in both private-sector industry cybersecurity benchmarking and information-sharing programs. You should also monitor appropriate industry and government initiatives, and routinely engage outside advisers to take a fresh look at your cyber-risk governance program. In my sailboat racing days, we used to call this getting your head outside the boat. You can't hyper-focus on the tasks in front of you. To be successful, you have to also keep abreast of what is happening outside your company and what others around you are doing in response. It's important to look outside the organization and get constant feedback from experts with broader industry experience. Otherwise you will only focus on what you see in the boat, and probably completely miss that giant oil tanker headed straight at you.

Before leaving office, President Barack Obama called cyber-risk "one of most serious economic and national security challenges" facing America. As more and more critical company assets – including intellectual property, corporate strategies and consumer information – are stored electronically, developing robust cyber-risk governance programs could not be more important. As a result, general counsel and their legal teams must be proactive about taking a leadership role on cyber-risk governance. By staying properly informed about the company's cyber-risk profile and liabilities, they can provide the necessary guidance to the board of directors, senior management and other stakeholders. Counsel who assert their dual role as the steward and shepherd of these programs can ensure that their company's most important business assets remain secure and that its risks – legal and otherwise – are kept to a minimum.

1 DAVID SHONKA  
Acting General Counsel

2  
3 LAURA D. BERGER (FL Bar No. 11762)  
Federal Trade Commission  
4 901 Market Street, Suite 570  
San Francisco, CA 94103  
5 P: (202) 326-2471/F: (415) 848-5184  
6 [lberger@ftc.gov](mailto:lberger@ftc.gov);

7 KEVIN H. MORIARTY (DC Bar No. 975904)  
CATHLIN TULLY (NY Bar)  
8 Federal Trade Commission  
600 Pennsylvania Ave N.W.  
9 Washington, DC 20580  
10 P: (202) 326-3644/F: (202) 326-3062  
[kmoriarty@ftc.gov](mailto:kmoriarty@ftc.gov); [ctully@ftc.gov](mailto:ctully@ftc.gov)

11  
12 *Attorneys for Plaintiff Federal Trade Commission*

13 **UNITED STATES DISTRICT COURT**  
14 **NORTHERN DISTRICT OF CALIFORNIA**  
15 **SAN FRANCISCO DIVISION**

16 FEDERAL TRADE COMMISSION, )  
17 )  
18 Plaintiff, )  
19 v. )  
20 D-LINK CORPORATION )  
21 and )  
22 D-LINK SYSTEMS, INC., )  
corporations, )  
23 Defendants. )  
24 )

No. 3:17-CV-00039-JD

**COMPLAINT FOR  
PERMANENT INJUNCTION AND  
OTHER EQUITABLE RELIEF**

25  
26 1. Plaintiff, the Federal Trade Commission (“FTC”), for its Complaint, brings this  
27 action under Section 13(b) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C.

1 § 53(b), to obtain permanent injunctive relief and other equitable relief against Defendants for  
2 engaging in unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15  
3 U.S.C. § 45(a), in connection with Defendants' failure to take reasonable steps to secure the  
4 routers and Internet-protocol cameras they designed for, marketed, and sold to United States  
5 consumers.

6 **JURISDICTION AND VENUE**

7 2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a),  
8 and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

9 3. Venue in the Northern District of California is proper under 28 U.S.C. § 1391(b)  
10 and (c) and 15 U.S.C. § 53(b).

11 **PLAINTIFF**

12 4. The FTC is an independent agency of the United States Government created by  
13 statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a),  
14 which prohibits unfair or deceptive acts or practices in or affecting commerce.

15 5. The FTC is authorized to initiate federal district court proceedings, by its own  
16 attorneys, to enjoin violations of the FTC Act and to secure such other equitable relief as may be  
17 appropriate in each case. 15 U.S.C. §§ 53(b), 56(a)(2)(A).

18 **DEFENDANTS**

19 6. Defendant D-Link Corporation ("D-Link") is a Taiwanese corporation with its  
20 principal office or place of business at No. 289, Xinhua 3<sup>rd</sup> Rd., Neihu District, Taipei City,  
21 Taiwan 114. D-Link transacts or has transacted business in this district and throughout the  
22 United States. At all times material to this Complaint, acting alone or in concert with others, D-  
23 Link purposefully directed its activities to the United States by designing, developing, marketing,  
24 and manufacturing routers, Internet-protocol ("IP") cameras, and related software and services,  
25 intended for use by consumers throughout the United States.

26 7. Defendant D-Link Systems, Inc., ("DLS") is a California corporation with its  
27 principal office or place of business at 17595 Mt. Herrmann St., Fountain Valley, California

1 92708. DLS transacts or has transacted business in this district and throughout the United States.  
2 At all times material to this Complaint, acting alone or in concert with others, DLS has  
3 advertised, marketed, distributed, or sold routers, IP cameras, and related software and services,  
4 intended for use by consumers throughout the United States. The Chairman of DLS's Board of  
5 Directors has served as D-Link's Chief Executive Officer and the two entities have coordinated  
6 closely regarding the security of Defendants' routers and IP cameras.

7 8. The FTC's claims against D-Link and DLS arise from or relate to Defendants'  
8 acts or practices aimed at or taking place in the United States.

9 **COMMERCE**

10 9. At all times material to this Complaint, Defendants have maintained a substantial  
11 course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act,  
12 15 U.S.C. § 44.

13 **DEFENDANTS' BUSINESS PRACTICES**

14 10. D-Link is a hardware device manufacturer that designs, develops, markets, and  
15 manufactures networking devices, including devices with core functions that relate to security,  
16 such as consumer routers and IP cameras. D-Link designs, develops, and manufactures these  
17 products, their marketing materials, and related software and services for distribution or sale to  
18 United States consumers through its subsidiary, DLS. D-Link is responsible for providing  
19 ongoing support to DLS for its products, including by remediating any design, usability, and  
20 security issues in Defendants' routers and IP cameras. D-Link also conducts security testing  
21 of the software for Defendants' routers and IP cameras. When releasing new software for such  
22 routers and IP cameras, D-Link uses a digital signature issued in its name, known as a "private  
23 key," to sign the software, in order to assure entities, such as browsers and operating systems,  
24 that the software comes from an authentic or "trusted" source and is not malware.

25 11. DLS is a subsidiary of D-Link and is nearly 98% owned by D-Link and its  
26 holding company, D-Link Holding Company, Ltd. DLS provides marketing and after-sale  
27 services integral to D-Link's operations, including by marketing and acting as the sole

1 distributor of Defendants' routers and IP cameras throughout the United States. DLS also  
2 recommends to D-Link features that D-Link should include in products designed for the  
3 United States market. Among other services, DLS acts as the primary point-of-contact for  
4 problems that United States consumers have with Defendants' routers, IP cameras, or related  
5 software and services; conducts initial inquiries into the validity of security vulnerability  
6 reports for products sold in the United States; and transmits to D-Link any such reports that it  
7 believes may warrant software security updates from D-Link. DLS also assists in notifying  
8 United States consumers about the availability of security updates through means such as  
9 DLS's websites.

10 12. Defendants have provided software applications that enable users to access their  
11 routers and IP cameras from a mobile device ("mobile apps"), including a free "mydlink Lite"  
12 mobile app. Defendants designed the mydlink Lite app to require the user to enter a user name  
13 and password ("login credentials") the first occasion that a user employs the app on a particular  
14 mobile device. After that first occasion, the app stores the user's login credentials on that  
15 mobile device, keeping the user logged into the mobile app on that device.

#### 16 **DEFENDANTS' ROUTERS**

17 13. Defendants' routers, like other routers, operate to forward data packets along a  
18 network. In addition to routing network traffic, they typically play a key role in securing  
19 consumers' home networks, functioning as a hardware firewall for the local network, and  
20 acting as the first line of defense in protecting consumer devices on the local network, such as  
21 computers, smartphones, IP cameras, and other connected appliances, against malicious  
22 incoming traffic from the Internet.

#### 23 **DEFENDANTS' IP CAMERAS**

24 14. Defendants' IP cameras, akin to many such IP cameras, play a key security role  
25 for consumers, by enabling consumers to monitor private areas of their homes or businesses, to  
26 detect any events that may place the property or its occupants at risk. In many instances,  
27 Defendants offer them as a means to monitor the security of a home while consumers are away,

1 or to monitor activities within the household, including the activities of young children, while a  
2 consumer is at home. Consumers seeking to monitor the security of their homes or the safety  
3 of young children may access live video and audio feeds (“live feeds”) from their cameras over  
4 the Internet, using a mobile device or other computer.

5 **DEFENDANTS’ SECURITY FAILURES**

6 15. Defendants have failed to take reasonable steps to protect their routers and IP  
7 cameras from widely known and reasonably foreseeable risks of unauthorized access, including  
8 by failing to protect against flaws which the Open Web Application Security Project has ranked  
9 among the most critical and widespread web application vulnerabilities since at least 2007.

10 Among other things:

- 11 a. Defendants repeatedly have failed to take reasonable software testing and  
12 remediation measures to protect their routers and IP cameras against well-  
13 known and easily preventable software security flaws, such as “hard-coded”  
14 user credentials and other backdoors, and command injection flaws, which  
15 would allow remote attackers to gain control of consumers’ devices;
- 16 b. Defendant D-Link has failed to take reasonable steps to maintain the  
17 confidentiality of the private key that Defendant D-Link used to sign  
18 Defendants’ software, including by failing to adequately restrict, monitor, and  
19 oversee handling of the key, resulting in the exposure of the private key on a  
20 public website for approximately six months; and
- 21 c. Defendants have failed to use free software, available since at least 2008, to  
22 secure users’ mobile app login credentials, and instead have stored those  
23 credentials in clear, readable text on a user’s mobile device.

24 **THOUSANDS OF CONSUMERS AT RISK**

25 16. As a result of Defendants’ failures, thousands of Defendants’ routers and  
26 cameras have been vulnerable to attacks that subject consumers’ sensitive personal  
27 information and local networks to a significant risk of unauthorized access. In fact, the press

1 has reported that Defendants' routers and cameras have been vulnerable to a range of such  
2 attacks and have been compromised by attackers, including by being made part of large scale  
3 networks of computers infected by malicious software, known as "botnets."

4 17. The risk that attackers would exploit these vulnerabilities to harm consumers was  
5 significant. In many instances, remote attackers could take simple steps, using widely available  
6 tools, to locate and exploit Defendants' devices, which were widely known to be vulnerable. For  
7 example, remote attackers could search for vulnerable devices over the Internet and obtain their  
8 IP addresses using readily available tools, such as a popular search engine that can locate devices  
9 running particular software versions or operating in particular locations. Alternatively, attackers  
10 could use readily accessible scanning tools to identify vulnerable devices operating in particular  
11 areas or on particular networks. In many instances, an attacker could then take simple steps to  
12 exploit vulnerabilities in Defendants' routers and IP cameras, impacting not only consumers who  
13 purchased these devices, but also other consumers, who access the Internet in public or private  
14 locations served by the routers or who visit locations under the IP cameras' surveillance.

15 18. By creating these vulnerabilities, Defendants put consumers at significant risk of  
16 harm in a variety of ways. An attacker could compromise a consumer's router, thereby obtaining  
17 unauthorized access to consumers' sensitive personal information. For example, using a  
18 compromised router, an attacker could re-direct consumers seeking a legitimate financial site to a  
19 spoofed website, where they would unwittingly provide the attacker with sensitive financial  
20 account information. Alternatively, using a compromised router, an attacker could obtain  
21 consumers' tax returns or other files stored on the router's attached storage device or could use  
22 the router to attack other devices on the local network, such as computers, smartphones, IP  
23 cameras, or connected appliances. Similarly, by exploiting the vulnerabilities described in  
24 Paragraph 15, an attacker could compromise a consumer's IP camera, thereby monitoring  
25 consumers' whereabouts to target them for theft or other criminal activity or to observe and  
26 record over the Internet their personal activities and conversations or those of their young  
27 children. In many instances, attackers could carry out such exploits covertly, such that

1 consumers would have no reason to know that an attack was ongoing. Finally, during the time  
2 Defendant D-Link's private key was available on a public website, consumers seeking to  
3 download legitimate software from Defendants were at significant risk of downloading malware,  
4 signed by malicious actors using D-Link's private key.

#### 5 **DEFENDANTS' SECURITY STATEMENTS**

6 19. Defendants have disseminated or caused to be disseminated to consumers  
7 statements regarding the security of their products, including their routers and IP cameras.

#### 8 **SECURITY EVENT RESPONSE POLICY**

9 20. From approximately December 2013 until early September 2015, after highly-  
10 publicized security flaws were found to affect many of its products, Defendant DLS posted a  
11 Security Event Response Policy on its product support webpage,  
12 <http://support.dlink.com/securityadvisories.aspx>, in the general form of Exhibit 1. Within  
13 its Security Event Response Policy, under a bolded heading "D-Link's commitment to Product  
14 Security," Defendant DLS stated:

15 D-Link prohibits at all times, including during product development by D-Link or its  
16 affiliates, any intentional product features or behaviors which allow unauthorized access  
17 to the device or network, including but not limited to undocumented account  
18 credentials, covert communication channels, 'backdoors' or undocumented traffic  
19 diversion. All such features and behaviors are considered serious and will be given the  
20 highest priority.

#### 21 **PROMOTIONAL CLAIMS**

22 21. Defendants highlight their routers' security features in a wide range of materials  
23 available on Defendant DLS's website, including user manuals and promotional brochures,  
24 which describe these features alongside language that specifically references the device's  
25 "security". Such materials include, but are not limited to, brochures in the general form of  
26 Exhibits 2-5, which state:



1 a. Under a bolded, italicized, all-capitalized heading, “**EASY TO SECURE**,” that  
2 the router:

3 supports the latest wireless security features to help prevent unauthorized  
4 access, be it from over a wireless network or from the Internet. Support for  
5 WPA™ and WPA2™ standards ensure that you will be able to use the best  
6 possible encryption, regardless of your client devices. In addition [the router]  
7 utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from  
8 across the Internet.

9 Delivering great wireless performance, network security and coverage [the  
10 router] is ideal for upgrading your existing wireless network. (See PX 2).

11 b. Under a bolded, italicized, all-capitalized heading, “**ADVANCED NETWORK**  
12 **SECURITY**,” that the router:

13 ensures a secure Wi-Fi network through the use of WPA/WPA2 wireless  
14 encryption. Simply press the WPS button to quickly establish a secure  
15 connection to new devices. The [router] also utilizes dual-active firewalls  
16 (SPI and NAT) to prevent potential attacks and intrusions from across the  
17 Internet. (See PX 3).

18 c. Under a bolded heading, “**Advanced Network Security**,” that the router:

19 supports the latest wireless security features to help prevent unauthorized  
20 access, be it from over a wireless network or from the Internet. Support for  
21 WPA™ and WPA2™ standards ensure that you will be able to use the best  
22 possible encryption method. In addition, this [router] utilizes Stateful Packet  
23 Inspection Firewalls (SPI) to help prevent potential attacks from across the  
24 Internet. (See PX 4).

25 d. Under a heading “128-bit Security Encryption,” that the router:

26 protects your network with 128-bit AES data security encryption – the same  
27 technology used in E-commerce or online banking. Create your own network  
28

1 name and password or put it at the tip of your fingers with ‘Push Button  
2 Security’ standard on every Amplifi device. With hassle-free plug and play  
3 installation, and advanced Wi-Fi protected setup, the [router] is not only one  
4 of the fastest routers available, its [sic] also one of the safest. (See PX 5).

5 22. Defendants highlight the security of their IP cameras in a wide range of  
6 materials available on Defendant DLS’s website, including user manuals and promotional  
7 brochures, which describe these features alongside language that specifically references the  
8 device’s “security”. Such materials include, but are not limited to, brochures in the general  
9 form of Exhibit 6, which display the word “SECURITY” in large, capital letters, in a vividly-  
10 colored footer across the bottom of each page. (See PX 6). In addition, Defendants have  
11 designed their IP camera packaging, including in the general form of Exhibit 7, to display  
12 security-related terms. Such terms include the words “secure connection,” next to a lock icon,  
13 among the product features listed on the side of the box (see PX 7).

#### 14 **INTERACTIVE SECURITY FEATURES**

15 23. Defendants’ routers offer numerous security features that Defendants present  
16 alongside instructions that specifically reference the device’s “security”. In particular, in many  
17 instances, to begin using the router, users must access a graphical user interface (hereinafter,  
18 “Defendants’ router GUI”), in the general form of Exhibits 8 and 9, which includes  
19 instructions, such as:

- 20 a. “To secure your new networking device, please set and verify a password  
21 below” (see PX 8); and  
22 b. “It is highly recommended that you create a password to keep your router  
23 secure.” (See PX 9).

24 24. Defendants’ IP cameras offer numerous security features that Defendants  
25 present alongside language that specifically references the device’s “security”. In particular, to  
26 begin using the camera, in many instances, users must access a GUI (hereinafter “Defendants’  
27 IP camera GUI”), in the general form of Exhibits 10 and 11, which include language, such as:

- 1 a. instructions to “Set up an Admin ID and Password” or “enter a password” in  
2 order “to secure your camera” (*see* PX 10); and
- 3 b. security-related banners, including, but not limited to, the words “SECURICAM  
4 Network,” alongside a lock icon, across the top of the GUI (*see* PX 11).

5 **D-LINK DIRECTS ITS PRACTICES TO U.S. CONSUMERS**

6 25. D-Link controls decisions about which products and features Defendants will  
7 offer to United States consumers. Upon deciding to design and develop a new product for sale in  
8 the United States, D-Link is responsible for writing the “Product Requirements Document,”  
9 which sets forth the functions and features that the product will possess, including any security  
10 features. D-Link also controls decisions about whether to conduct security testing and review of  
11 these products and their related software, before offering them to U.S. consumers. Further, to the  
12 extent that D-Link decides to conduct security review and testing of a product before offering it  
13 to United States consumers, D-Link is responsible for conducting or procuring such review and  
14 testing and for determining whether the results warrant revisions to the product. Once a new  
15 product is launched in the United States, D-Link is responsible for providing ongoing support to  
16 DLS for the product, including by determining whether to remediate any design, usability, and  
17 security issues that are reported in Defendants’ routers and IP cameras. For example, if a  
18 security vulnerability is reported in Defendants’ routers or IP cameras and related software, D-  
19 Link is responsible for determining whether a security update is warranted to address the  
20 vulnerability and, if so, for developing the update. When D-Link develops new products for  
21 United States consumers, DLS may request that D-Link include certain features in the products,  
22 but DLS does not participate in drafting the Product Requirements Documents or in designing  
23 and testing any security features these products may have.

24 **VIOLATIONS OF THE FTC ACT**

25 26. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits “unfair or deceptive acts  
26 or practices in or affecting commerce.”



1 **Router Promotional Misrepresentations**

2 34. Through the means described in Paragraph 21, Defendants have represented,  
3 directly or indirectly, expressly or by implication, that the routers described by these claims were  
4 secure from unauthorized access.

5 35. In truth and in fact, as described in Paragraphs 15-18, Defendants' routers were  
6 not secure from unauthorized access and control.

7 36. Therefore, the making of the representation set forth in Paragraph 34 of this  
8 Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of  
9 Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

10 **COUNT IV**

11 **IP Camera Promotional Misrepresentations**

12 37. Through the means described in Paragraph 22, Defendants have represented,  
13 directly or indirectly, expressly or by implication, that the IP cameras described by these claims  
14 were secure from unauthorized access and control.

15 38. In truth and in fact, as described in Paragraphs 15-18, Defendants' IP cameras  
16 were not secure from unauthorized access and control.

17 39. Therefore, the making of the representation set forth in Paragraph 37 of this  
18 Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of  
19 Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

20 **COUNT V**

21 **Router GUI Misrepresentations**

22 40. Through the means described in Paragraph 23, Defendants have represented,  
23 directly or indirectly, expressly or by implication, that the routers described by these claims were  
24 secure from unauthorized access.

25 41. In truth and in fact, as described in Paragraphs 15-18, Defendants' routers were  
26 not secure from unauthorized access and control.



1           B.       Award Plaintiff the costs of bringing this action, as well as such other and  
2 additional relief as the Court may determine to be just and proper.

3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Respectfully submitted,

DAVID SHONKA  
Acting General Counsel

Dated: January 5, 2017

/s/ Cathlin Tully  
LAURA D. BERGER  
KEVIN H. MORIARTY  
CATHLIN TULLY

Attorneys for Plaintiff  
FEDERAL TRADE COMMISSION

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

IN RE THE HOME DEPOT, INC.  
SHAREHOLDER DERIVATIVE  
LITIGATION

CIVIL ACTION FILE  
NO. 1:15-CV-2999-TWT

**OPINION AND ORDER**

This is a shareholder derivative action. It is before the Court on the Defendants' Motion to Dismiss [Doc. 45]. For the reasons set forth below, the Defendants' Motion to Dismiss [Doc. 45] is GRANTED.

**I. Background**

This case arises out of the breach of Home Depot's security systems and the theft of their customers' personal financial data (the "Breach") over the course of several months in 2014. Plaintiffs Bennek and Frohman are current Home Depot shareholders, and held shares in Home Depot at the time of the Breach.<sup>1</sup> The nominal Defendant, The Home Depot, Inc. ("Home Depot") is a multinational home

---

<sup>1</sup> Compl. ¶¶ 22-23.



improvement retailer that is incorporated in Delaware, with its principal place of business in Georgia.<sup>2</sup>

Included as defendants in the suit are three current and former officers of Home Depot (the “Officers”). Francis Blake was previously Chairman of the Board from January 2007 to February 2015, and served as CEO during that time until November 2014. Matthew Carey is Home Depot’s Executive Vice President and Chief Information Officer (“CIO”). Craig Menear served as President of Home Depot’s retail division from February to October 2014, and was appointed as CEO, President, and placed on the Board on November 1, 2014. On February 2, 2015, Menear was appointed Chairman of the Board.<sup>3</sup>

Also included as defendants are a number of current and former members of Home Depot’s Board of Directors. Home Depot’s Board currently consists of twelve members, nine of whom are named as defendants.<sup>4</sup> One of them is Menear, who is also the Company’s CEO and President.<sup>5</sup> The remaining eight current directors are Defendants Bousbib, Brenneman, Brown, A. Carey, Codina, Foulkes, Katen, and

---

<sup>2</sup> Id. ¶ 24.

<sup>3</sup> Id. ¶¶ 25-27.

<sup>4</sup> Id. ¶ 258.

<sup>5</sup> Id. ¶ 27.

Vadon, all of whom were Directors when the Breach occurred (collectively, the “Outside Directors”).<sup>6</sup> Defendants Hill and Ackerman are former Directors who were on the Board during the Breach (collectively, the “Former Directors”).<sup>7</sup>

On September 2, 2014, Home Depot learned that it may have been the victim of a criminal breach of its payment card data systems.<sup>8</sup> After an investigation, Home Depot confirmed that the Breach had occurred and that hackers had managed to steal the financial data of 56 million customers between April and September of 2014.<sup>9</sup> This followed on the heels of a number of well publicized data breaches that occurred at major retailers like Target and Neiman Marcus the previous year.<sup>10</sup> The hackers used a third-party vendor’s user name and password to enter into Home Depot’s network.<sup>11</sup> The hackers then gained elevated rights which allowed them to access the rest of Home Depot’s network and install a custom version of malware called

---

<sup>6</sup> Id. ¶ 258.

<sup>7</sup> Id. ¶¶ 36-37.

<sup>8</sup> Id. ¶ 214.

<sup>9</sup> Id. ¶ 230.

<sup>10</sup> Id. ¶¶ 75, 77.

<sup>11</sup> Id. ¶ 237.

BlackPOS.<sup>12</sup> A similar version of BlackPOS was used in the Target data breach a few months prior, and essentially allowed the hackers to capture a customer's financial data every time a card was swiped at one of Home Depot's Point of Sale ("POS") terminals (e.g., a cash register).<sup>13</sup> A little over a year after the Breach occurred, Home Depot reported that it had registered a net cost to the Company of \$152 million.<sup>14</sup> After all is said and done, the total cost to Home Depot because of the Breach has been estimated to eventually reach nearly \$10 billion.<sup>15</sup>

In August of 2015, Bennek filed a derivative complaint against Home Depot, and Frohman's derivative case was later consolidated with Bennek's. The Plaintiffs allege that the Defendants breached their duty of loyalty to Home Depot because the Defendants failed to institute internal controls sufficient to oversee the risks that Home Depot faced in the event of a breach and because they disbanded a Board of Directors committee that was supposed to have oversight of those risks.<sup>16</sup> As a result of their alleged failure to take the risk of a data breach seriously and immediately

---

<sup>12</sup> Id.

<sup>13</sup> Id. ¶¶ 76, 219.

<sup>14</sup> Id. ¶ 250.

<sup>15</sup> Id. ¶ 252.

<sup>16</sup> Id. ¶ 6.

implement security measures, the Breach occurred.<sup>17</sup> The Plaintiffs also allege that the Defendants wasted corporate assets, and that the Current Directors violated Section 14(a) of the Securities Exchange Act in their 2014 and 2015 proxy filings.<sup>18</sup>

All of the Plaintiffs' charges against the Defendants ultimately relate to what the Defendants knew before the Breach and what they did about that knowledge. According to the Complaint, Home Depot's by-laws authorized the Board to delegate any or all of its powers to committees to the extent allowed by law.<sup>19</sup> The by-laws provided for no procedure to do this, other than referencing resolutions of the Board.<sup>20</sup> The Company's Governance Guidelines, however, said that the roles of committees are defined "by the Company's by-laws and by Committee charters adopted by the Board."<sup>21</sup> When it came to overseeing the company's information technology (IT) and digital security, Home Depot had previously instituted what was

---

<sup>17</sup> Id. ¶ 264.

<sup>18</sup> Id. ¶¶ 299, 305.

<sup>19</sup> Id. ¶ 170.

<sup>20</sup> Id.

<sup>21</sup> Id. ¶ 171.

called the Infrastructure Committee.<sup>22</sup> The Infrastructure Committee, however, was dissolved by Home Depot in May 2012.<sup>23</sup>

Home Depot said in its 2012 Proxy Statement that the responsibility for IT and data security which had previously been the domain of the Infrastructure Committee was now being borne by the Audit Committee.<sup>24</sup> However, the Audit Committee's charter was never amended to reflect this change.<sup>25</sup> And according to the Complaint, Home Depot's 2014 and 2015 Proxy Statements, which were issued after the Breach had begun, did not include any indication that the Audit Committee's charter had not been changed to reflect its new duties.<sup>26</sup>

In addition to raising the issue of whether anyone had proper oversight over IT and data security, the Complaint also alleges a number of deficiencies in Home Depot's network security as it stood at the time of the Breach. According to the Complaint, Home Depot's contracts with financial institutions required them to comply with the Payment Card Industry Data Security Standards ("PCI DSS"), which

---

<sup>22</sup> Id. ¶ 174.

<sup>23</sup> Id. ¶ 177.

<sup>24</sup> Id. ¶ 178.

<sup>25</sup> Id. ¶ 180.

<sup>26</sup> Id. ¶ 183.

established a minimum level of protection for data security.<sup>27</sup> PCI DSS 2.0, the version of the standards in place at the time of the Breach, required Home Depot to: (1) install and maintain a firewall, (2) protect against malware and regularly update its anti-virus software, (3) encrypt transmission of cardholder data, (4) not store cardholder data beyond the time necessary to authorize a transaction, (5) limit access to payment card data, and (6) to regularly test its data security systems.<sup>28</sup>

On multiple occasions before the Breach, the Board and the Audit Committee were informed by M. Carey that Home Depot was out of compliance with PCI DSS on multiple levels.<sup>29</sup> M. Carey acknowledged that Home Depot was out of compliance, and admitted that Home Depot would likely continue to be out of compliance until February 2015.<sup>30</sup> M. Carey assured the Board that there was a plan in place, and that it was in the process of being implemented.<sup>31</sup> During this time, the Board continued to receive regular updates from M. Carey.<sup>32</sup>

---

<sup>27</sup> Id. ¶ 68.

<sup>28</sup> Id. ¶ 85.

<sup>29</sup> See, e.g., id. ¶¶ 199-210.

<sup>30</sup> Id. ¶ 207.

<sup>31</sup> Id. ¶¶ 207-09, 229, 240, 267.

<sup>32</sup> Id. ¶ 279.

On September 8, 2014, Home Depot acknowledged that there had been a breach of its network.<sup>33</sup> At the time of the Breach, Home Depot's security systems were still "desperately out of date," according to then-CEO, the Defendant Blake.<sup>34</sup> For example, encryption technology had only been installed at twenty-five percent of its stores by the time the Breach was discovered in September 2015.<sup>35</sup> In response, Home Depot accelerated its efforts to increase its security, and was able to install encryption technology on the remaining seventy-five percent of its stores in just six days.<sup>36</sup>

As a result of the harm caused to Home Depot by its delay in responding to threats Home Depot acknowledged as significant, the Plaintiffs filed this derivative suit. The Plaintiffs claim that the Defendants breached their duties of care and loyalty, wasted corporate assets, and violated Section 14(a) of the Securities Exchange Act. The Defendants now move to dismiss the claims against them under Rules 12(b)(6) and 23.1(b)(3) of the Federal Rules of Civil Procedure.

---

<sup>33</sup> Id. ¶ 220.

<sup>34</sup> Id. ¶ 233.

<sup>35</sup> Id. ¶ 124.

<sup>36</sup> Id. ¶ 125.

## II. Legal Standard

A complaint should be dismissed under Rule 12(b)(6) only where it appears that the facts alleged fail to state a “plausible” claim for relief.<sup>37</sup> A complaint may survive a motion to dismiss for failure to state a claim, however, even if it is “improbable” that a plaintiff would be able to prove those facts; even if the possibility of recovery is extremely “remote and unlikely.”<sup>38</sup> In ruling on a motion to dismiss, the court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff.<sup>39</sup> Generally, notice pleading is all that is required for a valid complaint.<sup>40</sup> Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff’s claim and the grounds upon which it rests.<sup>41</sup> However, in a shareholder derivative case, the complaint shall also allege with

---

<sup>37</sup> Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009); Fed. R. Civ. P. 12(b)(6).

<sup>38</sup> Bell Atlantic v. Twombly, 550 U.S. 544, 556 (2007).

<sup>39</sup> See Quality Foods de Centro America, S.A. v. Latin American Agribusiness Dev. Corp., S.A., 711 F.2d 989, 994-95 (11th Cir. 1983); see also Sanjuan v. American Bd. of Psychiatry & Neurology, Inc., 40 F.3d 247, 251 (7th Cir. 1994) (noting that at the pleading stage, the plaintiff “receives the benefit of imagination”).

<sup>40</sup> See Lombard’s, Inc. v. Prince Mfg., Inc., 753 F.2d 974, 975 (11th Cir. 1985), cert. denied, 474 U.S. 1082 (1986).

<sup>41</sup> See Erickson v. Pardus, 551 U.S. 89, 93 (2007) (citing Twombly, 550 U.S. at 555).



particularity the efforts, if any, made by the plaintiff to obtain the action the plaintiff desires from the directors or comparable authority and, if necessary, from the shareholders or members, and the reasons for the plaintiff's failure to obtain the action or for not making the effort.<sup>42</sup>

### III. Discussion

Rule 23.1 clearly “contemplates both the demand requirement and the possibility that demand may be excused...[but] it does not create a demand requirement of any particular dimension.”<sup>43</sup> Because the demand doctrine is a matter of substance, the Court looks to the state of incorporation to provide the rule of decision.<sup>44</sup> In this case, Home Depot is incorporated in Delaware; therefore, the Court looks to Delaware’s substantive law.

“A cardinal precept of the General Corporation Law of the State of Delaware is that directors, rather than shareholders, manage the business and affairs of the corporation.”<sup>45</sup> Shareholder derivative suits restrict this managerial authority. Therefore, as a prerequisite to a shareholder derivative suit, Delaware law requires

---

<sup>42</sup> Fed. R. Civ. P. 23.1(b)(3).

<sup>43</sup> Kamen v. Kemper Fin. Servs., Inc., 500 U.S. 90, 96 (1991).

<sup>44</sup> Id. at 96-97.

<sup>45</sup> Stepak v. Addison, 20 F.3d 398, 402 (11th Cir. 1994) (quoting Aronson v. Lewis, 473 A.2d 805, 811 (Del. 1984)).

an aggrieved shareholder to demand that the board take the desired action.<sup>46</sup> This demand requirement “insure[s] that a stockholder exhausts his intracorporate remedies, and ... provide[s] a safeguard against strike suits.”<sup>47</sup>

It is undisputed that no demand was made in this instance. The Plaintiff shareholder thus has the burden of demonstrating that demand is excused because it would have been futile. In situations like this case where the Plaintiffs complain of Board inaction and do not challenge a specific decision of the Board, a finding of demand futility is authorized only where “*particularized* factual allegations of [the] derivative stockholder complaint create a *reasonable doubt* that, as of the time the complaint is filed, the board of directors could have properly exercised its independent and disinterested business judgment in responding to a demand.”<sup>48</sup> Because the independence of the Board is determined at the time of filing, the Court only need look to the claims against the Current Directors. And further, because the Board acts by will of the majority, the Plaintiffs’ Complaint must show that a majority

---

<sup>46</sup> Id.

<sup>47</sup> Aronson v. Lewis, 473 A.2d 805, 811 (Del. 1984), *overruled on other grounds by* Brehm v. Eisner, 746 A.2d 244 (Del. 2000).

<sup>48</sup> Rales v. Blasband, 634 A.2d 927, 934 (Del. 1993) (emphasis added); accord In re Citigroup Inc. Shareholder Derivative Litigation, 964 A.2d 106, 121 (Del. Ch. 2009).

of the Directors were not independent. As such, the Court only need address the Plaintiffs' claims against the Outside Directors (the Defendants Bousbib, Brenneman, Brown, A. Carey, Codina, Foulkes, Katen, and Vadon), who make up a majority of the Board<sup>49</sup> and are all similarly situated, to determine whether the Board of Directors was independent.

Interest is demonstrated where a director “will receive a personal financial benefit from a transaction that is not equally shared by the stockholders,” or “where a corporate decision will have a materially detrimental impact on a director, but not on the corporation and the stockholders.”<sup>50</sup> Only the former is at issue here.

Initially, it seems obvious that the Board was interested given that a majority of its members are named in this lawsuit. After all, very few people would choose to sue themselves. However, as this Court previously noted, under Delaware law “derivative action plaintiffs do not ring the futility bell merely by including a majority of the directors as defendants.”<sup>51</sup> To do so would eviscerate the demand requirement

---

<sup>49</sup> At the time of filing, the Board consisted of twelve members. Compl. ¶ 258. There are eight non-officer Current Directors, making up a majority of the Board.

<sup>50</sup> Rales, 634 A.2d at 936.

<sup>51</sup> In re Coca-Cola Enterprises, Inc. Derivative Litigation, 478 F. Supp. 2d 1369, 1374 (N.D. Ga. 2007).

entirely. Instead, Delaware law requires the Plaintiffs to show director conduct that is “so egregious on its face that board approval cannot meet the test of business judgment, and a *substantial likelihood* of director liability therefore exists.”<sup>52</sup>

The Plaintiffs plead claims against the Outside Directors for breaches of their duty of loyalty, corporate waste, and violations of Section 14(a) of the Securities Exchange Act. The Defendants argue that the Plaintiffs must plead particularized facts for these claims against each defendant individually. To the Court’s knowledge, Delaware courts have not directly addressed whether “group pleading” is sufficiently particular for demand futility. However, a number of District Courts have, and all of them have at least said that group pleading is not *per se* insufficient.<sup>53</sup> As long as the defendants are “similarly situated,” group pleading may be enough.

Individual and particularized facts for each defendant would be more necessary in cases, for example, where the directors are alleged to be financially interested in

---

<sup>52</sup> Aronson, 473 A.2d at 815 (emphasis added).

<sup>53</sup> See, e.g., In re American Apparel, Inc. S’holder Deriv. Litig., No. CV 10-06576 MMM RCX, 2012 WL 9506072, at \*41 (C.D. Cal. July 31, 2012) (concluding that such “group pleading is [not] per se impermissible [under Delaware law, in the context of derivative litigation], so long as group pleading is limited to defendants who are similarly situated”); In re Chemed Corporation, S’holder Deriv. Litig., No. CV 13-1854-LPS-CJB, 2015 WL 9460118, at \*10-11 (D. Del. Dec. 23, 2015); In re Johnson & Johnson Deriv. Litig., 865 F. Supp. 2d 545, 563 (D.N.J. 2011).

a proposed merger. In those cases, to determine whether a majority of the board of directors were interested would require an individual analysis. But in this case, all of the Plaintiffs' claims against the non-officer Current Directors essentially allege that they are liable because of information they received and decisions they took collectively. There is nothing to be gained by addressing each Outside Director individually because they are all similarly situated. As such, the Court now addresses each of the claims against the Outside Directors and takes them together as a group.

#### **A. Duty of Loyalty Claims**

The Plaintiffs' primary claim for liability is that the Directors breached their duty of loyalty to the company. In cases such as this one, where the Plaintiffs allege a failure of oversight on the part of the Board, the Plaintiffs must show that the Directors either "*knew* they were not discharging their fiduciary obligations or that the directors demonstrated a *conscious* disregard for their responsibilities such as by failing to act in the face of a known duty to act."<sup>54</sup> When added to the general demand futility standard, the Plaintiffs essentially need to show with particularized facts beyond a reasonable doubt that a majority of the Board faced substantial liability because it consciously failed to act in the face of a known duty to act. This is an

---

<sup>54</sup> In re Citigroup, 964 A.2d at 123 (emphasis in original).

incredibly high hurdle for the Plaintiffs to overcome, and it is not surprising that they fail to do so.

The Plaintiffs first attempt to clear this hurdle by pointing to the disbanding of the Infrastructure Committee. According to the Complaint, when the Board disbanded the Infrastructure Committee, it failed to amend the Audit Committee's charter to reflect the new responsibilities for data security that had been transferred from the Infrastructure Committee, as required by the Company's Corporate Governance Guidelines. The Plaintiffs argue, therefore, that the Board failed to designate anyone with the responsibility to oversee data security, thereby leaving them without a reporting system.

This argument is much too formal. Even if the Board's failure to amend the Audit Committee charter meant that it did not have authority to oversee data security, and the Court doubts that is true, it is irrelevant here. Demand futility is a fact based analysis. Whether or not the Audit Committee had technical authority, both the Committee and the Board believed it did. The Complaint itself details numerous instances where the Audit Committee received regular reports from management on the state of Home Depot's data security, and the Board in turn received briefings from both management and the Audit Committee. Based on those facts alone, there can be

no question that the Board was fulfilling its duty of loyalty to ensure that a reasonable system of reporting existed.

The Plaintiffs then argue that the Board “failed to ensure that a plan was in place to *immediately* remedy the deficiency [in Home Depot’s data security], and that the proposed remedy complied with PCI DSS.”<sup>55</sup> Importantly, the Plaintiffs repeatedly acknowledge that there *was* a plan, but that in the Plaintiffs’ opinion it moved too slowly.<sup>56</sup> Under Delaware law, however, directors violate their duty of loyalty only “if they knowingly and *completely* failed to undertake their responsibilities.”<sup>57</sup> In other words, as long as the Outside Directors pursued *any* course of action that was reasonable, they would not have violated their duty of loyalty. The Court suspects that is why the Plaintiffs awkwardly try to reframe their argument to say that the Board “failed to take *any* action to remediate the problems.”<sup>58</sup> But the Plaintiffs cannot escape the facts in their Complaint and their own contradictory arguments. At the end of the day, the Plaintiffs are alleging that the Board’s plan was not good enough.

---

<sup>55</sup> Compl. ¶ 204 (emphasis added).

<sup>56</sup> See, e.g., Compl. ¶¶ 87, 117-18, 200, 203-04.

<sup>57</sup> Lyondell Chemical Co. v. Ryan, 970 A.2d 235, 243-44 (Del. 2009).

<sup>58</sup> Pls.’ Resp. to Defs.’ Mot. to Dismiss, at 23.

The Plaintiffs may be right, but Delaware courts have held that “[b]ad faith cannot be shown by merely showing that the directors failed to do all they should have done under the circumstances.”<sup>59</sup> Rather, they use language like “utterly” and “completely” to describe the failure necessary to violate the duty of loyalty by inaction.<sup>60</sup> The cases cited in the Plaintiffs’ Response to the Defendants’ Motion to Dismiss [Doc. 52] work against their argument on this point. In Abbott Labs., the Seventh Circuit found demand excused where the complaint sufficiently alleged that in the face of numerous known violations of law, the directors “took *no* steps in an effort to prevent or remedy the situation...”<sup>61</sup> In Pfizer, the court held that demand was futile because the directors received numerous warnings of illegal marketing practices, but they “chose to disregard it.”<sup>62</sup> And in Veeco Instruments, the company failed to do *anything* for more than a year to address deficiencies in its accounting

---

<sup>59</sup> Wayne Cty. Employees' Ret. Sys. v. Corti, No. CIV.A. 3534-CC, 2009 WL 2219260, at \*14 (Del. Ch. July 24, 2009), aff'd, 996 A.2d 795 (Del. 2010).

<sup>60</sup> See Lyondell, 970 A.2d at 243-44 (“knowingly and completely failed to undertake their responsibilities,” and “the inquiry should have been whether those directors utterly failed to attempt to obtain the best sale price.”).

<sup>61</sup> In re Abbott Labs. Deriv. S’holders Litig., 325 F.3d 795, 809 (7th Cir. 2003).

<sup>62</sup> In re Pfizer Inc. S’holder Deriv. Litig., 722 F. Supp. 2d 453, 460 (S.D.N.Y. 2010).



department.<sup>63</sup> Though the board acted in that case, the court found demand excused because the board failed to act until *after* the harm had occurred.

But in this case, the Complaint acknowledges that the Board acted before the Breach occurred. The Board approved a plan that would have fixed many of Home Depot's security weaknesses and it would be fully implemented by February 2015. With the benefit of hindsight, one can safely say that the implementation of the plan was probably too slow, and that the plan probably would not have fixed all of the problems Home Depot had with its security. But the "Directors' decisions must be reasonable, not perfect."<sup>64</sup> While the Board probably should have done more, "[s]imply alleging that a board incorrectly exercised its business judgment and made a 'wrong' decision in response to red flags...is not enough to plead bad faith."<sup>65</sup>

Therefore, the Court finds that the Plaintiffs have failed to show beyond a reasonable doubt that a majority of the Board faced substantial liability because it consciously failed to act in the face of a known duty to act. As such, demand is not excused on the basis of the Plaintiffs' duty of loyalty claims.

---

<sup>63</sup> Veeco Instruments, Inc. v. Braun, 434 F. Supp. 2d 267 (S.D.N.Y. 2006).

<sup>64</sup> Lyondell, 970 A.2d at 243.

<sup>65</sup> Melbourne Mun. Firefighters' Pension Trust Fund on Behalf of Qualcomm, Inc. v. Jacobs, C.A. No. 10872-VCMR, 2016 WL 4076369, at \*9 (Del. Ch. Aug. 1, 2016).

## **B. Corporate Waste**

The Plaintiffs also allege that the Board wasted corporate assets. Under Delaware law, corporate waste is “an exchange that is so one sided that no business person of ordinary, sound judgment could conclude that the corporation has received adequate consideration.”<sup>66</sup> Because waste claims entail an action on the part of the Board, they are evaluated under the Aronson test.<sup>67</sup> To show demand futility under Aronson, the Plaintiffs “must provide particularized factual allegations that raise a reasonable doubt that ‘(1) the directors are disinterested and independent [or] (2) the challenged transaction was otherwise the product of a valid exercise of business judgment.’”<sup>68</sup> The Plaintiffs do not challenge the independence of the Board, but rather their allegations fall under the second prong of Aronson.

The Plaintiffs first maintain that the Board’s insufficient reaction to the threat posed by the holes in Home Depot’s data security caused significant losses to the Company, which they claim is a waste of Home Depot’s assets. The problem with the Plaintiffs’ argument is that there is no transaction. Corporate waste claims typically

---

<sup>66</sup> Brehm, 746 A.2d at 263 (quoting In re Walt Disney Co. Derivative Litig., 731 A.2d 342, 362 (Del. Ch. 1998)).

<sup>67</sup> Aronson, 473 A.2d at 805.

<sup>68</sup> In re Citigroup, 964 A.2d at 120 (quoting Brehm, 746 A.2d at 253).

involve situations where there has been an exchange of corporate assets for no corporate purpose or for no consideration; in effect, waste is a gift.<sup>69</sup> The Plaintiffs cite no case law to suggest anything to the contrary.

Rather, the Plaintiffs' claim is fundamentally a challenge to the Directors' exercise of their business judgment. To paraphrase the Delaware Chancery Court, what the Plaintiffs are asking the Court to conclude from the presence of these "red flags" is that the Directors failed to see the extent of Home Depot's security risk and therefore made a "wrong" business decision by allowing Home Depot to be exposed to the threat of a security breach.<sup>70</sup> With hindsight, it is easy to see that the Board's decision to upgrade Home Depot's security at a leisurely pace was an unfortunate one. But this decision falls squarely within the discretion of the Board and is under the protection of the business judgment rule.

Perhaps recognizing that their first claim of corporate waste does not quite fit, the Plaintiffs try to argue for the first time in their Response to the Defendants'

---

<sup>69</sup> See Lewis v. Vogelstein, 699 A.2d 327, 336 (Del. Ch. 1997) ("Most often the claim is associated with a transfer of corporate assets that serves no corporate purpose; or for which no consideration at all is received. Such a transfer is in effect a gift.").

<sup>70</sup> In re Citigroup, 964 A.2d at 130 (not excusing demand where the defendants' exposure to the subprime mortgage market led to significant losses for the company).

Motion to Dismiss [Doc. 52] that the Board also wasted corporate assets through its compensation package to M. Carey.<sup>71</sup> But as this Court has said previously, a “plaintiff cannot amend the complaint by arguments of counsel made in opposition to a motion to dismiss.”<sup>72</sup> On that ground alone this argument should fail, but it also fails on the merits.

A board’s decision on compensation “is entitled to great deference. It is the essence of business judgment for a board to determine if a particular individual warrant[s] large amounts of money, whether in the form of current salary or severance provisions.”<sup>73</sup> That is not to say that a board’s discretion is unlimited, of course; there is an “outer limit,” at which point the compensation is “so disproportionately large as to be unconscionable and constitute waste.”<sup>74</sup> As the Plaintiffs point out, Delaware courts did excuse demand where a company gave \$68 million, as well as an office, an administrative assistant, and a car and driver for up to five years, to its outgoing CEO who was allegedly responsible in part for billions of dollars in losses to the

---

<sup>71</sup> Pls.’ Resp. to Defs.’ Mot. to Dismiss, at 25.

<sup>72</sup> In re Androgel Antitrust Litig. (No. II), 687 F. Supp. 2d 1371, 1381 (N.D. Ga. 2010).

<sup>73</sup> Brehm, 746 A.2d at 263.

<sup>74</sup> Id. at 262 n. 56 (citing Saxe v. Brady, 184 A.2d 602, 610 (Del. Ch. 1962)).

company.<sup>75</sup> But that is certainly the exception to the rule. Much more often, Delaware courts have given significant deference to boards' decisions on executive compensation.<sup>76</sup>

This case is also very different than Citigroup. M. Carey is still an employee of the company, and Home Depot is still receiving substantial consideration through M. Carey's continued employment. By contrast, Citigroup had just given three times the amount of money paid to M. Carey to a former CEO who no longer worked for it. Though the Court understands the Plaintiffs are not happy with M. Carey's performance, the Board is in charge of executive compensation. For these reasons, demand is not excused on the basis of corporate waste.

### **C. Violations of Section 14(a) of the Securities Exchange Act**

The Plaintiffs lastly assert that the Current Director Defendants violated Section 14(a) of the Securities Exchange Act when they issued their 2014 and 2015 Proxy Statements. The Plaintiffs and the Defendants disagree on whether these claims are subject to the demand requirement. The Plaintiffs cite one case, Vides v. Amelio,

---

<sup>75</sup> See In re Citigroup, 964 A.2d at 138.

<sup>76</sup> See, e.g., Espinoza v. Zuckerberg, 124 A.3d 47 (Del. Ch. 2015) (“allegations that compensation is excessive or even lavish, as pleaded here, are insufficient as a matter of law to meet the standard required for a claim of waste.”) (internal citations omitted).

265 F. Supp. 2d 273, 276 (S.D.N.Y. 2003), for the claim that Delaware does not impose a demand requirement for Section 14(a) claims. The Vides court argued that the decision to include or omit information in a proxy statement did not require an exercise in business judgment. But as other courts have noted, while that may be true, directors must still use their business judgment in determining whether to pursue a lawsuit on account of those proxy statements.<sup>77</sup> Because the business judgment rule is the foundation for the demand requirement, most courts have held that Vides was mistaken and that the demand requirement applies equally to Section 14(a) claims, including another court in the Southern District of New York.<sup>78</sup> Though the Eleventh Circuit has not yet weighed in on the issue, this Court similarly finds the Vides court's reasoning to be incorrect, and holds that Section 14(a) claims are subject to the demand requirement.

---

<sup>77</sup> Bader v. Blankfein, No. 07-CV-1130 (SLT)(JMA), 2008 WL 5274442, at \*6 (E.D.N.Y. Dec. 19, 2008) (The Vides court “ignored the fact that directors must still use their business judgment in deciding what course of action to take when alerted to a materially false statement in a corporate proxy statement.”).

<sup>78</sup> See, e.g., St. Clair Shores Gen. Emps' Ret. Sys. v. Eibeler, No. 06 Civ. 688(SWK), 2006 WL 2849783, at \*4-6 (S.D.N.Y. Oct. 4, 2006) (expressly rejecting Vides and holding that Section 14(a) claims are subject to the demand requirement); Washtenaw Cty. Emps. Ret. Sys. v. Wells Real Estate Inv. Trust, Inc., Civil Action No. 1:07-CV-862-CAP, 2008 WL 2302679, at \*15 (N.D. Ga. Mar. 31, 2008); Bader, 2008 WL 5274442, at \*5-7 (collecting cases).

The decision to include or omit statements in a proxy is not a business decision; it is a legal one. Demand futility, therefore, is evaluated under Aronson's first prong, which excuses demand if the complaint provides particularized factual allegations that raise a reasonable doubt that the directors are disinterested and independent.<sup>79</sup> The primary way to show this is to show that a majority of the directors faced a *substantial* likelihood of liability on the underlying claims.<sup>80</sup> However, a "mere threat of personal liability...is insufficient...."<sup>81</sup>

Section 14(a) and Rule 14-A-9 promulgated thereunder require that proxy statements not be false or misleading with regard to any material statement, nor omit to state any material fact necessary in order to make the statements therein not false or misleading.<sup>82</sup> A fact or statement is material if "there is a substantial likelihood that a reasonable shareholder would consider it important in deciding how to vote."<sup>83</sup> The Plaintiffs do not allege that the Defendants made any false or misleading statements, only that the Defendants omitted important information. As such, the Plaintiffs must

---

<sup>79</sup> Brehm, 746 A.2d at 253 (quoting Aronson, 473 A.2d at 814).

<sup>80</sup> Aronson, 473 A.2d at 815.

<sup>81</sup> Id.

<sup>82</sup> See 17 C.F.R. § 240.14-A-9; 15 U.S.C. § 78n(a)

<sup>83</sup> Virginia Bankshares, Inc. v. Sandberg, 501 U.S. 1083, 1084 (1991).

show that the Board had a duty to disclose the omitted material fact, which is determined by whether “the SEC regulations specifically require disclosure of the omitted information in a proxy statement, or the omission makes other statements in the proxy statement materially false or misleading.”<sup>84</sup>

Claims under Section 14(a) are also subject to the heightened pleading requirements of the Private Securities Litigation Reform Act (the “PSLRA”). The Plaintiffs argue that the PSLRA only applies when there are allegations of fraud, based solely on Washtenaw Cty. Emps. Ret. Sys. v. Wells Real Estate Inv. Trust, Inc., Civil Action No. 1:07-CV-862-CAP, 2008 WL 2302679, at \*10 (N.D. Ga. March 31, 2008). The Supreme Court, however, has stated that the PSLRA “impose[s] heightened pleading requirements and a loss causation requirement upon ‘any private action’ arising from the Securities Exchange Act.”<sup>85</sup> Though it is true that the subsection title for the PSLRA is labeled as “Requirements for securities fraud actions,” that does not mean that the Act requires fraudulent intention to apply.<sup>86</sup> Section (b)(1) states that the PSLRA applies in “*any* private action arising under this

---

<sup>84</sup> Resnik v. Swartz, 303 F.3d 147, 151 (2d Cir. 2002)

<sup>85</sup> Stoneridge Inv. Partners, LLC v. Scientific-Atlanta, 552 U.S. 148, 165 (2008).

<sup>86</sup> See 15 U.S.C. § 78u-4(b)(1).



chapter...”<sup>87</sup> “Chapter” refers back to the 15 U.S.C. Ch. 2B, which is the code location for the Securities Exchange Act. Since Section 14(a) falls under this chapter in the Code, it is clear that the heightened pleading requirements of the PSLRA do apply to Section 14(a) claims.

When taken together, Section 14(a), Rule 14-A-9 and the PSLRA require the Plaintiffs to specify with particularity: (1) omissions in the Proxy Statements that made other statements either false or misleading, (2) how those omissions were material, (3) each statement in the Proxy Statements that was made false or misleading, (4) the reason or reasons why the statement is misleading, and (5) how the omission caused the loss complained of.

The Plaintiffs allege that the Defendants failed to disclose in their 2014 Proxy Statement that Home Depot had known, specific threats to its data security, and that neither the 2014 nor the 2015 Proxy Statements disclosed that the Audit Committee’s charter was not amended. As to the latter claim, the Court has already stated that this argument is much too formal. Regardless of whether the charter was amended, everyone believed and acted as if the Committee did have oversight over data security during the relative time period. So the fact that the Board did not disclose that the charter had not been amended could not possibly be material.

---

<sup>87</sup> Id. (emphasis added).

As for the alleged omission regarding data security threats, the Plaintiffs also fail to sufficiently plead their claims on a number of fronts. They first fail to specifically identify which statements in the 2014 Proxy Statement were rendered false or misleading as a result of the omission. As the Court discussed above, for a Section 14(a) claim to be successful, directors must have had a duty to disclose the omitted information. “Disclosure of an item of information is not required...simply because it may be relevant or of interest to a reasonable investor.”<sup>88</sup> By not showing specific statements in the proxy that were rendered misleading or false, the Plaintiffs have failed to demonstrate a duty on the part of the Board to disclose the information, as well as failing to satisfy the requirements of the PSLRA.

On that reason alone, the Court could dismiss the Section 14(a) claim. But the Plaintiffs also fail to plead with particularity how the omissions caused the loss complained of. In order to succeed under Section 14(a), the Plaintiffs must show “that the proxy solicitation itself, rather than the particular defect in the solicitation materials, was an essential link in the accomplishment of the transaction.”<sup>89</sup> The Eleventh Circuit has said that Section 14(a) claims must show two types of causation:

---

<sup>88</sup> Resnik v. Swartz, 303 F.3d 147, 151 (2d Cir. 2002).

<sup>89</sup> Edward J. Goodman Life Income Trust v. Jabil Circuit, Inc., 594 F.3d 783, 796 (11th Cir. 2010) (citing Mills v. Elec. Auto-Lite Co., 396 U.S. 375, 385 (1970)).

transaction and loss causation.<sup>90</sup> In other words, the shareholders must have voted for the 2014 Proxy Statement because of the omission (i.e., transaction causation), and the losses to the company must have resulted directly from the 2014 Proxy Statement vote, not from the omission itself (i.e., loss causation).<sup>91</sup>

Assuming for the sake of argument that the Plaintiffs' allegations of materiality are sufficient to show transaction causation, the Plaintiffs still fail to show loss causation. The Plaintiffs make no statement showing that the security breaches to the company would not have occurred but for the Defendants being reelected to the Board. In fact, the Plaintiffs acknowledge in the Complaint that "[b]y the time the 2014 Proxy Statement was issued...the 2014 Data Breach had likely begun."<sup>92</sup> Regardless of the election, the Breach had already started.

Courts have also regularly dismissed Section 14(a) claims based on the election of directors because the losses are indirect. The Eleventh Circuit, in a case in which corporate insiders made misrepresentations about compensation policy, dismissed the plaintiffs' claim because "damages suffered by the shareholders were caused not by

---

<sup>90</sup> Id. at 796-97.

<sup>91</sup> Id. at 796 ("The transaction at issue must be the source of the plaintiff's injury.").

<sup>92</sup> Compl. ¶ 183.

the policies that they approved via proxy, but by management's failure to follow those policies.”<sup>93</sup> In making its decision, the Eleventh Circuit looked to a Third Circuit case, in which a shareholder claimed he would not have voted for the reelection of the directors if they would have disclosed information about criminal activity and mismanagement at the company.<sup>94</sup> The Third Circuit dismissed the shareholder complaint because, again, the election of the directors did not cause the harm.<sup>95</sup> Nothing is different about this case. The election of directors based on the 2014 Proxy Statement did not cause the harm alleged; rather, the insufficient urgency of the Board to correct the holes in Home Depot’s security did.

The Plaintiffs have failed to specify which statements in the 2014 or 2015 Proxy Statements were rendered misleading or false by the omissions, have failed to show the materiality of the Audit Committee omission, and have failed to show causation. The claim is insufficiently pleaded under the PSLRA, and does not demonstrate the necessary duty to disclose required under Section 14(a). As a result, the Plaintiffs have not shown beyond a reasonable doubt that the Defendants would have been interested in the litigation because they have not demonstrated a substantial

---

<sup>93</sup> Jabil, 594 F.3d at 797.

<sup>94</sup> General Electric Co. v. Cathcart, 980 F.2d 927 (3d Cir.1992).

<sup>95</sup> Id. at 933.

likelihood that the Defendants would have been liable for a Section 14(a) violation. The Court therefore finds that demand was not futile for the Section 14(a) claims.

#### **IV. Conclusion**

For the foregoing reasons, the Plaintiffs have failed to show that demand was futile on any of the claims alleged. Because the pleading requirements of Rule 23.1 are more demanding than those under 12(b)(6), the Court need not address the Defendants' 12(b)(6) argument. The Defendants' Motion to Dismiss [Doc. 45] is GRANTED.

SO ORDERED, this 30 day of November, 2016.

/s/Thomas W. Thrash  
THOMAS W. THRASH, JR.  
United States District Judge

## Press Release

---

# SEC: Morgan Stanley Failed to Safeguard Customer Data

### FOR IMMEDIATE RELEASE

2016-112

Washington D.C., June 8, 2016— The Securities and Exchange Commission today announced that Morgan Stanley Smith Barney LLC has agreed to pay a \$1 million penalty to settle charges related to its failures to protect customer information, some of which was hacked and offered for sale online.

The SEC issued an order finding that Morgan Stanley failed to adopt written policies and procedures reasonably designed to protect customer data. As a result of these failures, from 2011 to 2014, a then-employee impermissibly accessed and transferred the data regarding approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties.

“Given the dangers and impact of cyber breaches, data security is a critically important aspect of investor protection. We expect SEC registrants of all sizes to have policies and procedures that are reasonably designed to protect customer information,” said Andrew Ceresney, Director of the SEC Enforcement Division.

According to the SEC’s order instituting a settled administrative proceeding:

- The federal securities laws require registered broker-dealers and investment advisers to adopt written policies and procedures reasonably designed to protect customer records and information.
- Morgan Stanley’s policies and procedures were not reasonable, however, for two internal web applications or “portals” that allowed its employees to access customers’ confidential account information.
- For these portals, Morgan Stanley did not have effective authorization modules for more than 10 years to restrict employees’ access to customer data based on each employee’s legitimate business need.
- Morgan Stanley also did not audit or test the relevant authorization modules, nor did it monitor or analyze employees’ access to and use of the portals.
- Consequently, then-employee Galen J. Marsh downloaded and transferred confidential data to his personal server at home between 2011 and 2014.
- A likely third-party hack of Marsh’s personal server resulted in portions of the confidential data being posted on the Internet with offers to sell larger quantities.

The SEC’s order finds that Morgan Stanley violated Rule 30(a) of Regulation S-P, also known as the “Safeguards Rule.” Morgan Stanley agreed to settle the charges without admitting or denying the findings. In a separate order, Marsh agreed to an industry and penny stock bar with the right to apply for reentry after five years. He was criminally convicted for his actions last year and received 36 months of probation and a \$600,000 restitution order.

The SEC’s investigation was conducted by William Martin and Simona Suh of the Enforcement Division’s Market Abuse Unit and supervised by Joseph G. Sansone, Co-Chief of the unit. The SEC appreciates the assistance of the New York Field Office of the Federal Bureau of Investigation and the U.S. Attorney’s Office for the Southern

District of New York.

###

## Related Materials

---

- [SEC order - Morgan Stanley](#)
- [SEC order - Marsh](#)

**UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA**

---

MARY DAVIS, MAUREEN COLLIER,  
and THE POLICE RETIREMENT  
SYSTEMS OF ST. LOUIS, Derivatively  
on behalf of TARGET CORPORATION,

Plaintiff,

v.

GREGG W. STEINHAFEL, BETH M.  
JACOB, JAMES A. JOHNSON, JOHN  
MULLIGAN, ANNE M. MULCAHY,  
ROXANNE S. AUSTIN, CALVIN  
DARDEN, MARY E. MINNICK,  
DERICA W. RICE, JOHN G. STUMPF,  
DOUGLAS M. BAKER, JR., HENRIQUE  
DE CASTRO, KENNETH L. SALAZAR,  
and SOLOMON D. TRUJILLO,

Defendants,

- and-

TARGET CORPORATION, a Minnesota  
corporation,

Nominal Defendant.

Civil Action No. 14-cv-00203  
(PAM-JJK)

---

**Memorandum of Law of the Special Litigation Committee of  
the Board of Directors of Target Corporation in Support of its  
Motion for Approval and Dismissal**



## Questions Presented

On March 30, 2016, the Special Litigation Committee (SLC) of Target Corporation's Board of Directors issued its Report addressing the derivative claims arising out of the December 2013 data breach. As a result of its 21-month investigation, the SLC decided that it was not in Target's best interests to pursue derivative claims arising out of the 2013 data breach against the named officers and directors.

Under Minnesota law, federal courts defer to a corporation's special litigation committee decision to dismiss a derivative action if the SLC demonstrates (1) that it possessed a disinterested independence and (2) that it conducted a good faith investigation into the derivative allegations.

Accordingly, the SLC has moved to dismiss the consolidated derivative action here. In order to decide whether to defer to the SLC's decision and grant its motion to dismiss—a motion supported by the SLC's 91-page report and the affidavits of the two SLC members—the Court need answer only two questions:

1. An SLC demonstrates disinterested independence if it was sufficiently independent to base its decision on the merits. Here, Chief Justice Kathleen Blatz (ret.) and Professor John Matheson were not Target board members before being appointed and will not be board members after their work is done. Neither has personal or professional ties to Target or any defendant; they hired their own counsel and experts; and they designed and conducted the investigation. Did the SLC possess disinterested independence?
2. An SLC demonstrates a good faith investigation not by its outcome, but rather by its investigative methodology and procedures. Here, the SLC retained independent counsel and experts, interviewed 68 witnesses, reviewed and analyzed thousands of documents, met frequently, and considered myriad factors bearing on Target's best interests in deciding whether to pursue claims against the officers and directors for the data breach. Did the SLC conduct a good faith investigation?

If the answer to these two questions is yes, the Court should fulfill the Minnesota legislature's intent of placing the decision of whether or not to pursue derivative litigation back into the hands of the rightful owner—the corporation—and should defer to the SLC's determination and grant its motion to dismiss the consolidated derivative complaint.

### **Factual Background<sup>1</sup>**

In the three week period between November 27 and December 18, 2013, Target Corporation experienced a data breach in which a hacker stole the payment card data of up to 40 million of its customers and stole personally identifiable information—specifically names, residence addresses, phone numbers, and/or email addresses—of up to 70 million of its customers. The announcement of the breach led to widespread media attention, negatively affected Target's sales, and had an immediate and detrimental effect on Target's reputation with consumers. As a result, congressional committees sought testimony and information from Target, regulatory agencies began investigations, and private litigants initiated claims.

### **Procedural history**

Among those private litigants were six Target shareholders. One made a derivative demand on Target's Board of Directors that it investigate and bring actions against the Board members and the company's CEO, CFO, and CIO (the "Demand").

---

<sup>1</sup> The factual background set forth here closely tracks the Report of the Special Litigation Committee at p. 1 and pp. 28–45. The Report is attached to the Affidavit of Kathleen A. Blatz ("Blatz Aff.") at Exhibit B.

The others sued the Board members and officers in five derivative actions. One of those actions was brought in Hennepin County District Court for the State of Minnesota. That case was stayed pending resolution of this derivative action.<sup>2</sup> The other four were brought in the United States District Court for the District of Minnesota and were ultimately consolidated into this action.<sup>3</sup>

The crux of the claims made here is twofold: The derivative shareholders claim that Target's officers and directors (1) failed to properly provide for and oversee an information security program and (2) failed to give customers prompt and accurate information in disclosing the breach.<sup>4</sup> The claimed failures by the Board and officers, it is alleged, were the result of the officers' and directors' conscious disregard of their duties and constituted breach of their fiduciary duties to Target.<sup>5</sup> Derivative plaintiffs' complaint identified a variety of damages, including damage to Target's reputation, damage to Target's bottom line from decreased traffic, and expenses incurred in connection with the breach, and it sought remedies on Target's behalf, including money damages from the defendants and corporate governance changes.<sup>6</sup>

On June 11, 2014, in response to the Demand—which was made after this suit was filed—and in accordance with Minn. Stat. § 302A.241, Subd. 1, Target's Board of

---

<sup>2</sup> *Koeneke v. Austin et al.*, No. 27-cv-14-1832, Stipulation & Order Staying Action, May 21, 2014.

<sup>3</sup> *Davis et al. v. Steinhafel et al.*, No. 14-203, Consolidation Order, Apr. 14, 2014, Docket No. 34.

<sup>4</sup> *See generally Davis et al. v. Steinhafel et al.*, No. 14-203, Verified Consolidated Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets, July 18, 2014, Docket No. 48.

<sup>5</sup> *See id.*

<sup>6</sup> *Id.*

Directors established the SLC;<sup>7</sup> and by resolution adopted on July 24, 2014, Target's Board expanded the SLC's charge to include all the derivative suits.<sup>8</sup> The resolutions vested the SLC with complete power and authority to investigate the allegations, claims, and requests for relief; to determine whether and/or to what extent Target should pursue whatever rights and remedies it has relating to such allegations, claims, and requests for relief; and to respond to the litigation on behalf of the Board and the Company. After the Board formed the SLC, the Court granted a joint agreed motion by the parties to stay the case pending the SLC's decision,<sup>9</sup> and the case remained stayed until April.<sup>10</sup>

### **The SLC's members and their independence**

Both members of the SLC are disinterested and independent.<sup>11</sup> Neither member of the SLC had ever served on Target's Board of Directors, been employed by Target, or otherwise represented Target.<sup>12</sup> They will not remain Target Board members once their duties as the SLC are completed.<sup>13</sup> As members of the Special Litigation Committee of the Board, they do not attend regular meetings and have no duties with respect to the operation of the business.<sup>14</sup> The members of the SLC are solely tasked with executing the duties set forth in the resolutions, which are investigating the claims, determining the

---

<sup>7</sup> Copies of the Board Resolutions are attached to the Affidavit of Kathleen A. Blatz at Ex. A.

<sup>8</sup> Blatz Aff. Ex. A.

<sup>9</sup> *Davis et al. v. Steinhafel et al.*, No. 14-203, Order, June 23, 2014, Docket No. 45.

<sup>10</sup> *Davis et al. v. Steinhafel et al.*, No. 14-203, Fifth Joint Report to the Court, Jan. 29, 2016, Docket No. 55.

<sup>11</sup> Blatz Aff. ¶ 5; Affidavit of John H. Matheson ("Matheson Aff.") ¶ 5.

<sup>12</sup> Blatz Aff. ¶ 5; Matheson Aff. ¶ 5.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

best interests of Target with respect to the Demand and derivative litigation, and responding on behalf of Target.<sup>15</sup> Their compensation for their work on the SLC is not based on their decision but is based solely on their normal hourly rates.<sup>16</sup> Neither member has any material personal, professional, familial, or financial ties with Target or with any of the officers or directors named in the derivative actions or the Demand.<sup>17</sup>

After having served as a District Judge in Minnesota's Fourth Judicial District beginning in 1994, the Honorable Kathleen A. Blatz was appointed to the Minnesota Supreme Court in 1996 and was appointed Chief Justice in 1998.<sup>18</sup> She served in that capacity until her retirement on January 10, 2006.<sup>19</sup>

Chief Justice Blatz received a bachelor's degree from the University of Notre Dame, *summa cum laude*, Phi Beta Kappa.<sup>20</sup> She received her Master of Social Work degree and her Juris Doctor degree, *cum laude*, from the University of Minnesota.<sup>21</sup>

Prior to being appointed a judge, Chief Justice Blatz served in the Minnesota House of Representatives.<sup>22</sup> In 1978, she was elected to the first of eight terms.<sup>23</sup> During her legislative tenure, she served on various committees, including the Tax, Financial Institutions and Insurance, and Judiciary Committees.<sup>24</sup> At the legislature, Chief Justice

---

<sup>15</sup> Blatz Aff. Ex. A.

<sup>16</sup> Blatz Aff. ¶ 6; Matheson Aff. ¶ 6.

<sup>17</sup> Blatz Aff. ¶ 5; Matheson Aff. ¶ 5.

<sup>18</sup> Blatz Aff. ¶ 7–8.

<sup>19</sup> Blatz Aff. ¶ 7.

<sup>20</sup> Blatz Aff. ¶ 14.

<sup>21</sup> *Id.*

<sup>22</sup> Blatz Aff. ¶ 9.

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

Blatz held several leadership positions, including that of Assistant Minority Leader and Chair of the Crime and Family Law Committee.<sup>25</sup> During her legislative career, she also practiced law at Popham, Haik, Schnobrich & Kaufman Ltd. and later served as an Assistant Hennepin County Attorney.<sup>26</sup>

Currently, Chief Justice Blatz is an attorney principally engaged as an arbitrator in commercial disputes.<sup>27</sup> She is a qualified arbitrator for the American Arbitration Association and is on the roster of arbitrators selected for large, complex commercial disputes.<sup>28</sup> She has also served on numerous boards, including as a director on the Columbia Funds Board, where she chairs the Governance Committee, and as a director/trustee on the Blue Cross Blue Shield of Minnesota/Aware Integrated, Inc. Board, where she chairs the Business Development Committee.<sup>29</sup>

Chief Justice Blatz also served on a special litigation committee for the Board of Directors of UnitedHealth Group Inc.<sup>30</sup> That SLC was charged with investigating shareholder derivative claims involving, among other claims, breaches of fiduciary duties by its officers and directors.<sup>31</sup>

John H. Matheson is the Law Alumni Distinguished Professor of Law and Director of the Corporate Institute at the University of Minnesota Law School.<sup>32</sup> He is an

---

<sup>25</sup> Blatz Aff. ¶ 10.

<sup>26</sup> Blatz Aff. ¶ 11.

<sup>27</sup> Blatz Aff. ¶ 12.

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*

<sup>30</sup> Blatz Aff. ¶ 13.

<sup>31</sup> *Id.*

<sup>32</sup> Matheson Aff. ¶ 7.

internationally recognized expert in the area of corporate and business law and has taught in China, Germany, Ireland, England, the Netherlands, Uruguay, and Lithuania.<sup>33</sup> He teaches courses in the business law area, including business associations/corporations, contracts, advanced corporate law, and comparative corporate governance.<sup>34</sup>

Professor Matheson received a bachelor's degree from Illinois State University with high honors.<sup>35</sup> He received his J.D., *cum laude*, from Northwestern University School of Law, where he was Editor-in-Chief of the Northwestern University Law Review.<sup>36</sup> After completing his J.D., he clerked for Judge Robert A. Sprecher of the United States Court of Appeals for the Seventh Circuit.<sup>37</sup> After his clerkship, Professor Matheson joined Hedlund, Hunter & Lynch (now Latham & Watkins) in Chicago.<sup>38</sup> In 1982, he joined the University of Minnesota Law School faculty.<sup>39</sup> Professor Matheson is also a practicing lawyer.<sup>40</sup> He is Of Counsel to Kaplan, Strangis and Kaplan, P.A., specializing in corporate governance counseling, fiduciary duties, mergers and acquisitions, and securities law matters.<sup>41</sup> He is a member of the American Law Institute.<sup>42</sup>

---

<sup>33</sup> *Id.*

<sup>34</sup> *Id.*

<sup>35</sup> Matheson Aff. ¶ 8.

<sup>36</sup> *Id.*

<sup>37</sup> Matheson Aff. ¶ 9.

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*

<sup>40</sup> Matheson Aff. ¶ 10.

<sup>41</sup> *Id.*

<sup>42</sup> *Id.*

Professor Matheson is a five-time recipient of the school's annual Professor of the Year Award for Excellence in Teaching and Counseling.<sup>43</sup> In 2008, Professor Matheson received the University-wide Award for Outstanding Contributions to Postbaccalaureate, Graduate, and Professional Education and was inducted into the Academy of Distinguished Teachers.<sup>44</sup> He is the first professor of the Law School to be so honored by the University.<sup>45</sup>

Professor Matheson's several books and numerous journal articles predominantly address business and corporate law issues.<sup>46</sup> He recently published the third edition of his treatise on Minnesota Corporate Law, *Corporation Law and Practice*.<sup>47</sup> One of Professor Matheson's co-authored articles, "Challenging Delaware's Desirability as a Haven for Incorporation," received the 2007 National Burton Award for Legal Excellence.<sup>48</sup>

Professor Matheson also served as the reporter for the 2006, 2008, 2010, and 2014 amendments to the Minnesota Business Corporation Act.<sup>49</sup> Although the Reporter's

---

<sup>43</sup> Matheson Aff. ¶ 11.

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

<sup>46</sup> Matheson Aff. ¶ 12.

<sup>47</sup> *Id.*

<sup>48</sup> *Id.*; see Philip S. Garon et al., *Challenging Delaware's Desirability as a Haven for Incorporation*, 32 Wm. Mitchell L. Rev. 769 (2006).

<sup>49</sup> Matheson Aff. ¶ 13.



Notes do not have the effect of law, Minnesota courts often give them substantial consideration in statutory interpretation.<sup>50</sup>

Professor Matheson has also served as the chair of a special litigation committee for Medtronic, Inc.<sup>51</sup> That special litigation committee was tasked with investigating shareholder derivative claims involving, among other things, alleged director and officer breaches of fiduciary duties.<sup>52</sup>

### **Overview of the SLC's investigative methodology**

Over a period of twenty-one months, the SLC conducted an investigation into the circumstances surrounding Target's data breach and evaluated the claims made in the Demand and derivative complaints.<sup>53</sup> Its aim was to conduct its investigation in accordance with the fundamental principles of independence and good faith.<sup>54</sup> During its investigation, with the assistance of independent counsel, it searched databases containing hundreds of thousands of documents, reviewed thousands of documents, interviewed 68 witnesses (five of them twice), received information and opinions from independent experts it hired, considered the applicable law, and deliberated. The SLC examined the roles of current and former officers, directors, employees, and third-party consultants in Target's data security program.<sup>55</sup> In evaluating the claims detailed in the

---

<sup>50</sup> See generally *Niccum v. Hydra Tool Corp.*, 438 N.W.2d 96, 99 (Minn. 1989) (considering Reporter's Notes to determine intent of legislature); *Whetstone v. Hossfeld Mfg. Co.*, 457 N.W.2d 380, 383 (Minn. 1990) (same).

<sup>51</sup> Matheson Aff. ¶ 14.

<sup>52</sup> *Id.*

<sup>53</sup> Blatz Aff. ¶ 20; Matheson Aff. ¶ 20.

<sup>54</sup> Blatz Aff. ¶ 21; Matheson Aff. ¶ 21.

<sup>55</sup> Blatz Aff. ¶ 20; Matheson Aff. ¶ 20.

Demand and derivative complaints, it focused on discovering reliable, truthful, and reasonably complete information about all the relevant issues and all aspects of the underlying claims.<sup>56</sup> It considered the evidence collected and evaluated the credibility of the people it interviewed.<sup>57</sup> In its deliberations, the SLC considered whether valid legal claims exist; it also undertook a comprehensive weighing and balancing of the legal, ethical, commercial, professional, public relations, fiscal, and other factors common to reasoned business decisions in deciding whether it would be in Target's best interests to pursue claims against the officers and directors named in the Demand and derivative complaints. A nonexclusive list of the factors the SLC considered is included in its report.<sup>58</sup>

#### **Retention of counsel and experts<sup>59</sup>**

In July 2014, the SLC retained Gaskins Bennett Birrell Schupp, LLP as its independent counsel to provide legal advice and to assist the SLC with all phases of its work, including document collection and review, planning and administration of the SLC's investigation, preparation for and participation in witness interviews, and selection and retention of experts.<sup>60</sup> Counsel has never represented Target or any of the individual defendants.<sup>61</sup> Counsel provided legal guidance concerning the available methods to

---

<sup>56</sup> Blatz Aff. ¶ 21; Matheson Aff. ¶ 21.

<sup>57</sup> Blatz Aff. ¶ 31; Matheson Aff. ¶ 31.

<sup>58</sup> Blatz Aff. Ex. B, pp. 87–90.

<sup>59</sup> Although the retention of counsel and experts is a factor bearing on both the SLC's disinterested independence and its good faith methodology, to avoid redundancy, it is only discussed in this section.

<sup>60</sup> Blatz Aff. ¶ 15; Matheson Aff. ¶ 15.

<sup>61</sup> *Id.*

resolve the claims against defendants in the derivative actions and putative defendants identified in the Demand, advised the SLC on the applicable legal standard and the law governing derivative claims, and assisted in the preparation of the SLC's final report.<sup>62</sup> The SLC relied on the assistance and advice of its counsel throughout its investigation.<sup>63</sup>

The SLC also retained two experts and relied on their expertise in the investigation.<sup>64</sup> The SLC retained Evan Francen, co-founder and President of FRSecure LLC, a full-service information security company, to provide consulting services on the technical aspects of the data breach.<sup>65</sup> William McCracken, a member of the National Association of Corporate Directors Board of Directors, was also retained to consult on issues of corporate governance related to data security.<sup>66</sup>

#### **Documents utilized during the investigation**

Throughout the course of its investigation, the SLC, with assistance from counsel, reviewed and analyzed thousands of documents, including electronically stored information.<sup>67</sup> The documents can be categorized into five groups. First, throughout the investigation, the SLC propounded its own written information requests and document requests to Target, and Target provided written answers and produced over 55,000 documents in response to those specific requests.<sup>68</sup> Second, the SLC requested relevant

---

<sup>62</sup> Blatz Aff. ¶ 16; Matheson Aff. ¶ 16.

<sup>63</sup> *Id.*

<sup>64</sup> Blatz Aff. ¶ 17; Matheson Aff. ¶ 17.

<sup>65</sup> Blatz Aff. ¶ 18; Matheson Aff. ¶ 18.

<sup>66</sup> Blatz Aff. ¶ 19; Matheson Aff. ¶ 19.

<sup>67</sup> Blatz Aff. ¶ 23; Matheson Aff. ¶ 23.

<sup>68</sup> *Id.*

documents from all of the director-defendants.<sup>69</sup> In response, they collectively produced approximately 1,300 documents.<sup>70</sup> Third, the SLC had complete, unrestricted access to the database of approximately 465,000 documents produced in the Target MDL and maintained by Target's outside counsel.<sup>71</sup> Fourth, the SLC requested and received the transcripts of all depositions taken in the Target MDL.<sup>72</sup> Coordinating Lead Counsel over the MDL and Lead Counsel for the financial institution plaintiffs made deposition transcripts available to the SLC, as did counsel for Target.<sup>73</sup> Finally, the SLC and counsel reviewed many documents available through public sources.<sup>74</sup> Throughout its investigation, the SLC, in its role as a duly constituted Committee of the Board established to evaluate claims the company might have against its officers and directors, asked for and received access to documents that included attorney-client privileged and other confidential information with the understanding that it would, absent intentional waiver, maintain their confidentiality.<sup>75</sup>

At the SLC's request and under its supervision, counsel for the SLC performed comprehensive searches of all the available documents, reviewed and analyzed documents retrieved, reported on their findings, and provided thousands of pages of

---

<sup>69</sup> Blatz Aff. ¶ 24; Matheson Aff. ¶ 24.

<sup>70</sup> *Id.*

<sup>71</sup> Blatz Aff. ¶ 25; Matheson Aff. ¶ 25.

<sup>72</sup> *Id.*

<sup>73</sup> *Id.*

<sup>74</sup> Blatz Aff. ¶ 26; Matheson Aff. ¶ 26.

<sup>75</sup> Blatz Aff. ¶ 27; Matheson Aff. ¶ 27.

relevant materials for further review by the SLC.<sup>76</sup> Document review and analysis by the SLC and its counsel continued throughout the investigation.<sup>77</sup>

The SLC and its counsel also accessed and analyzed Target's financial reports and disclosures through the SEC's EDGAR database, including Target's form 10-Ks, form 10-Qs, its annual definitive proxy statements along with definitive additional materials when available, and various 8-Ks during the relevant period.<sup>78</sup> The SLC and its counsel also accessed and analyzed pleadings, decisions, and other papers in the related cases and investigations, and reviewed the legal holds issued to Target employees and directors.<sup>79</sup> Counsel accessed, read, and analyzed various information-security-related articles and articles concerning corporate-risk governance, including information-security-risk governance in particular, and discussed these topics with the SLC and its experts.<sup>80</sup> The SLC members themselves conducted research on pertinent topics, such as the corporate governance of information security risk.<sup>81</sup>

### **Interviews**

The SLC, with counsel, conducted 73 interviews of 68 individuals.<sup>82</sup> These interviews were a key part of the SLC's investigative process as they helped the SLC corroborate and contextualize the documentary information it had gathered, evaluate the significance of data, gain an understanding of Target's corporate culture—especially as it

---

<sup>76</sup> Blatz Aff. ¶ 28; Matheson Aff. ¶ 28.

<sup>77</sup> Blatz Aff. ¶ 30; Matheson Aff. 30.

<sup>78</sup> Blatz Aff. ¶ 29; Matheson Aff. ¶ 29.

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

<sup>81</sup> *Id.*

<sup>82</sup> Blatz Aff. ¶ 34; Matheson Aff. ¶ 34.

related to data security—assess employees’ morale, understand employees’ attitudes towards Target’s data security policies and processes, and determine how those policies and procedures were implemented throughout the company.<sup>83</sup> The SLC members actively participated in all these interviews.<sup>84</sup> Most of the interviews were conducted in-person, with three having been conducted via videoconference.<sup>85</sup> The SLC members traveled to Washington, D.C. twice, New York City, and San Diego<sup>86</sup> to conduct interviews during the course of its investigation.<sup>87</sup>

Those interviewed included Target’s current and former officers who are named as defendants; the current and former members of Target’s Board of Directors who are named defendants; Target’s current and former chief compliance officer; personnel from the general counsel’s office; members of Target’s corporate security team; members of the Target Information Protection team; members of the Target Technology Services team; Target’s point-of-sale hardware engineers; Target’s network engineers; Target’s internal auditors; and representatives from Target’s third-party cardholder data security assessor and its independent auditor.<sup>88</sup>

In addition to the 73 interviews in which the SLC members participated personally, as part of the investigation, counsel conducted two supplemental interviews

---

<sup>83</sup> *Id.*

<sup>84</sup> *Id.*

<sup>85</sup> *Id.*

<sup>86</sup> Chief Justice Blatz traveled to San Diego; Professor Matheson participated via conference call.

<sup>87</sup> Blatz Aff. ¶ 34; Matheson Aff. ¶ 34.

<sup>88</sup> Blatz Aff. ¶ 35; Matheson Aff. ¶ 35. A list of interviewees is included as Appendix G to the Report. For a more fulsome discussion of the roles of the interviewees, see Blatz Aff. Ex. B at pp. 40–41.

and reported to the members of the SLC the substance of the interviews, issues raised, and information gleaned from them.<sup>89</sup> Those interviewed were employees involved in data risk assessments and risk treatment.<sup>90</sup> Counsel also met and had telephone conversations with a number of attorneys possessing relevant information, including Coordinating Lead Counsel in the MDL.<sup>91</sup>

### **SLC meetings**

Throughout its investigation, members of the SLC and counsel, in addition to engaging in telephone calls on a regular basis, met in person on more than 100 occasions.<sup>92</sup> The SLC reviewed the evidence developed, analyzed legal memoranda provided by counsel, assessed the credibility of the witnesses, and ascertained what additional information might be necessary or desirable in order to determine what course of action would be in the best interests of Target.<sup>93</sup>

During one meeting, the SLC toured Target's new Cyber Fusion Center and met with Target's Chief Information Security Officer, Target's Vice President of Cyber Security, its Vice President of Information Security, and its Senior Director of Cyber Security, to discuss Target's cybersecurity teams and their roles.<sup>94</sup>

---

<sup>89</sup> Blatz Aff. ¶ 37; Matheson Aff. ¶ 37.

<sup>90</sup> *Id.*

<sup>91</sup> *Id.*

<sup>92</sup> Blatz Aff. ¶ 31; Matheson Aff. ¶ 31.

<sup>93</sup> *Id.*

<sup>94</sup> Blatz Aff. ¶ 33; Matheson Aff. ¶ 33.

At another meeting, and at the SLC's invitation, Target's counsel gave a presentation on the facts and issues raised in the Demand and derivative complaints from Target's perspective.<sup>95</sup>

Counsel for the individual director defendants requested the opportunity to make a presentation on behalf of their clients, and the SLC agreed to hear the presentation during one of its meetings.<sup>96</sup>

The SLC also twice—at the beginning and toward the end of its investigation—invited counsel for the derivative shareholder plaintiffs and the Demand shareholder to make a presentation on the issues arising from their allegations, including their view of the factors bearing on whether there were rights and remedies Target had against the defendants named in the complaint that were in Target's best interests to pursue.<sup>97</sup> Counsel for the consolidated federal derivative plaintiffs, along with counsel for the state derivative plaintiff, responded with a telephone presentation and a written submission in October 2014.<sup>98</sup> They also provided a written submission in response to the SLC's second invitation in February 2016.<sup>99</sup>

The SLC, in conducting its investigation, considered and evaluated the derivative plaintiffs' counsel's investigative suggestions, including suggested interview questions, witnesses, and experts.<sup>100</sup> While the SLC considered the perspective offered by

---

<sup>95</sup> Blatz Aff. ¶ 32; Matheson Aff. ¶ 32.

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

<sup>98</sup> *Id.*

<sup>99</sup> *Id.*

<sup>100</sup> Blatz Aff. ¶ 36; Matheson Aff. ¶ 36.



plaintiffs' counsel, it conducted its own investigation and did so independently.<sup>101</sup> It did not share the information it gathered or its conclusions with the derivative plaintiffs, the individual defendants, Target, or their respective counsel before it issued its report.<sup>102</sup>

The SLC is confident that it received sufficient pertinent information to thoroughly understand the facts and the relevant parties' positions and views and reach an informed, reasoned judgment as to the best interests of Target with respect to the derivative actions and the shareholder Demand.<sup>103</sup> Once it concluded its investigation, the SLC reviewed the material developed, deliberated, and adopted its final report.<sup>104</sup>

#### **The SLC's report and conclusions**

On March 30, 2016, the SLC issued its 91-page report.<sup>105</sup> The SLC sent the Report and Appendices to Target's Board of Directors and sent copies to counsel for, variously, Target Corporation, the derivative plaintiff shareholders, Lead Coordinating Counsel for plaintiffs in the MDL, the shareholder who made the Demand on the Board, and the individual defendants.<sup>106</sup> The Report described the SLC's members, its formation, and its investigative methodology and set forth the factors it weighed in making its determinations. The Report did not set forth detailed factual findings. The SLC

---

<sup>101</sup> *Id.*

<sup>102</sup> *Id.*

<sup>103</sup> Blatz Aff. ¶ 38; Matheson Aff. ¶ 38.

<sup>104</sup> *Id.*

<sup>105</sup> Blatz Aff. ¶ 39; Matheson Aff. ¶ 39.

<sup>106</sup> Copies of the transmittal letters are attached as Ex. A to the Affidavit of Steve Gaskins.

determined that publishing detailed findings would not be in Target's best interests because doing so could imprudently create risks for the Company.<sup>107</sup>

The SLC concluded that it would not be in Target's best interests to pursue claims against the officers or directors identified in the Demand and derivative complaints, including those named in this action. It also determined that it should seek dismissal with prejudice of the pending claims, and so has filed this motion to dismiss the consolidated derivative complaint.

### **Argument**

**The Court should defer to the SLC's decision to dismiss these claims because the SLC demonstrated disinterested independence and an adequate, appropriate investigative methodology pursued in good faith.**

It is fundamental that a derivative case—which is brought by a shareholder for the benefit of the corporation in which he or she owns stock—belongs to the company, not to the shareholder who brought it.<sup>108</sup> It is also fundamental that the board of directors is in charge of the business decisions of a corporation, including who it should or should not sue.<sup>109</sup> In an instance in which directors or officers of a corporation are self-dealing to the detriment of the company or are committing crimes, or otherwise breaching their fiduciary duties, equity allows a shareholder to bring suit against wrongdoers on behalf of

---

<sup>107</sup> Blatz Aff. Ex. B at p. 68.

<sup>108</sup> *In re UnitedHealth Group Inc. S'holder Derivative Litig.*, 754 N.W.2d 544, 556 (Minn. 2008) (hereinafter "*UnitedHealth I*").

<sup>109</sup> Minn. Stat. §302A.201, Subd. 1 ("The business and affairs of a corporation shall be managed by or under the direction of a board...").

the corporation.<sup>110</sup> That equitable doctrine, however, is in tension with the right of a corporation to have its officers and directors run its business.

Minn. Stat. § 302A.241, which authorizes the use of special litigation committees, was enacted in part to address that tension and was designed to enable a corporation to dismiss, settle, or pursue a derivative suit despite a conflict of interest on the part of some or all of its directors. Under Minnesota law, corporations on whose behalf shareholder derivative claims have been made may establish a special litigation committee “consisting of one or more independent directors or other independent persons to consider legal rights or remedies of the corporation and whether those rights and remedies should be pursued.”<sup>111</sup> “Committees other than special litigation committees . . . are subject at all times to the direction and control of the board.”<sup>112</sup> Thus, by statute, an SLC is not subject to a board’s direction and control,<sup>113</sup> and special litigation committees remove the substantive decision about whether to pursue the claims advanced in a shareholder’s derivative action from both the alleged wrongdoers and from potentially disgruntled shareholders—who might “bring nuisance lawsuits with little merit” or even legitimate suits not worth pursuing—and places that decision in the hands of independent

---

<sup>110</sup> See *Janssen v. Best and Flanagan*, 662 N.W.2d 876, 882 (Minn. 2003).

<sup>111</sup> Minn. Stat. § 302A.241, Subd. 1.

<sup>112</sup> *Id.*

<sup>113</sup> See *id.*; *UnitedHealth I*, 754 N.W.2d at 550.

persons.<sup>114</sup> However, courts do insist that there be some judicial oversight to assure that the SLC's process is fulsome and that the SLC members are independent.<sup>115</sup>

Under Minnesota law, a special litigation committee is charged with fully informing itself of the legal and factual issues underlying derivative claims and determining whether pursuit of those claims is in the best interests of the corporation.<sup>116</sup> In making its determination, a special litigation committee has an obligation to undertake a “comprehensive weighing and balancing of factors” that takes into account the legal, ethical, commercial, professional, public relations, fiscal, and other factors “common to reasoned business decisions.”<sup>117</sup>

It is now well settled that when evaluating a motion to dismiss a derivative action, what an SLC's investigation has uncovered and the relative weight accorded in evaluating and balancing the factors considered by the SLC “are beyond the scope of judicial concern.”<sup>118</sup> Rather, Minnesota law requires a court to defer to a special litigation committee's decision with respect to a shareholder derivative action if the proponent of that decision demonstrates that (1) the members of the SLC possessed a

---

<sup>114</sup> See *Janssen*, 662 N.W.2d at 882–83 (discussing the rationale for applying the business judgment rule in derivative lawsuits).

<sup>115</sup> See, e.g., *Drilling v. Berman*, 589 N.W.2d 503, 510 (Minn. Ct. App. 1999) (an investigation “so restricted in scope, so shallow in execution, or otherwise so Pro forma or halfhearted as to constitute a pretext or sham” would prevent application of the business judgment rule).

<sup>116</sup> *Janssen*, 662 N.W.2d at 884.

<sup>117</sup> *Id.* at 883, 889.

<sup>118</sup> *In re UnitedHealth Group Inc. S'holder Derivative Litig.*, 591 F. Supp. 2d 1023, 1030 (D. Minn. 2008) (joint order of J. Rosenbaum and J. McGunnigle, also filed in Minn. Dist. Ct. No. 27-CV-06-8085) (hereinafter “*UnitedHealth II*”) (quoting *Drilling*, 589 N.W.2d at 508).

disinterested independence and (2) the SLC's investigative procedures and methodologies were adequate, appropriate, and pursued in good faith.<sup>119</sup>

The SLC asks this Court to approve the SLC's exercise of its business judgment in the disposition of the shareholder derivative claims and dismiss the above-captioned action because the SLC and its processes satisfy both prongs of the applicable Minnesota test.

**1) The members of the SLC possess a disinterested independence.**

In determining whether SLC members are disinterested and independent, the Minnesota Supreme Court has directed courts to consider the totality of the circumstances, including, but not limited to, the following eleven factors:

(1) whether the committee's members are defendants in the litigation; (2) whether members are exposed to direct and substantial liability; (3) whether the "members are outside, non-management directors"; (4) whether the members were on the board when the alleged wrongdoing occurred; (5) whether the "members participated in the alleged wrongdoing"; (6) whether the members approved conduct involving the alleged wrongdoing; (7) whether the members or their affiliated firms "had business dealings with the corporation other than as directors"; (8) whether the members "had business or social relationships with one or more of the defendants"; (9) whether the members received advice from independent counsel or other independent advisors; (10) the severity of the alleged wrongdoing; and (11) the size of the committee.<sup>120</sup>

An examination of these factors demonstrates the disinterested independence of this SLC. First, neither member is a defendant nor were they Target directors until appointment to this SLC; thus, they do not have exposure to any type of liability in this

---

<sup>119</sup> *UnitedHealth I*, 754 N.W.2d at 559.

<sup>120</sup> *Id.* at 560 n.11 (citing 2 Dennis J. Block et al., *The Business Judgment Rule: Fiduciary Duties of Corporate Directors* 1746–53 (5th ed. 1998)).

litigation, they were not on the board when the alleged wrongdoing occurred, and they were not in a position to approve or participate in any alleged wrongdoing. Chief Justice Blatz and Professor Matheson were even more independent than outside, non-management directors would be. Neither the members nor their advisors had material business dealings with Target, and neither member had business or social relationships with any named defendant. The members received advice from both independent counsel and independent experts. The breadth and depth of the SLC investigation was appropriate for the severity of the allegations, and the size of the committee was appropriate for the workload of the investigation and the determinations made by the committee. The statute authorizes a committee of one or more members and this committee had two members, which helped to assure diversity of opinion and point-of-view.

Other factors further demonstrate the disinterested independence of this SLC. Target played no role in the conduct of the SLC's investigation of the shareholder derivative claims other than providing the SLC with access to documents and witnesses. The SLC independently selected the Target current and former employees it wished to interview and conducted those interviews independently. In addition, after establishing the SLC, Target's Board of Directors had no say in or influence on the way the SLC conducted its investigation. Indeed, the resolution appointing the SLC expressly provided that the SLC "is granted full power and authority [] to investigate the allegations, claims, and requests for relief . . ." in the Demand and shareholder derivative claims.

In *UnitedHealth II*, after concluding that “the SLC is clearly disinterested and independent” based on the application of the eleven factors noted by the Minnesota Supreme Court, the federal and Minnesota courts jointly noted that the SLC’s members were former justices of the Minnesota Supreme Court who had no connection to UnitedHealth prior to accepting appointment to the SLC, did not face any liability in connection with the lawsuits, and received advice from independent experts and counsel.<sup>121</sup> The courts held that these facts “strongly suggest[ed] the SLC [was] in a position to base its decision on the merits.”<sup>122</sup>

In *Kokocinski v. Collins*, the court concluded the SLC members possessed a disinterested independence where the two members were not defendants in the case, had never served on the board and had no personal ties to the company, and received counsel and advice from an outside law firm and experts who also had no ties to the company.<sup>123</sup>

The same result is appropriate here—based on the foregoing, the Court should conclude that the SLC possessed a disinterested independence.

**2) The SLC’s investigative procedures and methodologies were adequate, appropriate, and pursued in good faith.**

The second element this Court must analyze is the adequacy of the procedures the special litigation committee utilized to gather the information it used to support its decision regarding the shareholder derivative claims.<sup>124</sup> The focus of this factor is on the

---

<sup>121</sup> 591 F. Supp. 2d at 1028.

<sup>122</sup> *Id.* at 1028–29.

<sup>123</sup> *Kokocinski v. Collins, et al.*, No. 12–633, Mem. Op. & Order Granting Motions to Dismiss (“*Kokocinski Order*”), Mar. 30, 2015, Docket No. 98, pp. 29–30.

<sup>124</sup> *UnitedHealth I*, 754 N.W.2d at 559 (citing *Auerbach*, 393 N.E.2d at 1001–03).

SLC's investigative process and methodology. Whether an SLC's methods demonstrate good faith depends on the nature of the particular investigation.<sup>125</sup> Minnesota courts look to the totality of the circumstances, and the factors underlying this decision include the following: (1) the length and scope of the investigation; (2) the committee's use of independent counsel or experts; (3) the corporation's or the defendants' involvement, if any, in the investigation; and (4) the adequacy and reliability of the information supplied to the committee.<sup>126</sup> "Evidence that 'the investigation has been so restricted in scope, so shallow in execution, or otherwise so pro forma or halfhearted as to constitute a pretext or sham . . . would raise questions of good faith.'"<sup>127</sup>

In *UnitedHealth II*, both courts, federal and state, determined that the SLC's procedures were adequate, appropriate, and performed in good faith when the SLC presented evidence—its Report and affidavits of the SLC members—showing the investigation's comprehensive scope.<sup>128</sup> In *UnitedHealth II*, the court also considered the fact that the SLC was granted, and exercised, complete power and authority to investigate, and each member personally prepared for and interviewed 50 witnesses, reviewed thousands of pages of documents, and reviewed cases and other materials to develop an understanding of the law governing the derivative claims while also

---

<sup>125</sup> *UnitedHealth II*, 591 F. Supp. 2d at 1029.

<sup>126</sup> *Id.* (citing *Drilling*, 589 N.W.2d at 509).

<sup>127</sup> *Kokocinski* Order at 34 (quoting *UnitedHealth II*, 591 F. Supp. 2d at 1029) (internal quotation omitted).

<sup>128</sup> *UnitedHealth II*, 591 F. Supp. 2d at 1029.



employing independent counsel and independent financial experts as evidence of its good faith investigation.<sup>129</sup>

In *Kokocinski*, the comprehensive scope of the investigation included the SLC's preparation for and interview of 60 witnesses over the course of eighteen months.<sup>130</sup> Chief Judge Tunheim noted in *Kokocinski* that the SLC's counsel conducted even more interviews and noted the number of pages of documents the SLC reviewed as evidence of its good faith investigation.<sup>131</sup> The defendants' involvement in both *UnitedHealth II* and *Kokocinski*, like this one, was limited to responding to requests for information and participating in interviews that the SLC requested.<sup>132</sup> And in each of those cases, it was shown that the SLC had full access to documents it requested, including those subject to a claim of attorney-client or attorney-work-product privilege.<sup>133</sup>

Similarly, the SLC here undertook a comprehensive investigation that lasted twenty-one months. It was granted and exercised complete power and authority to investigate the allegations, claims, and requests for relief, it employed independent counsel and independent experts, it reviewed thousands of pages of documents, and it interviewed scores of witnesses. The SLC developed an understanding of the applicable legal standard and the law governing derivative claims. Target's and the individual defendants' involvement was limited to responding to requests for information and participating in interviews of witnesses that were selected by the SLC. The SLC had full

---

<sup>129</sup> *Id.*

<sup>130</sup> *Kokocinski* Order at 34.

<sup>131</sup> *Id.*

<sup>132</sup> *Id.* at 35; *UnitedHealth II*, 591 F. Supp. 2d at 1029.

<sup>133</sup> *Kokocinski* Order at 35; *UnitedHealth II*, 591 F. Supp. 2d at 1029.

access to documents it requested, including those subject to a claim of attorney-client privilege or attorney-work-product privilege and had full access to the database in the MDL. In addition, the SLC did not share the information it gathered or its conclusions with Target, the individual defendants, the plaintiffs, or their respective counsel until the issuance of its report. All of the foregoing factors demonstrate that the SLC's investigative procedures and methodologies were adequate, appropriate, and pursued in good faith.

### **Conclusion**

Under Minnesota law, courts do not second-guess an SLC's conclusions or re-examine the merits of its decisions; rather, the Court's inquiry is limited to determining whether the SLC's members are disinterested and independent and whether the SLC's methodology indicates that its decision was the product of a good faith investigation.<sup>134</sup> Here, the Report and the SLC members' affidavits establish that the investigation was independent, extensive, and focused on the best interests of the company. Thus, the SLC has established the necessary factual predicate for the Court to approve the dismissal of the above-captioned action. Therefore, the SLC respectfully requests the Court to grant its motion for approval and dismissal and to enter judgment dismissing this matter with prejudice.

---

<sup>134</sup> *UnitedHealth II*, 591 F. Supp. 2d at 1030.

Respectfully submitted,

Dated: May 6, 2016

**GASKINS BENNETT BIRRELL SCHUPP, LLP**

/s/ Steve W. Gaskins

Steve W. Gaskins, Esq. #147643

Daniel P. Brees, Esq. #395284

Ian S. Birrell, Esq. #396379

333 South Seventh Street, Suite 3000

Minneapolis, MN 55402

Phone: 612.333.9500

Fax: 612.333.9579

sgaskins@gaskinsbennett.com

dbrees@gaskinsbennett.com

ibirrell@gaskinsbennett.com

*Attorneys for the Special Litigation Committee of Target Corporation's Board of Directors*

UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY

---

DENNIS PALKON, Derivatively on Behalf  
of WYNDHAM WORLDWIDE  
CORPORATION,

Plaintiff,

v.

STEPHEN P. HOLMES, ERIC A.  
DANZIGER, SCOTT G. MCLESTER,  
JAMES E. BUCKMAN, MICHAEL H.  
WARGOTZ, GEORGE HERRERA,  
PAULINE D.E. RICHARDS, MYRA J.  
BIBLOWIT, BRIAN MULRONEY,  
STEVEN A. RUDNITSKY, AND DOES 1-  
10,

Individual Defendants,

-and-

WYNDHAM WORLDWIDE  
CORPORATION, a Delaware corporation,

Nominal Defendant.

---

Civil Action No. 2:14-CV-01234 (SRC)

OPINION

CHESLER, District Judge

This matter comes before the Court upon the motion filed by Defendants Myra J. Biblowit, James E. Buckman, Eric A. Danziger, George Herrera, Stephen P. Holmes, Scott G. McLester, Brian Mulroney, Pauline D.E. Richards, Steven A. Rudnitsky, Michael H. Wargotz, and Wyndham Worldwide Corporation (collectively “Defendants”) to dismiss the Complaint

pursuant to Rules 23.1(b) and 12(b)(6) of the Federal Rules of Civil Procedure. Plaintiff Dennis Palkon (“Plaintiff”) opposes the motion. The Court has considered the parties’ submissions. For the reasons that follow, the Court grants the motion to dismiss, and the case will be closed.

## **I. BACKGROUND**

This case involves a shareholder who seeks to compel a corporate board of directors to bring a lawsuit on the company’s behalf. The shareholder’s proposed suit pertains to breaches of the company’s online networks, during which hackers accessed the personal and financial information of a large number of customers. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(a)(2), as the parties are citizens of different states and the amount in controversy exceeds \$75,000. The Court draws the following facts from the complaint, and assumes them to be true for purposes of this motion only.

### **A. Facts**

Wyndham Worldwide Corporation (“WWC”) is a large hospitality company that operates hotels and resorts globally. The company is incorporated in Delaware and headquartered in Parsippany, New Jersey. As part of the hospitality business, WWC’s subsidiaries often collect customers’ personal and financial data. WWC hotels let customers make room reservations online, which requires the customers to enter their personal credit card information.

On three occasions between April 2008 and January 2010, that information was stolen. Hackers breached WWC’s main network and those of its hotels. They performed a “brute force attack,” which means they guessed user IDs and passwords to enter an administrator’s account, and then used “memory-scraping malware” to collect sensitive data. Through these methods, the hackers obtained the personal information of over six-hundred thousand customers.

In April 2010, the Federal Trade Commission (“FTC”) began to investigate the cyber-

attacks against WWC, and in June 2012, it commenced a legal action against the company for its security practices. WWC retained the law firm of Kirkland & Ellis, LLP (“Kirkland”) to represent it in the FTC action.

In November 2012, a WWC shareholder sent a letter to WWC’s Board of Directors (“the Board”) demanding that it bring a lawsuit based on the online breaches. The Board instructed its Audit Committee to evaluate the demand. That committee then consulted with Kirkland, which found that the “shareholder demand letter [was] not well grounded.” On March 5, 2013, the Audit Committee recommended that WWC not bring the lawsuit, and on March 11, the full Board voted to adopt that recommendation.

Approximately three months later, on June 11, 2013, Plaintiff Dennis Palkon (“Plaintiff”) sent a letter to the Board similarly demanding that it “investigate, address, and promptly remedy the harm inflicted” on the company by the breaches. Plaintiff is a Pennsylvania resident who owned shares of WWC when it was hacked. WWC’s General Counsel, Scott McLester (“McLester”), wrote to Plaintiff on June 28 that he had submitted the demand to the Board.

The Board met on August 8 to discuss Plaintiff’s demand as well as developments in the FTC action. The Board voted unanimously not to pursue Plaintiff’s proposed litigation. On August 20, McLester wrote to Plaintiff’s counsel to report that the Board had found it “not in the best interests of [WWC] to pursue the claims” in Plaintiff’s demand. The letter further provided that the Board was declining Plaintiff’s demand for the same reasons it had refused the earlier, November 2012 demand, which was “virtually identical.” Plaintiff is represented by the same counsel who pursued that earlier demand.

Although it decided not to bring a lawsuit based on the breaches, the Board discussed the cyber-attacks, WWC’s security policies, and proposed security enhancements at fourteen

meetings between October 2008 and August 2012. The Audit Committee reviewed the same matters in at least sixteen meetings during that period. WWC hired technology firms to investigate each breach and to issue recommendations on enhancing the company's security. Following the second and third breaches, WWC began to implement those recommendations.

### **B. Procedural History and Defendants' Motion to Dismiss**

On February 25, 2014, Plaintiff filed a derivative lawsuit against WWC and numerous of its corporate officials. At the heart of Plaintiff's Complaint is an assertion that Defendants failed to implement adequate data-security mechanisms, such as firewalls and elaborate passwords, and that this failure allowed hackers to steal customers' data. He further claims that Defendants failed to timely disclose the data breaches after they occurred. Plaintiff claims that these actions damaged WWC's reputation and cost it significant legal fees. Most pertinently, given these allegations, Plaintiff contends that the Board's decision to refuse his demand was wrongful.

Defendants moved to dismiss Plaintiff's Complaint on June 2, 2014. Defendants argue three points to support their motion. First, they urge that the Board's refusal to pursue Plaintiff's demand was a good-faith exercise of business judgment, made after a reasonable investigation. Second, even if the Board's refusal had been wrongful, Defendants assert that the Complaint fails to state a claim upon which relief can be granted. Third, Defendants claim that Plaintiff's alleged damages are speculative and unripe.

Plaintiff opposes the motion for three corresponding reasons. He first contends that the Board wrongfully refused his demand by relying on an investigation dominated by conflicted counsel. He next urges that he adequately pleaded his legal claims, as WWC failed to institute reasonable security protections. Last, Plaintiff asserts that shareholders have already suffered damages due to the costs of defending against the FTC investigation.

## II. DISCUSSION

### A. Motions to Dismiss

Defendants move to dismiss pursuant to Rules 23.1(b) and 12(b)(6) of the Federal Rules of Civil Procedure. Accordingly, the Court will accept as true all of the factual allegations in Plaintiff's Complaint, as well as the reasonable inferences therefrom. See In re Forest Labs. Derivative Litig., 450 F. Supp. 2d 379, 387 (S.D.N.Y.2006) (applying Delaware law). The Court will not, however, accept a "legal conclusion couched as a factual allegation." Baraka v. McGreevey, 481 F.3d 187, 195 (3d Cir. 2007); Fowler v. UPMC Shadyside, 578 F.3d 203, 210-11 (3d Cir. 2009); see also Ashcroft v. Iqbal, 556 U.S. 662, 679 (2009) ("While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations.").

### B. Demand Refusal

Because WWC is a Delaware corporation, the substantive law of that state governs. See Kamen v. Kemper Fin. Servs., 500 U.S. 90, 108-09 (1991); Blasband v. Rales, 971 F.2d 1034, 1047 (3d Cir. 1992). Under Delaware law, "[t]he decision to bring a law suit or to refrain from litigating a claim on behalf of a corporation is a decision concerning the management of the corporation[.]" and it is "part of the responsibility of the board of directors." Spiegel v. Buntrock, 571 A.2d 767, 773 (Del. 1990). A shareholder who wishes to sue on behalf of a corporation, therefore, cannot do so independently, and must instead demand that the board of directors bring the action. Id.

If a board of directors refuses to pursue a shareholder's demand, that decision falls under the purview of the "business judgment rule." Id. at 773-74. Under that rule, courts presume that the board refused the demand "on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company." Id. at 774.



A shareholder dissatisfied with a board's refusal may seek to rebut that presumption by bringing a derivative action lawsuit. See id.; Rich ex rel. Fuqi Int'l v. Chong, 66 A.3d 963, 975 (Del. Ch. 2013). The shareholder must raise a reasonable doubt that the refusal was a business judgment, which requires pleading with particularity that the decision was either: (1) "made in bad faith," or (2) "based on an unreasonable investigation." In re Merrill Lynch & Co., 773 F. Supp. 2d 330, 351 (S.D.N.Y.2011) (quoting RCM Sec. Fund v. Stanton, 928 F.2d 1318, 1328 (2d Cir. 1991)) (applying Delaware law); see also Fed. R. Civ. P. 23.1(b)(3)(A) (providing that shareholder must plead with particularity the efforts to make a demand upon the board). This is a high burden. See In re Merrill Lynch, 773 F. Supp. 2d at 345 (noting that "few, if any, plaintiffs surmount this obstacle").

Based on these principles, here the Court must decide if Plaintiff pled with particularity facts which raise a reasonable doubt that the Board acted (1) in good faith, or (2) based on a reasonable investigation. For the reasons that follow, Plaintiff has failed to meet this burden.

### **C. Bad Faith**

Underlying Plaintiff's bad faith claim is the argument that the board's refusal was influenced by conflicted legal counsel. Plaintiff must show "that no reasonable business person could possibly" have made the refusal in good faith, or put differently, that the refusal goes "so far beyond the bounds of reasonable business judgment that its only explanation is bad faith." In re Tower Air, Inc., 416 F.3d 229, 238 (3d Cir. 2005). Plaintiff has not made such a demonstration with respect to either Kirkland or WWC's General Counsel.

Plaintiff first urges that Kirkland had a conflict of interest with respect to the shareholder demands because it already represented WWC in the FTC litigation. The principal case upon which Plaintiff relies is Stepak v. Addison, 20 F.3d 398, 400 (11th Cir. 1994). There, a board of

directors solicited the advice of an outside law firm to refuse a shareholder's demand. Significantly, however, that same firm "had represented the alleged wrongdoers in criminal proceedings involving the very subject matter of the demand." Id. The plaintiff urged, and the appellate panel found, that the firm had competing, conflicting duties, and thus could not impartially assess the shareholder demand. The firm faced "lingering and divided loyalties," to the criminal defendants who it represented, and was "hampered in its investigation of the shareholder's allegations by its continuing duty to preserve the secrets and confidences of its former clients." Id. at 405-06. Emphasizing that the outside proceedings were criminal, the panel concluded that the "firm's representation of the alleged wrongdoers in criminal investigations is clearly incompatible with its simultaneous handling of a reasonable and neutral investigation of their conduct on behalf of the corporation." Id. at 405.

This case presents no such concerns. Kirkland did not have multiple, conflicting duties. Instead, its obligations in the FTC and shareholder matters were identical: it had to act in WWC's best interest. Plaintiff concedes this mirroring obligation in his brief, where he writes that "Kirkland was simultaneously representing [WWC] in the FTC Action and was duty-bound to zealously protect the Company's interests in that case." [Docket Item # 38 at 13]. As Plaintiff expressly acknowledges, in the FTC Action Kirkland had to look after WWC's interests, just as it had to do for Plaintiff's demand. While the firm in Stepak had lingering confidentiality duties to individual criminal defendants, here Kirkland was duty-bound at all times to advocate for WWC, and for no one else. This fundamental distinction renders Stepak inapposite.

Plaintiff next argues that WWC's General Counsel was conflicted when he advised the Board, as he faced personal liability stemming from the cyber-attacks. This argument lacks factual support. Plaintiff has provided no indication that his demand exposed McLester to any

liability. Had the demand letter named McLester as a responsible party, Plaintiff's argument may carry more water. But the letter does not mention him. Furthermore, the subject matter of the demand was not an area with which McLester would likely be associated; he served as General Counsel, not as a technology or security official. See In re Bridgeport Holdings, 388 B.R. 548, 573 (Bankr. D. Del. 2008) ("Different corporate offices obviously hold different responsibilities."). Given that neither McLester nor other officials were named as targets, they had no reason to believe they were caught in Plaintiff's crosshairs.

To salvage this argument, Plaintiff asserts that McLester was "intimately involved in setting up the Company's data security in general[.]" (Compl. ¶ 80). Yet Plaintiff pleads no facts whatsoever as to what exactly McLester's supposed role was in the creation of the security programs. What was his intimate involvement? Without an answer to that question, Plaintiff's assertion falls short of the particularized pleading requirement of Rule 23.1(b), and it constitutes a conclusory allegation that the Court must disregard. See Iqbal, 556 U.S. at 679. Even if this allegation were substantiated, at most it would establish that personal liability may have been on McLester's radar. But WWC indemnified McLester against such liability [Docket Item # 14-3 at 25-28], and more importantly, the fear of personal liability alone does not render a corporate director conflicted. See Halpert Enters., 2007 WL 486561, at \*6.

Plaintiff also claims that McLester's conflict of interest spilled over to muddy Kirkland's ability to give neutral advice. Plaintiff has failed, however, to allege any particularized facts suggesting that McLester improperly influenced Kirkland, and even if he had influenced the firm, the Court has already found that McLester had no conflict of interest to impart.

#### **D. Unreasonable Investigation**

Plaintiff asserts that the Board's investigation was predetermined and thus unreasonable. Preliminarily, the Court notes that "there is no prescribed procedure or form a Board must follow when responding to a demand letter." In re Merrill Lynch, 773 F. Supp. 2d at 349. To assess the Board's investigation, then, the Court examines whether Plaintiff has pled particularized facts suggesting gross negligence, i.e., that "the Board acted with so little information that their decision was unintelligent and unadvised[.]" In re Gen. Motors Class E Stock Buyout Sec. Litig., 694 F. Supp. 1119, 1133 (D. Del. 1988) (internal quotation marks and citation omitted). In light of the ample information the Board had at its disposal when it rejected Plaintiff's demand, and considering the numerous steps the Board took to familiarize itself with the subject matter of the demand, Plaintiff has also failed to make this showing.

The Board's familiarity with the factual underpinnings of Plaintiff's demand did not begin with its arrival. Board members had already discussed the cyber-attacks at fourteen meetings from October 2008 to August 2012. "At every quarterly Board meeting, the General Counsel gave a presentation regarding the Breaches, and/or [WWC's] data-security generally." (Compl. ¶ 63). Similarly, WWC's "Audit Committee discussed these same issues in at least sixteen committee meetings during this same time period." (Id.). Board members' understanding of the subject matter of Plaintiff's demand had also already been developed pursuant to the FTC action, which stemmed from the same attacks. Finally, just before receiving Plaintiff's demand, the Board received and investigated a "virtually identical" demand letter brought by Plaintiff's counsel. (Compl. ¶¶ 75, 82). In response to that letter, the Board formally charged the Audit Committee with a review and discussed the matter at multiple meetings.

These earlier investigations, standing alone, would indicate that the Board had enough information when it assessed Plaintiff's claim. A board need not treat each demand as though it is the first; instead, board members may rely on earlier-obtained information. See In re Boston Scientific Corp. Shareholders Litig., 2007 WL 1696995, at \*5-6 (S.D.N.Y. June 13, 2007) (finding directors had sufficient information after they reviewed "earlier investigative work"); In re Merrill Lynch, 773 F. Supp. 2d at 349 (approving investigation where board "had already considered and rejected a similar demand" and "was already quite familiar with the allegations in plaintiff's letters from its consideration of the various other [related] proceedings"); Halpert Enterprises v. Harrison, 2007 WL 486561, at \*5-6 (S.D.N.Y. Feb. 14, 2007) (rejecting Plaintiff's notion that investigation was inadequate because it "merely referenced prior investigations").

All told, by the time Plaintiff submitted his letter, the Board's review of it did "not occur in a vacuum." [Docket Item #1-5 at 2]. Members were well versed on its allegations. Nevertheless, the Audit Committee and Board did specifically consider Plaintiff's submission. Board members met to discuss the demand on August 8, 2013, and they unanimously voted not to pursue it. In the Board's response to Plaintiff, it noted that it was rejecting Plaintiff's demand for the same reasons it had denied the earlier, "identical" demand. Those reasons were that: (1) "[WWC] has strong defenses to the FTC's allegations"; (2) the suit "would impair [WWC's] defenses in the FTC's lawsuit"; (3) "the claims contemplated are not yet ripe"; (4) "there has been no material damage to [WWC's] shareholders as a result of the FTC's lawsuit or the conduct at issue"; and (5) "there would be significant legal barriers to the claims contemplated by your letter."<sup>1</sup> [Docket Item #1-4 at 2-3].

---

<sup>1</sup> The fifth reason is particularly noteworthy. Because the law on demand-refusals resolves the motion, the Court need not reach the merits of Plaintiff's underlying claim. It is worth

To counter these explanations, Plaintiff simply notes that a letter-brief submitted on WWC's behalf states that the Board retained counsel to advise it "regarding rejection of the demand." Plaintiff contends that this phraseology shows that the refusal was preordained. Such isolated and post hoc language from a legal brief is "not evidence," In re eBay, Derivative Litig., 2011 WL 3880924, at \*5 n.8 (D. Del. Sept. 2, 2011), and even if it were, it could not overcome the extensive steps taken and information had by the Board, as reviewed above.

Given the business judgment rule's strong presumption, courts uphold even cursory investigations by boards refusing shareholder demands. See Levine v. Smith, 591 A.2d 194, 199, 214 (upholding investigation where board merely wrote to plaintiff that it had reviewed the demand and found that pursuing it would not be in the corporate interest). Here, the Court finds that WWC's Board had a firm grasp of Plaintiff's demand when it determined that pursuing it was not in the corporation's best interest.

### III. CONCLUSION

For the reasons above, the Court will grant Defendants' motion, dismissing Plaintiff's claims with prejudice. An appropriate Order will be filed.

s/ Stanley R. Chesler  
STANLEY R. CHESLER  
United States District Judge

Dated: October 20, 2014

---

acknowledging, however, that a board considering whether to file suit may consider the merits of the proposed action. Here, Plaintiff's claim rested on a novel theory. 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.

## MARKET INTELLIGENCE

# How the Yahoo Probe Points to Possible Cover-Up

Jeff John Roberts

Jan 23, 2017



Federal investigations into [Yahoo's handling of](#) two massive data breaches are becoming more serious, legal experts and a recent news [report](#) suggest. In the worst case scenario, investigators could conclude actions by Yahoo employees amounted to an illegal cover-up, and possibly even bring criminal charges.

These are the latest twists in a complicated story involving hacks on Yahoo ([YHOO, -0.10%](#)) in 2013 and 2014, which affected 1.5 billion customer accounts. The company only reported the breaches in September and December of last year, triggering investigations and putting Yahoo's planned merger with [Verizon \(VZ, +1.82%\)](#) in jeopardy.

According to a front page *Wall Street Journal* [story](#), the Securities and Exchange Commission is looking into whether the two breaches should have been disclosed sooner to investors. This is significant because the agency has never pursued charges against a company over a data breach that affected its valuation.

The Yahoo probe comes amid widespread uncertainty over what companies must do if they are hacked. While there are [laws](#) about disclosure, they vary from state to state, and the SEC only offers untested guidelines. As a result, the SEC sees the Yahoo situation as an ideal opportunity to clarify its rules, according to unnamed sources in the *Journal*.

This idea of using Yahoo to clear up the law makes sense, according to [Aaron Tantleff](#), an authority on data breaches at the law firm, Foley & Lardner.

"It involves a big incident that affects valuation and could derail a merger. It's one of the best potential test cases," says Tantleff, adding the case could lead to unprecedented criminal charges if it turns out Yahoo, which had been in merger talks when the breach was discovered, orchestrated a cover-up.

There is so far no proof Yahoo hushed up the breaches in order to protect its valuation or a possible deal, but there are a number of red flags, according to Tantleff.

These red flags relate to the 2014 breach, which saw hackers compromise more than 500,000 accounts, gaining access to consumers' personal information such as email addresses and birth dates, and answers to password-related security questions. (Yahoo says it discovered the [separate 2013 breach](#), which was even bigger, much later).

While Yahoo only disclosed the existence of the 2014 breach last September, the company has since conceded that some [employees knew about it](#) the same year. It's unclear why those employees failed to alert senior executives (or if in fact they did so), but a source familiar with Yahoo has previously told *Fortune* that the workers did not appreciate the scope or severity of the breach until later.

Meanwhile, Tantleff points to Yahoo CEO Marissa Mayer as another source of potential liability for the company. Specifically, it has emerged that Mayer [knew about the 2014 breach](#) as early as July of last year—well before the company publicly disclosed it in September. Verizon only declared its intention to buy Yahoo on July 25, raising questions of whether Mayer and Yahoo deliberately concealed material information from the phone giant and from investors.

There are other possible [explanations](#) for Yahoo's delay in disclosing the hacks. These include a failure to appreciate the significance of the hacks, as the company has suggested, as well as legal uncertainty about its obligations.

## Legal Swarm Around Yahoo

The Yahoo hacking incidents are notable not only for their scale—they are the two biggest data breaches in history—but for the intense legal scrutiny they are attracting. The company is facing more than a dozen class action suits over the breach, and also an onslaught of regulatory investigations.

In response to a question about the status of the investigations, a lawyer for the company said Yahoo could only restate the remarks it included in an SEC filing:

“[T]he Company is cooperating with federal, state, and foreign governmental officials and agencies seeking information and/or documents about the Security Incident and related matters, including the U.S. Federal Trade Commission, the U.S. Securities and Exchange Commission, a number of State Attorneys General, and the U.S. Attorney’s office for the Southern District of New York.”



The U.S. Attorney for New York is a notable inclusion on the list because the office is known for prosecuting cyber-crime and white collar criminal cases on behalf of the Justice Department.

In the case of the Yahoo breaches, the U.S. Attorney's Office is likely conducting an investigation into who carried out the hacks, but it also has the power to bring criminal charges against company executives in the event of a cover-up. A spokesperson for the office declined to comment, as did the SEC.

*Get Data Sheet*, Fortune's *technology newsletter*.

In press releases, Yahoo has blamed "state-sponsored actors" for both of the breaches, a position greeted with skepticism by some in the cyber-security community.

The ongoing controversy over the hacking incidents has taken a toll on the proposed deal between Yahoo and Verizon, leading the phone giant to demand a significant write down and even drop hints it could **back out** altogether.

Yahoo will announce its latest earnings result at market close on Monday. Its share price is up slightly.

**POMERANTZ LLP**

Jennifer Pafiti (SBN 282790)  
468 North Camden Drive  
Beverly Hills, CA 90210  
Telephone: (818) 532-6499  
E-mail: jpafiti@pomlaw.com  
- additional counsel on signature page -

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

MARK MADRACK, Individually and on  
Behalf of All Others Similarly Situated,

Plaintiff,

vs.

YAHOO! INC., MARISSA A. MAYER, and  
KENNETH A. GOLDMAN,

Defendants

Case No.

**CLASS ACTION COMPLAINT FOR  
VIOLATION OF THE FEDERAL  
SECURITIES LAWS**

JURY TRIAL DEMANDED

Plaintiff Mark Madrack (“Plaintiff”), individually and on behalf of all other persons similarly situated, by Plaintiff’s undersigned attorneys, for Plaintiff’s complaint against Defendants (defined below), alleges the following based upon personal knowledge as to Plaintiff and Plaintiff’s own acts, and information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through Plaintiff’s attorneys, which included, among other things, a review of the Defendants’ public documents, conference calls and announcements made by Defendants, United States Securities and Exchange Commission (“SEC”) filings, wire and press releases published by and regarding Yahoo! Inc. (“Yahoo” or the “Company”), analysts’ reports and advisories about the Company, and information readily obtainable on the Internet. Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

**NATURE OF THE ACTION**

1  
2 1. This is a federal securities class action on behalf of a class consisting of all persons other  
3 than Defendants who purchased or otherwise acquired common shares of Yahoo between November  
4 12, 2013 and December 14, 2016, both dates inclusive (the “Class Period”). Plaintiff seeks to recover  
5 compensable damages caused by Defendants’ violations of the federal securities laws and to pursue  
6 remedies under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the “Exchange Act”)  
7 and Rule 10b-5 promulgated thereunder.  
8

9 2. Yahoo, together with its subsidiaries, is a multinational technology company that  
10 provides a variety of internet services, including, *inter alia*, a web portal, search engine, Yahoo! Mail,  
11 Yahoo! News, Yahoo! Finance, advertising, and fantasy sports. As of February 2016, Yahoo had an  
12 estimated 1 billion monthly active users, roughly 280 million Yahoo! Mail users, and 205 million  
13 monthly unique visitors to its sites and services.  
14

15 3. Founded in January 1994, the Company was formerly known as “Jerry and David’s  
16 Guide to the World Wide Web” and changed its name to Yahoo! Inc. in March 1994. Yahoo is  
17 headquartered in Sunnyvale, California. The Company’s common stock trades on the Nasdaq Capital  
18 Market (“NASDAQ”) under the ticker symbol “YHOO.”  
19

20 4. On July 25, 2016, Verizon Communications, Inc. (“Verizon”) formally announced its  
21 intent to acquire Yahoo’s internet business for \$4.8 billion.

22 5. Throughout the Class Period, Defendants made materially false and misleading  
23 statements regarding the Company’s business, operational and compliance policies. Specifically,  
24 Defendants made false and/or misleading statements and/or failed to disclose that: (i) Yahoo failed to  
25 encrypt its users’ personal information and/or failed to encrypt its users’ personal data with an up-to-  
26 date and secure encryption scheme; (ii) consequently, sensitive personal account information from more  
27 than 1 billion users was vulnerable to theft; (iii) a data breach resulting in the theft of personal user data  
28

1 would foreseeably cause a significant drop in user engagement with Yahoo's websites and services; and  
2 (iv) as a result, Yahoo's public statements were materially false and misleading at all relevant times.

3 6. On September 22, 2016, Yahoo disclosed that hackers had stolen information in late  
4 2014 on more than 500 million accounts. Following the breach, Yahoo executives advised investors  
5 that the breach was not material, in part because the Company had not required to reset their passwords.

6 7. On this news, Yahoo's share price fell \$1.35, or 3.06%, to close at \$42.80 on September  
7 23, 2016.

8 8. On December 14, 2016, post-market, Yahoo announced that it had uncovered a data  
9 breach, stating that data from more than 1 billion user accounts was compromised in August 2013. In a  
10 press release and Current Report filed with the SEC on Form 8-K, Yahoo stated, in part:

11  
12 SUNNYVALE, Calif., December 14, 2016— Yahoo! Inc. (NASDAQ:YHOO) has  
13 identified data security issues concerning certain Yahoo user accounts. Yahoo has taken  
14 steps to secure user accounts and is working closely with law enforcement.

15 As Yahoo previously disclosed in November, law enforcement provided the company  
16 with data files that a third party claimed was Yahoo user data. The company analyzed this  
17 data with the assistance of outside forensic experts and found that it appears to be Yahoo  
18 user data. Based on further analysis of this data by the forensic experts, *Yahoo believes*  
19 *an unauthorized third party, in August 2013, stole data associated with more than one*  
20 *billion user accounts*. The company has not been able to identify the intrusion associated  
21 with this theft. Yahoo believes this incident is likely distinct from the incident the  
22 company disclosed on September 22, 2016.

23 *For potentially affected accounts, the stolen user account information may have*  
24 *included names, email addresses, telephone numbers, dates of birth, hashed passwords*  
25 *(using MD5) and, in some cases, encrypted or unencrypted security questions and*  
26 *answers*. The investigation indicates that the stolen information did not include  
27 passwords in clear text, payment card data, or bank account information. Payment card  
28 data and bank account information are not stored in the system the company believes was  
affected.

*Yahoo is notifying potentially affected users and has taken steps to secure their*  
*accounts, including requiring users to change their passwords. Yahoo has also*  
*invalidated unencrypted security questions and answers so that they cannot be used to*  
*access an account.*

1 Separately, Yahoo previously disclosed that its outside forensic experts were  
2 investigating the creation of forged cookies that could allow an intruder to access users'  
3 accounts without a password. Based on the ongoing investigation, the company believes  
4 an unauthorized third party accessed the company's proprietary code to learn how to  
5 forge cookies. The outside forensic experts have identified user accounts for which they  
6 believe forged cookies were taken or used. Yahoo is notifying the affected account  
7 holders, and has invalidated the forged cookies. The company has connected some of this  
8 activity to the same state-sponsored actor believed to be responsible for the data theft the  
9 company disclosed on September 22, 2016.

10 (Emphases added.)

11 9. Following Yahoo's announcement, several news sources reported that Verizon was  
12 considering ways to amend the terms of its deal with Yahoo to reflect the impact of the data breach and  
13 would likely seek "major concessions" from Yahoo.

14 10. On this news, Yahoo's share price fell \$2.50, or 6.11%, to close at \$38.41 on December  
15 15, 2016.

16 11. On December 15, 2016, after the market closed, the *Wall Street Journal* published an  
17 article entitled "Yahoo's Password Move May Put Verizon Deal at Risk." The article stated, in part:

18 Yahoo Inc.'s move to force some users to reset their passwords following a newly  
19 disclosed security breach could disrupt the planned sale of its core assets to Verizon  
20 Communications Inc., security experts say.

21 Yahoo didn't force users to reset their passwords after its September disclosure of  
22 another breach. *Experts say forcing users to reset their passwords typically causes some  
23 to drop a service.*

24 That is one reason why the newly disclosed hack—which Yahoo says occurred in 2013  
25 and affected more than one billion accounts—could prove more disruptive to Verizon's  
26 pending \$4.83 billion acquisition of Yahoo's core assets.

27 ...

28 *Yahoo is forcing users to reset their passwords now because some of the material taken  
in the 2013 breach wasn't encrypted, and other parts were protected by what is now  
considered an outdated encryption scheme,* according to a person familiar with that  
matter.

(Emphases added.)

1 12. On January 23, 2017, the *Wall Street Journal* reported that the SEC had opened an  
2 investigation into the timing of Yahoo's disclosures regarding the data breaches. The article reported,  
3 in part:

4 The Securities and Exchange Commission has opened an investigation, and in December  
5 issued requests for documents, as it looks into whether the tech company's disclosures  
6 about the cyberattacks complied with civil securities laws, the people said. The SEC  
7 requires companies to disclose cybersecurity risks as soon as they are determined to have  
8 an effect on investors.

9 The investigation is likely to center on a 2014 data breach at Yahoo that compromised the  
10 data of at least 500 million users, according to the people familiar with the matter. Yahoo  
11 disclosed that breach in September 2016, despite having linked the incident to state-  
12 sponsored hackers two years earlier.

13 To date, Yahoo hasn't explained why the company took two years to disclose the 2014  
14 incident publicly or who made the decision not to go public sooner with this information.  
15 In mid-December Yahoo also said it had recently discovered an August 2013 data breach  
16 that had exposed the private information of more than 1 billion Yahoo users.

17 13. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in  
18 the market value of the Company's common shares, Plaintiff and other Class members have suffered  
19 significant losses and damages.

#### 20 **JURISDICTION AND VENUE**

21 14. The claims asserted herein arise under and pursuant to §§10(b) and 20(a) of the  
22 Exchange Act (15 U.S.C. §§78j(b) and §78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17  
23 C.F.R. §240.10b-5).

24 15. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §1331  
25 and §27 of the Exchange Act.

26 16. Venue is proper in this Judicial District pursuant to §27 of the Exchange Act (15 U.S.C.  
27 §78aa) and 28 U.S.C. §1391(b). Yahoo's principal executive offices are located within this Judicial  
28 District.

1 17. In connection with the acts, conduct and other wrongs alleged in this Complaint,  
2 Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce,  
3 including but not limited to, the United States mail, interstate telephone communications and the  
4 facilities of the national securities exchange.

5 **PARTIES**

6  
7 18. Plaintiff, as set forth in the accompanying Certification, purchased common shares of  
8 Yahoo at artificially inflated prices during the Class Period and was damaged upon the revelation of the  
9 alleged corrective disclosure.

10 19. Defendant Yahoo! Inc. is incorporated in Delaware, and the Company's principal  
11 executive offices are located at 701 First Avenue, Sunnyvale, California, 94089. Yahoo's common  
12 stock trades on the NASDAQ under the ticker symbol "YHOO."

13  
14 20. Defendant Marissa A. Mayer ("Mayer") has served at all relevant times as the  
15 Company's Chief Executive Officer ("CEO") and Director.

16 21. Defendant Kenneth A. Goldman ("Goldman") has served at all relevant times as the  
17 Company's Chief Financial Officer ("CFO").

18  
19 22. The Defendants referenced above in ¶¶ 20-21 are sometimes referred to- herein as the  
20 "Individual Defendants."

21 **SUBSTANTIVE ALLEGATIONS**

22 **Background**

23 23. Yahoo, together with its subsidiaries, is a multinational technology company that  
24 provides a variety of internet services, including, *inter alia*, a web portal, search engine, Yahoo! Mail,  
25 Yahoo! News, Yahoo! Finance, advertising, and fantasy sports. As of February 2016, Yahoo had an  
26 estimated 1 billion monthly active users, roughly 280 million Yahoo! Mail users, and 205 million  
27 monthly unique visitors to its sites and services.  
28

**Materially False and Misleading Statements Issued During the Class Period**

1  
2 24. The Class Period begins on November 12, 2013, when Yahoo filed a Quarterly Report  
3 on Form 10-Q with the SEC, announcing the Company’s financial and operating results for the quarter  
4 ended September 30, 2013 (the “Q3 2013 10-Q”). For the quarter, Yahoo announced net income of  
5 \$296.66 million, or \$0.28 per diluted share, on revenue of \$1.14 billion, compared to net income of  
6 \$3.12 billion, or \$2.64 per diluted share, on revenue of \$1.2 billion for the same period in the prior year.

7  
8 25. In the Q3 2013 10-Q, with respect to the efficacy of the Company’s encryption of user  
9 data, Yahoo simply stated, in part:

10 *If our security measures are breached, our products and services may be perceived as*  
11 *not being secure, users and customers may curtail or stop using our products and*  
12 *services, and we may incur significant legal and financial exposure.*

13 Our products and services involve the storage and transmission of Yahoo’s users’ and  
14 customers’ personal and proprietary information in our facilities and on our equipment,  
15 networks and corporate systems. Security breaches expose us to a risk of loss of this  
16 information, litigation, remediation costs, increased costs for security measures, loss of  
17 revenue, damage to our reputation, and potential liability. Our user data and corporate  
18 systems and security measures have been and may in the future be breached due to the  
19 actions of outside parties (including cyber attacks), employee error, malfeasance, a  
20 combination of these, or otherwise, allowing an unauthorized party to obtain access to  
21 our data or our users’ or customers’ data. Additionally, outside parties may attempt to  
22 fraudulently induce employees, users, or customers to disclose sensitive information in  
23 order to gain access to our data or our users’ or customers’ data.

24 Any breach or unauthorized access could result in significant legal and financial  
25 exposure, increased remediation and other costs, damage to our reputation and a loss of  
26 confidence in the security of our products, services and networks that could potentially  
27 have an adverse effect on our business. Because the techniques used to obtain  
28 unauthorized access, disable or degrade service, or sabotage systems change frequently or  
may be designed to remain dormant until a predetermined event and often are not  
recognized until launched against a target, we may be unable to anticipate these  
techniques or implement adequate preventative measures. If an actual or perceived breach  
of our security occurs, the market perception of the effectiveness of our security measures  
could be harmed and we could lose users and customers.

27 26. The Q3 2013 10-Q contained signed certifications pursuant to the Sarbanes-Oxley Act of  
28 2002 (“SOX”) by the Individual Defendants, stating that the financial information contained in the Q3



1 2013 10-Q was accurate and disclosed any material changes to the Company's internal control over  
2 financial reporting.

3 27. On February 28, 2014, Yahoo filed an Annual Report on Form 10-K with the SEC,  
4 announcing the Company's financial and operating results for the quarter and year ended December 31,  
5 2013 (the "2013 10-K"). For the quarter, Yahoo announced net income of \$348.19 million, or \$0.33  
6 per diluted share, on revenue of \$1.27 billion, compared to net income of \$272.27 million, or \$0.23 per  
7 diluted share, on revenue of \$1.35 billion for the same period in the prior year. For 2013, Yahoo  
8 announced net income of \$1.37 billion, or \$1.26 per diluted share, on revenue of \$4.68 billion,  
9 compared to net income of \$3.95 billion, or \$3.28 per diluted share, on revenue of \$4.99 billion for  
10 2012.  
11

12 28. In the 2013 10-K, with respect to the efficacy of the Company's encryption of user data,  
13 Yahoo simply stated, in part:  
14

15 ***If our security measures are breached, our products and services may be perceived as***  
16 ***not being secure, users and customers may curtail or stop using our products and***  
17 ***services, and we may incur significant legal and financial exposure.***

18 Our products and services involve the storage and transmission of Yahoo's users' and  
19 customers' personal and proprietary information in our facilities and on our equipment,  
20 networks and corporate systems. Security breaches expose us to a risk of loss of this  
21 information, litigation, remediation costs, increased costs for security measures, loss of  
22 revenue, damage to our reputation, and potential liability. Security breaches or  
23 unauthorized access have resulted in and may in the future result in a combination of  
24 significant legal and financial exposure, increased remediation and other costs, damage to  
25 our reputation and a loss of confidence in the security of our products, services and  
26 networks that could have an adverse effect on our business. We take steps to prevent  
27 unauthorized access to our corporate systems, however, because the techniques used to  
28 obtain unauthorized access, disable or degrade service, or sabotage systems change  
frequently or may be designed to remain dormant until a triggering event, we may be  
unable to anticipate these techniques or implement adequate preventative measures. If an  
actual or perceived breach of our security occurs, the market perception of the  
effectiveness of our security measures could be harmed and we could lose users and  
customers.

1 29. The 2013 10-K contained signed certifications pursuant to SOX by the Individual  
2 Defendants, stating that the financial information contained in the 2013 10-K was accurate and  
3 disclosed any material changes to the Company's internal control over financial reporting.

4 30. On May 8, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,  
5 announcing the Company's financial and operating results for the quarter ended March 31, 2014 (the  
6 "Q1 2014 10-Q"). For the quarter, Yahoo announced net income of \$311.58 million, or \$0.29 per  
7 diluted share, on revenue of \$1.13 billion, compared to net income of \$390.29 million, or \$0.35 per  
8 diluted share, on revenue of \$1.14 billion for the same period in the prior year.

9 31. In the Q1 2014 10-Q, with respect to the efficacy of the Company's encryption of user  
10 data, Yahoo simply stated, in part:  
11

12 ***If our security measures are breached, our products and services may be perceived as***  
13 ***not being secure, users and customers may curtail or stop using our products and***  
14 ***services, and we may incur significant legal and financial exposure.***

15 Our products and services involve the storage and transmission of Yahoo's users' and  
16 customers' personal and proprietary information in our facilities and on our equipment,  
17 networks and corporate systems. Security breaches expose us to a risk of loss of this  
18 information, litigation, remediation costs, increased costs for security measures, loss of  
19 revenue, damage to our reputation, and potential liability. Security breaches or  
20 unauthorized access have resulted in and may in the future result in a combination of  
21 significant legal and financial exposure, increased remediation and other costs, damage to  
22 our reputation and a loss of confidence in the security of our products, services and  
23 networks that could have an adverse effect on our business. We take steps to prevent  
24 unauthorized access to our corporate systems, however, because the techniques used to  
25 obtain unauthorized access, disable or degrade service, or sabotage systems change  
26 frequently or may be designed to remain dormant until a triggering event, we may be  
27 unable to anticipate these techniques or implement adequate preventative measures. If an  
28 actual or perceived breach of our security occurs, the market perception of the  
effectiveness of our security measures could be harmed and we could lose users and  
customers.

29 32. The Q1 2014 10-Q contained signed certifications pursuant to SOX by the Individual  
30 Defendants, stating that the financial information contained in the Q1 2014 10-Q was accurate and  
31 disclosed any material changes to the Company's internal control over financial reporting.

1 33. On August 7, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,  
2 announcing the Company's financial and operating results for the quarter ended June 30, 2014 (the "Q2  
3 2014 10-Q"). For the quarter, Yahoo announced net income of \$269.71 million, or \$0.26 per diluted  
4 share, on revenue of \$1.08 billion, compared to net income of \$331.15 million, or \$0.30 per diluted  
5 share, on revenue of \$1.14 billion for the same period in the prior year.

6 34. In the Q2 2014 10-Q, with respect to the efficacy of the Company's encryption of user  
7 data, Yahoo simply stated, in part:  
8

9 *If our security measures are breached, our products and services may be perceived as*  
10 *not being secure, users and customers may curtail or stop using our products and*  
11 *services, and we may incur significant legal and financial exposure.*

12 Our products and services involve the storage and transmission of Yahoo's users' and  
13 customers' personal and proprietary information in our facilities and on our equipment,  
14 networks and corporate systems. Security breaches expose us to a risk of loss of this  
15 information, litigation, remediation costs, increased costs for security measures, loss of  
16 revenue, damage to our reputation, and potential liability. Security breaches or  
17 unauthorized access have resulted in and may in the future result in a combination of  
18 significant legal and financial exposure, increased remediation and other costs, damage to  
19 our reputation and a loss of confidence in the security of our products, services and  
20 networks that could have an adverse effect on our business. We take steps to prevent  
21 unauthorized access to our corporate systems, however, because the techniques used to  
22 obtain unauthorized access, disable or degrade service, or sabotage systems change  
23 frequently or may be designed to remain dormant until a triggering event, we may be  
24 unable to anticipate these techniques or implement adequate preventative measures. If an  
25 actual or perceived breach of our security occurs, the market perception of the  
26 effectiveness of our security measures could be harmed and we could lose users and  
27 customers.

28 35. The Q2 2014 10-Q contained signed certifications pursuant to SOX by the Individual  
Defendants, stating that the financial information contained in the Q2 2014 10-Q was accurate and  
disclosed any material changes to the Company's internal control over financial reporting.

36. On November 7, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,  
announcing the Company's financial and operating results for the quarter ended September 30, 2014  
(the "Q3 2014 10-Q"). For the quarter, Yahoo announced net income of \$6.77 billion, or \$6.70 per

1 diluted share, on revenue of \$1.15 billion, compared to net income of \$296.66 million, or \$0.28 per  
2 diluted share, on revenue of \$1.14 billion for the same period in the prior year.

3 37. In the Q3 2014 10-Q, with respect to the efficacy of the Company's encryption of user  
4 data, Yahoo simply stated, in part:

5 *If our security measures are breached, our products and services may be perceived as*  
6 *not being secure, users and customers may curtail or stop using our products and*  
7 *services, and we may incur significant legal and financial exposure.*

8 Our products and services involve the storage and transmission of Yahoo's users' and  
9 customers' personal and proprietary information in our facilities and on our equipment,  
10 networks and corporate systems. Security breaches expose us to a risk of loss of this  
11 information, litigation, remediation costs, increased costs for security measures, loss of  
12 revenue, damage to our reputation, and potential liability. Security breaches or  
13 unauthorized access have resulted in and may in the future result in a combination of  
14 significant legal and financial exposure, increased remediation and other costs, damage to  
15 our reputation and a loss of confidence in the security of our products, services and  
16 networks that could have an adverse effect on our business. We take steps to prevent  
17 unauthorized access to our corporate systems, however, because the techniques used to  
18 obtain unauthorized access, disable or degrade service, or sabotage systems change  
19 frequently or may be designed to remain dormant until a triggering event, we may be  
20 unable to anticipate these techniques or implement adequate preventative measures. If an  
21 actual or perceived breach of our security occurs, the market perception of the  
22 effectiveness of our security measures could be harmed and we could lose users and  
23 customers.

24 38. The Q3 2014 10-Q contained signed certifications pursuant to SOX by the Individual  
25 Defendants, stating that the financial information contained in the Q3 2014 10-Q was accurate and  
26 disclosed any material changes to the Company's internal control over financial reporting.

27 39. On February 27, 2015, Yahoo filed an Annual Report on Form 10-K with the SEC,  
28 announcing the Company's financial and operating results for the quarter and year ended December 31,  
2014 (the "2014 10-K"). For the quarter, Yahoo announced net income of \$166.34 million, or \$0.17  
per diluted share, on revenue of \$1.25 billion, compared to net income of \$348.19 million, or \$0.33 per  
diluted share, on revenue of \$1.27 billion for the same period in the prior year. For 2014, Yahoo  
announced net income of \$7.52 billion, or \$7.45 per diluted share, on revenue of \$4.62 billion,

1 compared to net income of \$1.37 billion, or \$1.26 per diluted share, on revenue of \$4.68 billion for  
2 2013.

3 40. In the 2014 10-K, with respect to the efficacy of the Company's encryption of user data,  
4 Yahoo simply stated, in part:

5 *If our security measures are breached, our products and services may be perceived as*  
6 *not being secure, users and customers may curtail or stop using our products and*  
7 *services, and we may incur significant legal and financial exposure.*

8 Our products and services involve the storage and transmission of Yahoo's users' and  
9 customers' personal and proprietary information in our facilities and on our equipment,  
10 networks and corporate systems. Security breaches expose us to a risk of loss of this  
11 information, litigation, remediation costs, increased costs for security measures, loss of  
12 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
13 fraudulently induce employees, users, or customers to disclose sensitive information to  
14 gain access to our data or our users' or customers' data. In addition, hardware, software  
15 or applications we procure from third parties may contain defects in design or  
16 manufacture or other problems that could unexpectedly compromise network and data  
17 security. Security breaches or unauthorized access have resulted in and may in the future  
18 result in a combination of significant legal and financial exposure, increased remediation  
19 and other costs, damage to our reputation and a loss of confidence in the security of our  
20 products, services and networks that could have an adverse effect on our business. We  
21 take steps to prevent unauthorized access to our corporate systems, however, because the  
22 techniques used to obtain unauthorized access, disable or degrade service, or sabotage  
23 systems change frequently or may be designed to remain dormant until a triggering event,  
24 we may be unable to anticipate these techniques or implement adequate preventative  
25 measures. If an actual or perceived breach of our security occurs, the market perception  
26 of the effectiveness of our security measures could be harmed and we could lose users  
27 and customers.  
28

41. The 2014 10-K contained signed certifications pursuant to SOX by the Individual  
Defendants, stating that the financial information contained in the 2014 10-K was accurate and  
disclosed any material changes to the Company's internal control over financial reporting.

42. On May 7, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,  
announcing the Company's financial and operating results for the quarter ended March 31, 2015 (the  
"Q1 2015 10-Q"). For the quarter, Yahoo announced net income of \$21.20 million, or \$0.02 per

1 diluted share, on revenue of \$1.23 billion, compared to net income of \$311.58 million, or \$0.29 per  
2 diluted share, on revenue of \$1.13 billion for the same period in the prior year.

3 43. In the Q1 2015 10-Q, with respect to the efficacy of the Company's encryption of user  
4 data, Yahoo simply stated, in part:

5 *If our security measures are breached, our products and services may be perceived as*  
6 *not being secure, users and customers may curtail or stop using our products and*  
7 *services, and we may incur significant legal and financial exposure.*

8 Our products and services involve the storage and transmission of Yahoo's users' and  
9 customers' personal and proprietary information in our facilities and on our equipment,  
10 networks and corporate systems. Security breaches expose us to a risk of loss of this  
11 information, litigation, remediation costs, increased costs for security measures, loss of  
12 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
13 fraudulently induce employees, users, or customers to disclose sensitive information to  
14 gain access to our data or our users' or customers' data. In addition, hardware, software  
15 or applications we procure from third parties may contain defects in design or  
16 manufacture or other problems that could unexpectedly compromise network and data  
17 security. Security breaches or unauthorized access have resulted in and may in the future  
18 result in a combination of significant legal and financial exposure, increased remediation  
19 and other costs, damage to our reputation and a loss of confidence in the security of our  
20 products, services and networks that could have an adverse effect on our business. We  
21 take steps to prevent unauthorized access to our corporate systems, however, because the  
22 techniques used to obtain unauthorized access, disable or degrade service, or sabotage  
23 systems change frequently or may be designed to remain dormant until a triggering event,  
24 we may be unable to anticipate these techniques or implement adequate preventative  
25 measures. If an actual or perceived breach of our security occurs, the market perception  
26 of the effectiveness of our security measures could be harmed and we could lose users  
27 and customers.

28 44. The Q1 2015 10-Q contained signed certifications pursuant to SOX by the Individual  
Defendants, stating that the financial information contained in the Q1 2015 10-Q was accurate and  
disclosed any material changes to the Company's internal control over financial reporting.

45. On August 7, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,  
announcing the Company's financial and operating results for the quarter ended June 30, 2015 (the "Q2  
2015 10-Q"). For the quarter, Yahoo announced a net loss of \$21.55 million, or \$0.02 per diluted

1 share, on revenue of \$1.24 billion, compared to net income of \$269.71 million, or \$0.26 per diluted  
2 share, on revenue of \$1.08 billion for the same period in the prior year.

3 46. In the Q2 2015 10-Q, with respect to the efficacy of the Company's encryption of user  
4 data, Yahoo simply stated, in part:

5 ***If our security measures are breached, our products and services may be perceived as***  
6 ***not being secure, users and customers may curtail or stop using our products and***  
7 ***services, and we may incur significant legal and financial exposure.***

8 Our products and services involve the storage and transmission of Yahoo's users' and  
9 customers' personal and proprietary information in our facilities and on our equipment,  
10 networks and corporate systems. Security breaches expose us to a risk of loss of this  
11 information, litigation, remediation costs, increased costs for security measures, loss of  
12 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
13 fraudulently induce employees, users, or customers to disclose sensitive information to  
14 gain access to our data or our users' or customers' data. In addition, hardware, software  
15 or applications we procure from third parties may contain defects in design or  
16 manufacture or other problems that could unexpectedly compromise network and data  
17 security. Security breaches or unauthorized access have resulted in and may in the future  
18 result in a combination of significant legal and financial exposure, increased remediation  
19 and other costs, damage to our reputation and a loss of confidence in the security of our  
20 products, services and networks that could have an adverse effect on our business. We  
21 take steps to prevent unauthorized access to our corporate systems, however, because the  
22 techniques used to obtain unauthorized access, disable or degrade service, or sabotage  
23 systems change frequently or may be designed to remain dormant until a triggering event,  
24 we may be unable to anticipate these techniques or implement adequate preventative  
25 measures. If an actual or perceived breach of our security occurs, the market perception  
26 of the effectiveness of our security measures could be harmed and we could lose users  
27 and customers.  
28

47. The Q2 2015 10-Q contained signed certifications pursuant to SOX by the Individual  
Defendants, stating that the financial information contained in the Q2 2015 10-Q was accurate and  
disclosed any material changes to the Company's internal control over financial reporting.

48. On November 5, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,  
announcing the Company's financial and operating results for the quarter ended September 30, 2015  
(the "Q3 2015 10-Q"). For the quarter, Yahoo announced net income of \$76.26 million, or \$0.08 per

1 diluted share, on revenue of \$1.23 billion, compared to net income of \$6.77 billion, or \$6.70 per diluted  
2 share, on revenue of \$1.15 billion for the same period in the prior year.

3 49. In the Q3 2015 10-Q, with respect to the efficacy of the Company's encryption of user  
4 data, Yahoo simply stated, in part:

5 *If our security measures are breached, our products and services may be perceived as*  
6 *not being secure, users and customers may curtail or stop using our products and*  
7 *services, and we may incur significant legal and financial exposure.*

8 Our products and services involve the storage and transmission of Yahoo's users' and  
9 customers' personal and proprietary information in our facilities and on our equipment,  
10 networks and corporate systems. Security breaches expose us to a risk of loss of this  
11 information, litigation, remediation costs, increased costs for security measures, loss of  
12 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
13 fraudulently induce employees, users, or customers to disclose sensitive information to  
14 gain access to our data or our users' or customers' data. In addition, hardware, software  
15 or applications we procure from third parties may contain defects in design or  
16 manufacture or other problems that could unexpectedly compromise network and data  
17 security. Security breaches or unauthorized access have resulted in and may in the future  
18 result in a combination of significant legal and financial exposure, increased remediation  
19 and other costs, damage to our reputation and a loss of confidence in the security of our  
20 products, services and networks that could have an adverse effect on our business. We  
21 take steps to prevent unauthorized access to our corporate systems, however, because the  
22 techniques used to obtain unauthorized access, disable or degrade service, or sabotage  
23 systems change frequently or may be designed to remain dormant until a triggering event,  
24 we may be unable to anticipate these techniques or implement adequate preventative  
25 measures. If an actual or perceived breach of our security occurs, the market perception  
26 of the effectiveness of our security measures could be harmed and we could lose users  
27 and customers.

28 50. The Q3 2015 10-Q contained signed certifications pursuant to SOX by the Individual  
Defendants, stating that the financial information contained in the Q3 2015 10-Q was accurate and  
disclosed any material changes to the Company's internal control over financial reporting.

51. On February 29, 2016, Yahoo filed an Annual Report on Form 10-K with the SEC,  
announcing the Company's financial and operating results for the quarter and year ended December 31,  
2015 (the "2015 10-K"). For the quarter, Yahoo announced a net loss of \$4.43 billion, or \$4.70 per  
diluted share, on revenue of \$1.27 billion, compared to net income of \$166.34 million, or \$0.17 per



1 diluted share, on revenue of \$1.25 billion for the same period in the prior year. For 2015, Yahoo  
2 announced a net loss of \$4.34 billion, or \$4.64 per diluted share, on revenue of \$4.97 billion, compared  
3 to net income of \$7.52 billion, or \$7.45 per diluted share, on revenue of \$4.62 billion for 2014.

4 52. In the 2015 10-K, with respect to the efficacy of the Company's encryption of user data,  
5 Yahoo simply stated, in part:

6  
7 ***If our security measures are breached, our products and services may be perceived as***  
8 ***not being secure, users and customers may curtail or stop using our products and***  
9 ***services, and we may incur significant legal and financial exposure.***

10 Our products and services involve the storage and transmission of Yahoo's users' and  
11 customers' personal and proprietary information in our facilities and on our equipment,  
12 networks and corporate systems. Security breaches expose us to a risk of loss of this  
13 information, litigation, remediation costs, increased costs for security measures, loss of  
14 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
15 fraudulently induce employees, users, or customers to disclose sensitive information to  
16 gain access to our data or our users' or customers' data. In addition, hardware, software  
17 or applications we procure from third parties may contain defects in design or  
18 manufacture or other problems that could unexpectedly compromise network and data  
19 security. Additionally, some third parties, such as our distribution partners, service  
20 providers and vendors, and app developers, may receive or store information provided by  
21 us or by our users through applications integrated with Yahoo. If these third parties fail to  
22 adopt or adhere to adequate data security practices, or in the event of a breach of their  
23 networks, our data or our users' data may be improperly accessed, used or disclosed.  
24 Security breaches or unauthorized access have resulted in and may in the future result in  
25 a combination of significant legal and financial exposure, increased remediation and  
26 other costs, damage to our reputation and a loss of confidence in the security of our  
27 products, services and networks that could have an adverse effect on our business. We  
28 take steps to prevent unauthorized access to our corporate systems, however, because the  
techniques used to obtain unauthorized access, disable or degrade service, or sabotage  
systems change frequently or may be designed to remain dormant until a triggering event,  
we may be unable to anticipate these techniques or implement adequate preventative  
measures. If an actual or perceived breach of our security occurs, the market perception  
of the effectiveness of our security measures could be harmed and we could lose users  
and customers.

53. The 2015 10-K contained signed certifications pursuant to SOX by the Individual  
Defendants, stating that the financial information contained in the 2015 10-K was accurate and  
disclosed any material changes to the Company's internal control over financial reporting.

1           54. On May 10, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,  
2 announcing the Company's financial and operating results for the quarter ended March 31, 2016 (the  
3 "Q1 2016 10-Q"). For the quarter, Yahoo announced a net loss of \$99.23 million, or \$0.10 per diluted  
4 share, on revenue of \$1.09 billion, compared to net income of \$21.20 million, or \$0.02 per diluted  
5 share, on revenue of \$1.23 billion for the same period in the prior year.

6           55. In the Q1 2016 10-Q, with respect to the efficacy of the Company's encryption of user  
7 data, Yahoo simply stated, in part:  
8

9           ***If our security measures are breached, our products and services may be perceived as***  
10 ***not being secure, users and customers may curtail or stop using our products and***  
11 ***services, and we may incur significant legal and financial exposure.***

12           Our products and services involve the storage and transmission of Yahoo's users' and  
13 customers' personal and proprietary information in our facilities and on our equipment,  
14 networks and corporate systems. Security breaches expose us to a risk of loss of this  
15 information, litigation, remediation costs, increased costs for security measures, loss of  
16 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
17 fraudulently induce employees, users, or customers to disclose sensitive information to  
18 gain access to our data or our users' or customers' data. In addition, hardware, software  
19 or applications we procure from third parties may contain defects in design or  
20 manufacture or other problems that could unexpectedly compromise network and data  
21 security. Additionally, some third parties, such as our distribution partners, service  
22 providers and vendors, and app developers, may receive or store information provided by  
23 us or by our users through applications integrated with Yahoo. If these third parties fail to  
24 adopt or adhere to adequate data security practices, or in the event of a breach of their  
25 networks, our data or our users' data may be improperly accessed, used or disclosed.  
26 Security breaches or unauthorized access have resulted in and may in the future result in  
27 a combination of significant legal and financial exposure, increased remediation and  
28 other costs, damage to our reputation and a loss of confidence in the security of our  
products, services and networks that could have an adverse effect on our business. We  
take steps to prevent unauthorized access to our corporate systems, however, because the  
techniques used to obtain unauthorized access, disable or degrade service, or sabotage  
systems change frequently or may be designed to remain dormant until a triggering event,  
we may be unable to anticipate these techniques or implement adequate preventative  
measures. If an actual or perceived breach of our security occurs, the market perception  
of the effectiveness of our security measures could be harmed and we could lose users  
and customers.

1 56. The Q1 2016 10-Q contained signed certifications pursuant to SOX by the Individual  
2 Defendants, stating that the financial information contained in the Q1 2016 10-Q was accurate and  
3 disclosed any material changes to the Company's internal control over financial reporting.

4 57. On July 25, 2016, Verizon formally announced its intent to acquire Yahoo's internet  
5 business for \$4.8 billion.

6 58. On August 8, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,  
7 announcing the Company's financial and operating results for the quarter ended June 30, 2016 (the "Q2  
8 2016 10-Q"). For the quarter, Yahoo announced a net loss of \$439.91 million, or \$0.46 per diluted  
9 share, on revenue of \$1.31 billion, compared to a net loss of \$21.55 million, or \$0.02 per diluted share,  
10 on revenue of \$1.24 billion for the same period in the prior year.  
11

12 59. In the Q2 2016 10-Q, with respect to the efficacy of the Company's encryption of user  
13 data, Yahoo simply stated, in part:  
14

15 ***If our security measures are breached, our products and services may be perceived as***  
16 ***not being secure, users and customers may curtail or stop using our products and***  
17 ***services, and we may incur significant legal and financial exposure.***

18 Our products and services involve the storage and transmission of Yahoo's users' and  
19 customers' personal and proprietary information in our facilities and on our equipment,  
20 networks and corporate systems. Security breaches expose us to a risk of loss of this  
21 information, litigation, remediation costs, increased costs for security measures, loss of  
22 revenue, damage to our reputation, and potential liability. Outside parties may attempt to  
23 fraudulently induce employees, users, or customers to disclose sensitive information to  
24 gain access to our data or our users' or customers' data. In addition, hardware, software  
25 or applications we procure from third parties may contain defects in design or  
26 manufacture or other problems that could unexpectedly compromise network and data  
27 security. Additionally, some third parties, such as our distribution partners, service  
28 providers and vendors, and app developers, may receive or store information provided by  
us or by our users through applications integrated with Yahoo. If these third parties fail to  
adopt or adhere to adequate data security practices, or in the event of a breach of their  
networks, our data or our users' data may be improperly accessed, used or disclosed.  
Security breaches or unauthorized access have resulted in and may in the future result in  
a combination of significant legal and financial exposure, increased remediation and  
other costs, damage to our reputation and a loss of confidence in the security of our  
products, services and networks that could have an adverse effect on our business. We  
take steps to prevent unauthorized access to our corporate systems, however, because the

1 techniques used to obtain unauthorized access, disable or degrade service, or sabotage  
2 systems change frequently or may be designed to remain dormant until a triggering event,  
3 we may be unable to anticipate these techniques or implement adequate preventative  
4 measures. If an actual or perceived breach of our security occurs, the market perception  
of the effectiveness of our security measures could be harmed and we could lose users  
and customers.

5 60. The Q2 2016 10-Q contained signed certifications pursuant to SOX by the Individual  
6 Defendants, stating that the financial information contained in the Q2 2016 10-Q was accurate and  
7 disclosed any material changes to the Company's internal control over financial reporting.

8 **The Truth Begins to Emerge**

9 61. On September 22, 2016, Yahoo disclosed that hackers had stolen information in late  
10 2014 on more than 500 million accounts. Following the breach, Yahoo executives advised investors  
11 that the breach was not material, in part because the Company had not required to reset their passwords.  
12

13 62. On this news, Yahoo's share price fell \$1.35, or 3.06%, to close at \$42.80 on September  
14 23, 2016.

15 63. On November 9, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,  
16 announcing in full the Company's financial and operating results for the quarter ended September 30,  
17 2016 (the "Q3 2016 10-Q"). For the quarter, Yahoo announced net income of \$162.83 million, or  
18 \$0.17 per diluted share, on revenue of \$1.31 billion, compared to net income of \$76.26 million, or  
19 \$0.08 per diluted share, on revenue of \$1.23 billion for the same period in the prior year.  
20

21 64. In the Q3 2016 10-Q, with respect to the efficacy of the Company's encryption of user  
22 data, Yahoo stated, in part:

23  
24 On September 22, 2016, we disclosed that, based on an ongoing investigation, a copy of  
25 certain user account information for at least 500 million user accounts was stolen from  
26 Yahoo's network in late 2014 (the "Security Incident"). We believe the user account  
27 information was stolen by a state-sponsored actor. The user account information taken  
28 included names, email addresses, telephone numbers, dates of birth, hashed passwords  
(the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security  
questions and answers. Our investigation to date indicates that the stolen information did  
not include unprotected passwords, payment card data, or bank account information.

1 Payment card data and bank account information are not stored in the system that the  
2 investigation found to be affected. Based on the investigation to date, we do not have  
3 evidence that the state-sponsored actor is currently in or accessing the Company's  
4 network.

5 ...

6 ***Our security measures may be breached as they were in the Security Incident and user***  
7 ***data accessed, which may cause users and customers to curtail or stop using our***  
8 ***products and services, and may cause us to incur significant legal and financial***  
9 ***exposure.***

10 Our products and services involve the storage and transmission of Yahoo's users' and  
11 customers' personal and proprietary information in our facilities and on our equipment,  
12 networks, and corporate systems. Yahoo is routinely targeted by outside third parties,  
13 including technically sophisticated and well-resourced state-sponsored actors, attempting  
14 to access or steal our user and customer data or otherwise compromise user accounts. We  
15 believe such a state-sponsored actor was responsible for the theft involved in the Security  
16 Incident. Security breaches or other unauthorized access or actions expose us to a risk of  
17 theft of user data, regulatory actions, litigation, investigations, remediation costs, damage  
18 to our reputation and brand, loss of user and partner confidence in the security of our  
19 products and services and resulting fees, costs, and expenses, loss of revenue, damage to  
20 our reputation, and potential liability. Outside parties may attempt to fraudulently induce  
21 employees, users, partners, or customers to disclose sensitive information or take other  
22 actions to gain access to our data or our users' or customers' data. In addition, hardware,  
23 software, or applications we procure from third parties may contain defects in design or  
24 manufacture or other problems that could unexpectedly compromise network and data  
25 security. In addition, our or our partners' implementation of software may contain  
26 security vulnerabilities or may not be implemented properly due to human error or  
27 limitations in our systems. Additionally, some third parties, such as our distribution  
28 partners, service providers, vendors, and app developers, may receive or store  
information provided by us or by our users through applications that are integrated with  
Yahoo properties and services. If these third parties fail to adopt or adhere to adequate  
data security practices, or in the event of a breach of their networks, our data or our users'  
data may be improperly accessed, used, or disclosed. Security breaches or other  
unauthorized access (such as the Security Incident) have resulted in, and may in the  
future result in, a combination of significant legal and financial exposure, increased  
remediation and other costs, damage to our reputation, and a loss of confidence in the  
security of our products, services, and networks that could have a significantly adverse  
effect on our business. We take steps to prevent unauthorized access to our corporate  
systems, however, because the techniques used to obtain unauthorized access, disable or  
degrade service, or sabotage systems change frequently or may be disguised or difficult  
to detect, or designed to remain dormant until a triggering event, we may be unable to  
anticipate these techniques or implement adequate preventative measures. Breaches of  
our security measures, such as the Security Incident, or perceived breaches, have caused  
and may in the future cause, the market perception of the effectiveness of our security  
measures to be harmed and cause us to lose users and customers.

1           65. The Q3 2016 10-Q contained signed certifications pursuant to SOX by the Individual  
2 Defendants, stating that the financial information contained in the Q3 2016 10-Q was accurate and  
3 disclosed any material changes to the Company's internal control over financial reporting.  
4

5           66. The statements referenced in ¶¶ 24-56, 58-60, and 63-65 above were materially false  
6 and/or misleading because they misrepresented and/or failed to disclose the following adverse facts  
7 pertaining to the Company's business, operational and financial results, which were known to  
8 Defendants or recklessly disregarded by them. Specifically, Defendants made false and/or misleading  
9 statements and/or failed to disclose that: (i) Yahoo failed to encrypt its users' personal information  
10 and/or failed to encrypt its users' personal data with an up-to-date and secure encryption scheme; (ii)  
11 consequently, sensitive personal account information from more than 1 billion users was vulnerable to  
12 theft; (iii) a data breach resulting in the theft of personal user data would foreseeably cause a significant  
13 drop in user engagement with Yahoo's websites and services; and (iv) as a result, Yahoo's public  
14 statements were materially false and misleading at all relevant times.  
15

16           67. On December 14, 2016, post-market, post-market, Yahoo announced that it had  
17 uncovered a data breach, stating that data from more than 1 billion user accounts was compromised in  
18 August 2013. In a press release and Current Report filed with the SEC on Form 8-K, Yahoo stated, in  
19 part:  
20

21           SUNNYVALE, Calif., December 14, 2016— Yahoo! Inc. (NASDAQ:YHOO) has  
22 identified data security issues concerning certain Yahoo user accounts. Yahoo has taken  
23 steps to secure user accounts and is working closely with law enforcement.

24           As Yahoo previously disclosed in November, law enforcement provided the company  
25 with data files that a third party claimed was Yahoo user data. The company analyzed this  
26 data with the assistance of outside forensic experts and found that it appears to be Yahoo  
27 user data. Based on further analysis of this data by the forensic experts, ***Yahoo believes  
an unauthorized third party, in August 2013, stole data associated with more than one  
billion user accounts.*** The company has not been able to identify the intrusion associated  
28 with this theft. Yahoo believes this incident is likely distinct from the incident the  
company disclosed on September 22, 2016.

1        *For potentially affected accounts, the stolen user account information may have*  
2        *included names, email addresses, telephone numbers, dates of birth, hashed passwords*  
3        *(using MD5) and, in some cases, encrypted or unencrypted security questions and*  
4        *answers.* The investigation indicates that the stolen information did not include  
5        passwords in clear text, payment card data, or bank account information. Payment card  
6        data and bank account information are not stored in the system the company believes was  
7        affected.

8        *Yahoo is notifying potentially affected users and has taken steps to secure their*  
9        *accounts, including requiring users to change their passwords. Yahoo has also*  
10        *invalidated unencrypted security questions and answers so that they cannot be used to*  
11        *access an account.*

12        Separately, Yahoo previously disclosed that its outside forensic experts were  
13        investigating the creation of forged cookies that could allow an intruder to access users'  
14        accounts without a password. Based on the ongoing investigation, the company believes  
15        an unauthorized third party accessed the company's proprietary code to learn how to  
16        forge cookies. The outside forensic experts have identified user accounts for which they  
17        believe forged cookies were taken or used. Yahoo is notifying the affected account  
18        holders, and has invalidated the forged cookies. The company has connected some of this  
19        activity to the same state-sponsored actor believed to be responsible for the data theft the  
20        company disclosed on September 22, 2016.

21        (Emphases added.)

22        68.     On this news, Yahoo's share price fell \$2.50, or 6.11%, to close at \$38.41 on December  
23        15, 2016.

24        69.     On December 15, 2016, after the market closed, the *Wall Street Journal* published an  
25        article entitled "Yahoo's Password Move May Put Verizon Deal at Risk." The article stated, in part:

26        Yahoo Inc.'s move to force some users to reset their passwords following a newly  
27        disclosed security breach could disrupt the planned sale of its core assets to Verizon  
28        Communications Inc., security experts say.

29        Yahoo didn't force users to reset their passwords after its September disclosure of  
30        another breach. *Experts say forcing users to reset their passwords typically causes some*  
31        *to drop a service.*

32        That is one reason why the newly disclosed hack—which Yahoo says occurred in 2013  
33        and affected more than one billion accounts—could prove more disruptive to Verizon's  
34        pending \$4.83 billion acquisition of Yahoo's core assets.

35        ...

1 *Yahoo is forcing users to reset their passwords now because some of the material taken*  
2 *in the 2013 breach wasn't encrypted, and other parts were protected by what is now*  
3 *considered an outdated encryption scheme*, according to a person familiar with that  
matter.

(Emphases added.)

4 70. On January 23, 2017, the *Wall Street Journal* reported that the SEC had opened an  
5 investigation into the timing of Yahoo's disclosures regarding the data breaches. The article reported,  
6 in part:

7  
8 The Securities and Exchange Commission has opened an investigation, and in December  
9 issued requests for documents, as it looks into whether the tech company's disclosures  
10 about the cyberattacks complied with civil securities laws, the people said. The SEC  
requires companies to disclose cybersecurity risks as soon as they are determined to have  
an effect on investors.

11 The investigation is likely to center on a 2014 data breach at Yahoo that compromised the  
12 data of at least 500 million users, according to the people familiar with the matter. Yahoo  
13 disclosed that breach in September 2016, despite having linked the incident to state-  
sponsored hackers two years earlier.

14 To date, Yahoo hasn't explained why the company took two years to disclose the 2014  
15 incident publicly or who made the decision not to go public sooner with this information.  
16 In mid-December Yahoo also said it had recently discovered an August 2013 data breach  
that had exposed the private information of more than 1 billion Yahoo users.

17 71. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in  
18 the market value of the Company's common shares, Plaintiff and other Class members have suffered  
19 significant losses and damages.

#### 21 **PLAINTIFF'S CLASS ACTION ALLEGATIONS**

22 72. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure  
23 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased or otherwise acquired  
24 Yahoo common shares traded on the NASDAQ during the Class Period (the "Class"); and were  
25 damaged upon the revelation of the alleged corrective disclosures. Excluded from the Class are  
26 Defendants herein, the officers and directors of the Company, at all relevant times, members of their  
27  
28



1 immediate families and their legal representatives, heirs, successors or assigns and any entity in which  
2 Defendants have or had a controlling interest.

3 73. The members of the Class are so numerous that joinder of all members is impracticable.  
4 Throughout the Class Period, Yahoo common shares were actively traded on the NASDAQ. While the  
5 exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through  
6 appropriate discovery, Plaintiff believes that there are hundreds or thousands of members in the  
7 proposed Class. Record owners and other members of the Class may be identified from records  
8 maintained by Yahoo or its transfer agent and may be notified of the pendency of this action by mail,  
9 using the form of notice similar to that customarily used in securities class actions.  
10

11 74. Plaintiff's claims are typical of the claims of the members of the Class as all members of  
12 the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is  
13 complained of herein.  
14

15 75. Plaintiff will fairly and adequately protect the interests of the members of the Class and  
16 has retained counsel competent and experienced in class and securities litigation. Plaintiff has no  
17 interests antagonistic to or in conflict with those of the Class.  
18

19 76. Common questions of law and fact exist as to all members of the Class and predominate  
20 over any questions solely affecting individual members of the Class. Among the questions of law and  
21 fact common to the Class are:

- 22 • whether the federal securities laws were violated by Defendants' acts as alleged  
23 herein;
- 24 • whether statements made by Defendants to the investing public during the Class  
25 Period misrepresented material facts about the financial condition, business,  
26 operations, and management of Yahoo;
- 27 • whether Defendants caused Yahoo to issue false and misleading financial  
28 statements during the Class Period;

- 1 • whether Defendants acted knowingly or recklessly in issuing false and misleading financial statements;
- 2 • whether the prices of Yahoo securities during the Class Period were artificially inflated because of Defendants' conduct complained of herein; and
- 3 • whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

4  
5  
6 77. A class action is superior to all other available methods for the fair and efficient  
7 adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the  
8 damages suffered by individual Class members may be relatively small, the expense and burden of  
9 individual litigation make it impossible for members of the Class to individually redress the wrongs  
10 done to them. There will be no difficulty in the management of this action as a class action.

11  
12 78. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-  
13 the-market doctrine in that:

- 14 • Defendants made public misrepresentations or failed to disclose material facts during the Class Period;
- 15 • the omissions and misrepresentations were material;
- 16 • Yahoo common shares are traded in efficient markets;
- 17 • the Company's shares were liquid and traded with moderate to heavy volume during the Class Period;
- 18 • the Company traded on the NASDAQ, and was covered by multiple analysts;
- 19 • the misrepresentations and omissions alleged would tend to induce a reasonable investor to misjudge the value of the Company's common shares; and
- 20 • Plaintiff and members of the Class purchased and/or sold Yahoo common shares between the time the Defendants failed to disclose or misrepresented material facts and the time the true facts were disclosed, without knowledge of the omitted or misrepresented facts.

21  
22  
23  
24  
25  
26  
27 79. Based upon the foregoing, Plaintiff and the members of the Class are entitled to a  
28 presumption of reliance upon the integrity of the market.

1 80. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of  
2 reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United*  
3 *States*, 406 U.S. 128, 92 S. Ct. 2430 (1972), as Defendants omitted material information in their Class  
4 Period statements in violation of a duty to disclose such information, as detailed above.

5 **COUNT I**

6 **Violation of Section 10(b) of The Exchange Act and Rule 10b-5**  
7 **Against All Defendants**

8 81. Plaintiff repeats and realleges each and every allegation contained above as if fully set  
9 forth herein.

10 82. This Count is asserted against Yahoo and the Individual Defendants and is based upon  
11 Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the  
12 SEC.  
13

14 83. During the Class Period, Yahoo and the Individual Defendants, individually and in  
15 concert, directly or indirectly, disseminated or approved the false statements specified above, which  
16 they knew or deliberately disregarded were misleading in that they contained misrepresentations and  
17 failed to disclose material facts necessary in order to make the statements made, in light of the  
18 circumstances under which they were made, not misleading.  
19

20 84. Yahoo and the Individual Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in  
21 that they:

- 22
- 23 • employed devices, schemes and artifices to defraud;
  - 24 • made untrue statements of material facts or omitted to state material facts  
25 necessary in order to make the statements made, in light of the circumstances  
26 under which they were made, not misleading; or
  - 27 • engaged in acts, practices and a course of business that operated as a fraud or  
28 deceit upon plaintiff and others similarly situated in connection with their  
purchases of Yahoo common shares during the Class Period.

1 85. Yahoo and the Individual Defendants acted with scienter in that they knew that the  
2 public documents and statements issued or disseminated in the name of Yahoo were materially false  
3 and misleading; knew that such statements or documents would be issued or disseminated to the  
4 investing public; and knowingly and substantially participated, or acquiesced in the issuance or  
5 dissemination of such statements or documents as primary violations of the securities laws. These  
6 Defendants by virtue of their receipt of information reflecting the true facts of Yahoo, their control  
7 over, and/or receipt and/or modification of Yahoo allegedly materially misleading statements, and/or  
8 their associations with the Company which made them privy to confidential proprietary information  
9 concerning Yahoo, participated in the fraudulent scheme alleged herein.  
10

11 86. Individual Defendants, who are the senior officers and/or directors of the Company, had  
12 actual knowledge of the material omissions and/or the falsity of the material statements set forth above,  
13 and intended to deceive Plaintiff and the other members of the Class, or, in the alternative, acted with  
14 reckless disregard for the truth when they failed to ascertain and disclose the true facts in the statements  
15 made by them or other Yahoo personnel to members of the investing public, including Plaintiff and the  
16 Class.  
17

18 87. As a result of the foregoing, the market price of Yahoo common shares was artificially  
19 inflated during the Class Period. In ignorance of the falsity of Yahoo's and the Individual Defendants'  
20 statements, Plaintiff and the other members of the Class relied on the statements described above and/or  
21 the integrity of the market price of Yahoo common shares during the Class Period in purchasing Yahoo  
22 common shares at prices that were artificially inflated as a result of Yahoo's and the Individual  
23 Defendants' false and misleading statements.  
24

25 88. Had Plaintiff and the other members of the Class been aware that the market price of  
26 Yahoo common shares had been artificially and falsely inflated by Yahoo's and the Individual  
27 Defendants' misleading statements and by the material adverse information which Yahoo's and the  
28

1 Individual Defendants did not disclose, they would not have purchased Yahoo's common shares at the  
2 artificially inflated prices that they did, or at all.

3 89. As a result of the wrongful conduct alleged herein, Plaintiff and other members of the  
4 Class have suffered damages in an amount to be established at trial.

5 90. By reason of the foregoing, Yahoo and the Individual Defendants have violated Section  
6 10(b) of the 1934 Act and Rule 10b-5 promulgated thereunder and are liable to the plaintiff and the  
7 other members of the Class for substantial damages which they suffered in connection with their  
8 purchase of Yahoo common shares during the Class Period.  
9

10 **COUNT II**

11 **Violation of Section 20(a) of The Exchange Act**  
12 **Against The Individual Defendants**

13 91. Plaintiff repeats and realleges each and every allegation contained in the foregoing  
14 paragraphs as if fully set forth herein.

15 92. During the Class Period, the Individual Defendants participated in the operation and  
16 management of Yahoo, and conducted and participated, directly and indirectly, in the conduct of  
17 Yahoo's business affairs. Because of their senior positions, they knew the adverse non-public  
18 information regarding the Company's inadequate internal safeguards in data security protocols.  
19

20 93. As officers and/or directors of a publicly owned company, the Individual Defendants had  
21 a duty to disseminate accurate and truthful information with respect to Yahoo's financial condition and  
22 results of operations, and to correct promptly any public statements issued by Yahoo which had become  
23 materially false or misleading.  
24

25 94. Because of their positions of control and authority as senior officers, the Individual  
26 Defendants were able to, and did, control the contents of the various reports, press releases and public  
27 filings which Yahoo disseminated in the marketplace during the Class Period. Throughout the Class  
28

1 Period, the Individual Defendants exercised their power and authority to cause Yahoo to engage in the  
2 wrongful acts complained of herein. The Individual Defendants therefore, were “controlling persons” of  
3 Yahoo within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in  
4 the unlawful conduct alleged which artificially inflated the market price of Yahoo common shares.

5 95. By reason of the above conduct, the Individual Defendants are liable pursuant to Section  
6 20(a) of the Exchange Act for the violations committed by Yahoo.  
7

8 **PRAYER FOR RELIEF**

9 WHEREFORE, Plaintiff demands judgment against Defendants as follows:

10 A. Determining that the instant action may be maintained as a class action under Rule 23 of  
11 the Federal Rules of Civil Procedure, and certifying Plaintiff as the Class representative;

12 B. Requiring Defendants to pay damages sustained by Plaintiff and the Class by reason of  
13 the acts and transactions alleged herein;

14 C. Awarding Plaintiff and the other members of the Class prejudgment and post- judgment  
15 interest, as well as their reasonable attorneys’ fees, expert fees and other costs; and  
16

17 D. Awarding such other and further relief as this Court may deem just and proper.  
18

19 **DEMAND FOR TRIAL BY JURY**

20 Plaintiff hereby demands a trial by jury.

21 Dated: January 24, 2017

22 Respectfully submitted,

23 **POMERANTZ LLP**

24 By: /s/ Jennifer Pafiti  
25 Jennifer Pafiti (SBN 282790)  
26 468 North Camden Drive  
27 Beverly Hills, CA 90210  
28 Telephone: (818) 532-6499  
E-mail: jpafiti@pomlaw.com

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**POMERANTZ, LLP**

Jeremy A. Lieberman  
J. Alexander Hood II  
Hui M. Chang  
600 Third Avenue, 20th Floor  
New York, New York 10016  
Telephone: (212) 661-1100  
Facsimile: (212) 661-8665  
E-mail: jalieberman@pomlaw.com  
E-mail: ahood@pomlaw.com  
E-mail: hchang@pomlaw.com

**POMERANTZ LLP**

Patrick V. Dahlstrom  
Ten South La Salle Street, Suite 3505  
Chicago, Illinois 60603  
Telephone: (312) 377-1181  
Facsimile: (312) 377-1184  
E-mail: pdahlstrom@pomlaw.com

**GOLDBERG LAW PC**

Michael Goldberg  
Brian Schall  
1999 Avenue of the Stars  
Los Angeles, California 90067  
Suite 1100  
Telephone: 1-800-977-7401  
Fax: 1-800-536-0065  
Email: michael@goldberglawpc.com  
Email: brian@goldberglawpc.com

*Attorneys for Plaintiff*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO

JAMES GRAHAM, Derivatively on Behalf of  
Nominal Defendant, THE WENDY'S COMPANY,

Plaintiffs,

vs.

NELSON PELTZ, PETER W. MAY, EMIL J.  
BROLICK, CLIVE CHAJET, EDWARD P.  
GARDEN, JANET HILL, JOSEPH A. LEVATO,  
J. RANDOLPH LEWIS, PETER H.  
ROTHSCHILD, DAVID E. SCHWAB II,  
ROLAND C. SMITH, RAYMOND S. TROUBH,  
JACK G. WASSERMAN, MICHELLE "MICH"  
J. MATHEWS-SPRADLIN, DENNIS M. KASS,  
MATTHEW PELTZ, TODD A. PENEGOR and  
ROBERT D. WRIGHT,

Defendants,

and

THE WENDY'S COMPANY,

Nominal Defendant.

CASE NO.: 1:16-cv-1153

**VERIFIED SHAREHOLDER  
DERIVATIVE COMPLAINT**  
(JURY TRIAL DEMANDED)

**INTRODUCTION**

Plaintiff James Graham ("Plaintiff"), by and through his undersigned attorneys, submits this Verified Shareholder Derivative Complaint (the "Complaint") against defendants named herein. Plaintiff alleges the following based upon information and belief, except as to those allegations concerning Plaintiff, which are alleged upon personal knowledge. Plaintiff's information and belief is based upon, among other things, the investigation conducted by and under the supervision of his counsel which included, among other things: (a) a review and analysis of regulatory filings filed by The Wendy's Company ("Wendy's" or the "Company")

with the United States Securities and Exchange Commission (“SEC”); (b) a review and analysis of press releases and media reports issued and disseminated by Wendy’s; (c) a review of other publicly available information concerning Wendy’s, including articles in the news media and analyst reports; and (d) complaints and related materials in litigation commenced against some or all of the Individual Defendants and/or the Company.

### **SUMMARY OF THE ACTION**

1. This is a shareholder’s derivative action brought for the benefit of Nominal Defendant Wendy’s. Wendy’s is the world’s third largest quick-service restaurant company in the hamburger sandwich segment. Wendy’s is primarily engaged in the business of operating, developing and franchising a system of distinctive quick-service restaurants serving high quality food. It maintains over 6,000 Wendy’s establishments in North America, with a majority franchisee owned and approximately 600 corporate owned. It also has over 400 franchised locations outside North America.

2. This derivative action is brought against certain members of the Company’s Board of Directors (the “Board”) and certain of its executive officers (collectively, the “Individual Defendants”) seeking to remedy the Defendants’ violations of state law and breaches of fiduciary duty during the period beginning October 1, 2012 through the present (the “Relevant Period”).

3. The Individual Defendants’ violations of state law and breaches of fiduciary duty arise out of a data breach that compromised its customers’ personal and financial information that stretched from October 2015 through June 2016 and affected well over 1,000 Wendy’s franchise locations. Wendy’s first reported the Data Breach in January 2016 on the heels of a report issued by noted security blogger Brian Krebs and stated that they had immediately began

an investigation. The Company provided an update on February 9, 2016, informing the public that cybersecurity experts found malware on some of the systems. The Company repeated this same disclosure in its 2015 Form 10-K filed with the SEC on March 3, 2016.

4. Then on May 11, 2016, the Company filed its Form 10-Q for the quarter ended April 3, 2016, and publicly disclosed some additional details about the Data Breach. Wendy's claimed that it believed that malware, installed through the use of compromised third-party credentials, affected one particular point of sale system at fewer than 300 of the approximate 5,500 franchise locations and that the Company's chosen point-of-sale ("POS") system, the Aloha POS system, installed at both corporate owned stores and at a majority of the franchise stores, had not been impacted by the Data Breach. Things got worse.

5. On June 9, 2016, Wendy's issued a press release disclosing that the earlier representations regarding the limited scope of the Data Breach was only the tip of the iceberg. The press release reported that an additional variant of the malware was discovered, and that it had affected a different POS system involving substantially more than the 300 stores already implicated in the Data Breach. As admitted by Wendy's, the Data Breach ran from October 2015 until June 2016, and although discovered in late January 2016, ran unabated for almost an additional six months. Further, in the June 9, 2016 press release, Wendy's did not deny that its chosen POS system for its corporate owned and franchisee stores, the Aloha POS system, had not been implicated in the Data Breach. To this day, the Company has failed to come clean and admit that the Aloha POS system had also been affected by the Data Breach.

6. Further, the Aloha POS system had been mandated for use by Wendy franchisees beginning in October 2012 with a deadline of July 1, 2014 for installation. The Aloha POS system proved fraught with defects from the very beginning and the deadline for installation was

delayed until July 1, 2015, and then again until March 31, 2016, though not all restaurants are required to have the Aloha POS system installed until at least December 31, 2016. It is alleged by one of Wendy's franchisees having over 150 stores that it is unlikely that the December 31, 2016 deadline will be met. And according to this same franchisee, some Wendy's restaurants will never have to install the Aloha POS system.

7. In addition, Plaintiff has not made a demand on Wendy's Board of Directors. Wendy's admits that certain defendants own a substantial amount of Company stock evidencing a controlling interest in the Company. As conceded by the Company, this concentration of ownership gives these defendants "significant influence over the outcome of actions requiring stockholder approval, including the election of directors and the approval of mergers, consolidations and the sale of all or substantially all of the Company's assets." These controlling shareholder defendants also have familial ties with other of the Individual Defendants. Further, other of the Individual Defendants worked at entities other than Wendy's with the controlling shareholder defendants, or were previously management employees at the Company and now are directors beholden to the controlling shareholder defendants. As described in detail in ¶¶ 137-166, for these and other reasons set forth therein, demand would be futile.

8. As a result of the foregoing, the Company is now subjected to a series of class action lawsuits that have been consolidated into two distinct groups: (i) on behalf of financial institutions alleging claims for negligence, negligence per se, violation of the Ohio Deceptive Trade Practices Act, declaratory and injunctive relief (the "Financial Institution Class Action"); and (ii) on behalf of customers of Wendy's alleging claims for breach of implied contract, negligence, violations of state consumer protection laws and violations of state data breach statutes (the "Consumer Class Action"). The cases are currently pending in the United States

District Court for the Western District of Pennsylvania and the United States District Court for the Middle District of Florida, respectively.<sup>1</sup>

9. The Individual Defendants breached their duties of loyalty, care and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures with respect to data security for the Company and its franchisees; (ii) failing to exercise their oversight duties by not monitoring the Company and its franchisees' compliance with federal and state laws, payment card industry regulations and its agreements with payment card processors and networks; (iii) failing to cause the Company to make full and fair disclosure concerning (a) the effectiveness of the Company and its franchisees' policies and procedures with respect to data security, and (b) the scope and impact of the Data Breach, resulting in the commencement of the Financial Institutions Class Action and Consumer Class Action; (iv) permitting the Company to violate the Payment Card Industry Data Security Standards ("PCI DSS") by, among other things, (a) allowing Wendy's and many of its franchisees to use the Aloha POS system that the Company knew was fraught with vulnerabilities; (b) failing to ensure that the Company installed and maintained an adequate firewall; (c) failing to ensure that payment card data was properly segmented from the remainder of Wendy's network; (d) failing to implement necessary protocols, such as software image hardening, password protecting programs that captured payment card data and encrypting payment card data at the point-of-sale; and (e) failing to upgrade the Company's systems to utilize EMV technology; (v) consciously disregarding the systemic and pervasive problems with the Aloha POS system; (vi) consciously permitting the Company to maintain an out of date operating system; and

---

<sup>1</sup> The consolidated cases are docketed at: *First Choice Federal Credit Union et al., v. The Wendy's Company et al.*, Case No.: 2:16-cv-00506 (W.D. PA), and *Jonathan Torres et al. v. Wendy's International LLC*, Case No. 6:16-cv-00210 (M.D. FL).

(vii) failing to exercise their oversight duties commensurate with the risk, given the recognition by senior management and the Board that a security breach could adversely affect the Company's business and operations, as evidenced by the fact that the Data Breach went undetected for several months and, it was not until after receiving questions from a third-party concerning banking industry sources who discovered a pattern of fraud on cards that were used at various Wendy's locations that the Company even publicly acknowledged that it was investigating claims of a possible credit card breach at some locations.

### **JURISDICTION AND VENUE**

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332. There is complete diversity among the parties and the amount in controversy exceeds the sum or value of \$75,000, exclusive of interest and costs.

11. This Court has jurisdiction over each Defendant named herein because each Defendant is either a corporation that conducts business in and maintains operations in this District, or is an individual who has sufficient minimum contact with this District so as to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

12. Venue is proper in this Court pursuant to 28 U.S.C. §1391(a) because one or more of the defendants either resides in or maintains executive offices in this District, a substantial portion of the transactions and wrongs complained of herein, including defendants' primary participation in the wrongful acts detailed herein and aiding in violation of fiduciary duties owed to Wendy's occurred in this District and defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that have an effect in this District.

**PARTIES**

13. Plaintiff James Graham is currently and has continuously been a stockholder of Wendy's since the beginning of the Relevant Period. Plaintiff is a citizen of Oregon.

14. Nominal Defendant Wendy's is incorporated under the laws of the State of Delaware and maintains its headquarters in Dublin, Ohio. Wendy's is the world's third largest quick-service restaurant company in the hamburger sandwich segment. Wendy's is primarily engaged in the business of operating, developing and franchising a system of distinctive quick-service restaurants serving high quality food. As of January 3, 2016, there were 6,076 Wendy's restaurants in operation in North America. Of these restaurants, 632 were operated by Wendy's and 5,444 by a total of 390 franchisees. Also as of January 3, 2016, there were 403 franchised Wendy's restaurants in operation in 27 countries and territories other than North America. Wendy's shares are listed and traded on the NASDAQ Exchange under the Ticker "WEN."

15. Defendant Nelson Peltz ("N. Peltz") has a long standing relationship with Wendy's as both a member of the Company's Board and as a member of management, as well as being a significant beneficial owner of Wendy's stock. He has served as a director of the Company since April 1993 and has served as non-executive Chairman of the Company since June 2007. Prior to that, N. Peltz served as the Company's Chairman and Chief Executive Officer ("CEO") and as a director or manager and an officer of certain of the Company's subsidiaries from April 1993 through June 2007. N. Peltz has been CEO and a founding partner of Trian Fund Management, L.P. ("Trian Partners"), a management company for various investment funds and accounts, since November 2005. From January 1989 to April 1993, N. Peltz was Chairman and CEO of Trian Group, Limited Partnership, which provided investment banking and management services for entities controlled by N. Peltz and Peter W. May. From

1983 to December 1988, N. Peltz was Chairman and CEO and a director of Triangle Industries, Inc. (“Triangle”), a metals and packaging company. Additionally, as of March 28, 2016, N. Peltz was the beneficial owner of 56,520,516 shares (21%) of the Company’s outstanding common stock. Of the over 56 million shares of Wendy’s stock beneficially owned by N. Peltz, 40,792,537 of those shares are owned by Trian Partners and its affiliates. N. Peltz also serves as a director of Mondelez International, Inc. since January 2014, Sysco Corporation since August 2015 and The Madison Square Garden Company since September 2015. He previously served as a director of H. J. Heinz Company from September 2006 to June 2013, Ingersoll Rand plc from August 2012 to June 2014, Legg Mason, Inc. from October 2009 to December 2014 and MSG Networks Inc. from December 2014 to September 2015. According to the Company’s proxy statement filed on Schedule 14A with the SEC on April 11, 2016 (the “2016 Proxy”), the Company touted that N. Peltz “has developed extensive experience working with management teams and boards of directors, as well as in acquiring, investing in and building companies and implementing operational improvements at the companies with which he has been involved. As result, Mr. Peltz has strong operating experience and strategic planning skills, valuable leadership and corporate governance experience.” Upon information and belief, N. Peltz is a citizen of New York.

16. Defendant Peter W. May (“May”) has a long standing relationship with Wendy’s as both a member of the Company’s Board and as a member of management, as well as being a significant beneficial owner of Wendy’s stock. He has served as a director of the Company since April 1993 and has served as the Company’s non-executive Vice Chairman since June 2007. May served as the President and Chief Operating Officer (“COO”) and as a director or manager and an officer of certain of the Company’s subsidiaries from April 1993 through June 2007.



May has been President and a founding partner of Trian Partners since November 2005. From January 1989 to April 1993, May was President and COO of Trian Group, Limited Partnership. From 1983 to December 1988, he was President and COO and a director of Triangle. As of March 28, 2016, May was the beneficial owner of 56,313,437 (21%) shares of the Company's outstanding common stock. Of the over 56 million shares of Wendy's stock beneficially owned by May, 40,792,537 of those shares are owned by Trian Partners and its affiliates. May has also served as a director of Tiffany & Co. since May 2008. According to the 2016 Proxy, the Company touted that May "has developed extensive experience working with management teams and boards of directors, as well as in acquiring, investing in and building companies and implementing operational improvements at the companies with which he has been involved. As a result, Mr. May has strong operating experience and strategic planning skills, valuable leadership and corporate governance experience." Upon information and belief, May is a citizen of Florida.

17. Defendant Emil J. Brolick ("Brolick") has a long standing relationship with Wendy's as both a member of the Company's Board and as a member of management. He has served as a director of the Company since September 2011. Brolick previously served as President and CEO from September 2011 to January 2016, and as CEO until his retirement from management duties on May 26, 2016. Brolick previously worked at Wendy's International for 12 years from 1988 to 2000, last serving as Senior Vice President of New Product Marketing, Research and Strategic Planning. Brolick was COO of Yum! Brands Inc. and President of two of Yum! Brands' U.S. operating segments, Long John Silver's and A&W All American Food Restaurants, from June 2008 to September 2011. From December 2006 to June 2008, he was President of U.S. Brand Building for Yum! Brands. Prior to that, Brolick served as President and

Chief Concept Officer of Taco Bell Corp., a position he held from July 2000 to November 2006. Upon information and belief, Brolick is a citizen of Ohio.

18. Defendant Janet Hill (“Hill”) is a long time director of the Company. She has served as a director of the Company since September 2008. She previously served as a director of Wendy’s International from 1994 until its merger with the Company in September 2008. Hill also serves as a director of Dean Foods Company since December 2001 and Carlyle Group Management L.L.C., the general partner of the Carlyle Group L.P., since May 2012. Hill previously served as a director of Sprint Nextel Corporation from 2005 to July 2013. She is also a member of the board of directors at two private companies, Echo360, Inc. and Esquire Bank. Upon information and belief, Hill is a citizen of Virginia.

19. Defendant Dennis M. Kass (“Kass”) has served as a director of the Company since December 2015. Kass also serves as an Advisory Partner of Trian Partners, an entity in which defendants N. Peltz, May, and Garden have a controlling interest, and was hired by Trian Partners in January 2015 as a founding member, on the heels of his appointment as a Wendy’s director. As part of his duties at Trian Advisory Partners, Kass may join the Boards of Directors of companies in which Trian Partners invests, such as Wendy’s. Kass also works with defendant M. Peltz, who is a member of the Investment Team of Trian Partners. Upon information and belief, Kass is a citizen of Florida.

20. Defendant Joseph A. Levato (“Levato”) has been either a director and/or member of Wendy’s management since 1993. He has served as a director of the Company since June 1996. Levato served as Executive Vice President (“EVP”) and Chief Financial Officer (“CFO”) of the Company and certain of its subsidiaries from April 1993 to August 1996, when he retired from the Company. Levato worked with defendants N. Peltz and May at Trian Group, Limited

Partnership and Triangle. He was Senior Vice President and Chief Financial Officer of Trian Group, Limited Partnership from January 1992 to April 1993. From 1984 to December 1988, Levato served as Senior Vice President and CFO of Triangle. Upon information and belief, Levato is a citizen of New Jersey.

21. Defendant Michelle “Mich” J. Mathews-Spradlin (“Mathews-Spradlin”) has served as a director of the Company since February 2015. From 1993 until her retirement in 2011, Mathews-Spradlin worked at Microsoft Corporation, where she served as Chief Marketing Officer (“CMO”) and Senior Vice President, Central Marketing Group from 2005 to 2011, Corporate Vice President, Marketing from 2001 to 2005, Vice President, Corporate Public Relations from 1999 to 2001 and head of the Corporate Public Relations function from 1993 to 1999. Prior to her employment at Microsoft, Mathews-Spradlin worked in the United Kingdom as a communications consultant for Microsoft from 1989 to 1993. Prior to that, she held various positions at General Motors Co. from 1986 to 1989. Mathews-Spradlin also serves as a Board member at several private companies, including Bitium, Inc., OANDA Global Corporation, The Bouqs Company and You & Mr. Jones. According to the 2016 Proxy, the Company touts that Mathews-Spradlin “possesses extensive experience in global brand management and a deep understanding of the technology industry attributable to her background as a senior executive at Microsoft Corporation.” Upon information and belief, Mathews-Spradlin is a citizen of California.

22. Defendant Matthew H. Peltz (“M. Peltz”) has served as a director of Wendy’s since December 2015 and is the son of defendant N. Peltz. M. Peltz also works with defendants N. Peltz, May, Kass, and Garden at Trian Partners. He is a Partner and has been a member of the Investment Team of Trian Partners since January 2008. Prior to that, he was with Goldman

Sachs & Co. from May 2006 to January 2008, where he worked as an investment banking analyst and subsequently joined Liberty Harbor, an affiliated multi-strategy hedge fund. M. Peltz previously served as a director of ARG Holding Corporation, the parent company of the Arby's restaurant brand, from September 2012 to December 2015. Upon information and belief, M. Peltz is a citizen of New York.

23. Defendant Todd A. Penegor ("Penegor") has served as a director of the Company since May 2016 and as CEO of the Company since May 27, 2016. Penegor joined the Company in June 2013 and served as the President and CFO of Wendy's from January 2016 to May 2016. Penegor previously served as Executive Vice President, CFO and International from December 2014 to January 2016 and as Senior Vice President and CFO from September 2013 to December 2014. Prior to joining the Company, Penegor worked at Kellogg Company, a global leader in food products, from 2000 to 2013 where he held several key leadership positions, including Vice President of Kellogg Company and President of U.S. Snacks from 2009 to June 2013, Vice President and CFO of Kellogg Europe from 2007 to 2009 and Vice President and CFO of Kellogg USA and Kellogg Snacks from 2002 to 2007. Prior to joining Kellogg, Penegor worked for 12 years at Ford Motor Company in various positions. According to the Company's proxy statement filed on Schedule 14A with the SEC on April 17, 2015 (the "2015 Proxy"), the Company stated that Penegor, "who was promoted from Senior Vice President and Chief Financial Officer to Executive Vice President, Chief Financial Officer and International, took on additional oversight of the Company's International division, in addition to maintaining his existing responsibilities for Finance, Development and Information Technology." Upon information and belief, Penegor is a citizen of South Carolina.

24. Defendant Peter H. Rothschild (“Rothschild”) has served as a director of Wendy’s and its subsidiaries for over a decade. He has been a director of the Company since May 2010 and served as a director of Wendy’s International from March 2006 until its merger with the Company in September 2008. Rothschild previously served as a director of Deerfield Capital Corp., predecessor to CIFC Corp., from December 2004 to April 2011 and as Interim Chairman of Deerfield Capital’s Board of directors from April 2007 to April 2011. Upon information and belief, Rothschild is a citizen of New York.

25. Defendant Clive Chajet (“Chajet”) was a director of the Company for almost a decade. He served as a director of the Company from June 1994 until his retirement from the Board on May 2014. Upon information and belief, Chajet is a citizen of New York.

26. Defendant Edward P. Garden (“Garden”) has a long standing relationship with Wendy’s as a director and member of management. He served as a director of the Company from December 2004 until his resignation from the Board on December 14, 2015. Garden previously served as Vice Chairman of the Company from December 2004 through June 2007 and as Executive Vice President of the Company from August 2003 until December 2004. Garden works with defendants N. Peltz, May, Kass, and M. Peltz at Trian Partners and is the son-in-law of N. Peltz. He has been Chief Investment Officer and a founding partner of Trian Partners since November 2005. Garden previously served as a director of Trian Acquisition I Corp. from October 2007 to May 2013. He also has served as a director of Family Dollar Stores, Inc. since 2011 and previously served as a director of Chemtura Corporation from January 2007 through March 2009. As of March 28, 2016, Garden was the beneficial owner of 41,032,902 (15.3%) shares of the Company’s outstanding common stock. Of the over 41 million of Wendy’s

stock beneficially owned by Garden, 40, 792,537 of those shares are owned by through Trian Partners and its affiliates. Upon information and belief, Garden is a citizen of Connecticut.

27. Defendant J. Randolph Lewis (“Lewis”) was a director at Wendy’s or its subsidiaries for well over a decade. He served as a director of the Company from September 2008 until his retirement from the Board in May 2016. Lewis previously served as a director of Wendy’s International from 2004 until its merger with the Company in September 2008. Lewis also served as Senior Vice President, Supply Chain and Logistics of Walgreen Co. until his retirement in January 2013. He joined Walgreen Co. in March 1992 as Divisional Vice President, Logistics and Planning and was promoted to Senior Vice President, Supply Chain and Logistics in 1996. Upon information and belief, Lewis is a citizen of Illinois.

28. Defendant David E. Schwab II (“Schwab”) was a director of Wendy’s for over 20 years. He served as a director of the Company from October 1994 until his retirement from the Board in May 2016. Upon information and belief, Schwab is a citizen of New York.

29. Defendant Roland C. Smith (“Smith”) served as a director of the Company from June 2007 until his resignation from the Board in May 2014. Smith previously served as the CEO of the Company from June 2007 to September 2011, as President of the Company from September 2008 to September 2011, and as Special Adviser to the Company from September 2011 to December 2011. Smith also served as CEO of Wendy’s International from September 2008 to September 2011. Smith served as CEO of Arby’s Restaurant Group, Inc. (“Arby’s”) from April 2006 to September 2008, as President of Arby’s from April 2006 to June 2006, and as interim President of Arby’s from January 2010 to May 2010. He currently serves as President and CEO of Delhaize America and as Executive Vice President of Delhaize Group, an international food retailer, positions he has held since October 2012. Previously, Mr. Smith

served as President and CEO of American Golf Corporation and National Golf Properties from February 2003 to November 2005, as President and CEO of AMF Bowling Worldwide, Inc. from April 1999 to January 2003, and as President and as Chief Executive Officer of Arby's, Inc., predecessor to Arby's, from February 1997 to April 1999. He also serves as Chairman of the Board of directors of Carmike Cinemas, Inc. Upon information and belief, Smith is a citizen of Georgia.

30. Defendant Raymond S. Troubh ("Troubh") was a director of Wendy's for almost 20 years. He served as a director of the Company from June 1994 until his retirement from the Board in May 2014. Troubh also serves as a director of Diamond Offshore Drilling, Inc., General American Investors Company and Gentiva Health Services, Inc. Over the course of his career, Troubh has served as a director of over 30 public companies of varying degrees of size and complexity, and has served as chairman of the compensation and audit committee of many of those companies. Upon information and belief, Troubh is a citizen of New York.

31. Defendant Jack G. Wasserman ("Wasserman") was a director at Wendy's for over a decade. He served as a director of the Company from March 2004 until his retirement from the Board in May 2015. Wasserman also serves as a director of Icahn Enterprises G.P., Inc., the general partner of Icahn Enterprises L.P., and previously served as a director of its operating subsidiaries – America Casino & Entertainment Properties LLC, from 2003 until its sale in 2008, and National Energy Group, Inc., from 1998 until its sale in 2006. Upon information and belief, Wasserman is a citizen of New York.

32. Defendant Robert D. Wright ("Wright") has served as Executive Vice President, Chief Operations Officer and International since May 30, 2016. Wright previously served as Executive Vice President, Chief Operations Officer of the Company from December 17, 2014 to

May 30, 2016. Prior to that, Wright served as Chief Operations Officer of the Company from March 10, 2014 to December 17, 2014. According to the 2015 Proxy, the Company stated that “Mr. Wright was promoted to Executive Vice President and Chief Operations Officer and assumed a larger portfolio of customer-facing responsibilities, including in-restaurant technology, restaurant facilities and the continuous improvement of the customer service experience, in addition to maintaining his existing responsibilities for Company and franchise restaurant operations.” According to information and belief, Wright is a citizen of Ohio.

33. Defendants Peltz, May, Brolick, Chajet, Garden, Hill, Levato, Lewis, Rothschild, Schwab, Smith, Wasserman, Mathews-Spradlin, Kass, M. Peltz, Penegor, Troubh and Wright are sometimes collectively referred to herein as the “Individual Defendants.”

34. Defendants Peltz, May, Brolick, Hill, Kass, Levato, Mathews-Spradlin, M. Peltz, Penegor and Rothschild are sometimes collectively referred to herein as the “Current Director Defendants.”

#### **FIDUCIARY DUTIES OF THE INDIVIDUAL DEFENDANTS**

35. By reason of their positions as officers, directors and/or fiduciaries of Wendy’s during the Relevant Period and because of their ability to control the business and corporate affairs of the Company, the Individual Defendants owed Wendy’s and its shareholders fiduciary obligations of good faith, loyalty and candor, and were and are required to use their utmost ability to control and manage the Company in a fair, just, honest and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of Wendy’s and its shareholders so as to benefit all shareholders equally and not in furtherance of their personal interest or benefit.



36. Each director and officer of the Company owes to Wendy's and its shareholders the fiduciary duty to exercise good faith and diligence in the administration of the Company's affairs and in the use and preservation of its property and assets, and the highest obligations of fair dealing.

37. The Individual Defendants, because of their positions of control and authority as directors and/or officers of Wendy's, were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of the various public statements issued by the Company. Due to their positions with Wendy's, each of the Individual Defendants had knowledge of material non-public information regarding the Company.

38. To discharge their duties, the Individual Defendants were required to exercise reasonable and prudent supervision over the management, policies, practices and controls of the Company. By virtue of such duties, the officers and directors of Wendy's were required to, among other things:

- a. Exercise good faith to ensure that the affairs of the Company were conducted in an efficient, business-like manner so as to make it possible to provide the highest quality performance of their business;
- b. Exercise good faith to ensure that the Company was operated in a diligent, honest and prudent manner and complied with all applicable federal, state and foreign laws, rules, regulations and requirements, and all contractual obligations, including acting only within the scope of its legal authority;
- c. Exercise good faith in supervising the preparation, filing and/or dissemination of financial statements, press releases, audits, reports or other information required

- by law, and in examining and evaluating any reports or examinations, audits, or other financial information concerning the financial condition of the Company;
- d. Refrain from unduly benefiting themselves and other Company insiders at the expense of the Company; and
  - e. When put on notice of problems with the Company's business practices and operations, exercise good faith in taking appropriate action to correct the misconduct and prevent its recurrence.

39. Moreover, Wendy's maintains a Code of Conduct and Ethics (the "Code"), which the Company describes is a "guide to legal and ethical behavior," and applies to directors and employees of the Company. With respect to the responsibility of the Board, the Code states the following, in relevant part:

Wendy's expects the members of its Board of Directors at all times to set the right tone by being mindful of their obligations as fiduciaries and by adhering to high standards of conduct, including the policies set out in this Code. Directors should seek to promote those standards in fulfilling their responsibilities to the Company and its stockholders. Directors must adhere to and promote our "open door" policy described above.

Like our employees, *directors are expected to act honestly, in compliance with law and in the best interests of the Company and its stockholders.* They must conduct themselves in a professional manner and act in good faith and with due care. *In their oversight of management, directors should be vigorous in their inquiries and exercise independent judgment to promote the interests of the Company. Directors are also expected to maintain the confidentiality of Company information* and to disclose any possible conflicts of interest that they may have with respect to matters being considered by the Board of Directors or any other aspect of the Company's business.

Any director who has concerns about compliance with this Code should direct his or her inquiry to the Chairman of the Audit Committee of the Board of Directors or to the General Counsel of Wendy's.

(Emphasis added).

34. With respect to legal compliance, the Code states the following, in relevant part:

#### **COMPLIANCE WITH LAW**

Wendy's strives to be an honorable company and employer. Employees must always operate within the law in all business dealings. *It is the Company's express policy that it and its employees obey all applicable U.S. federal, state and local and international laws and regulations.* Employees have a personal responsibility to become familiar and comply with the laws and regulations related to their job responsibilities. There are also other laws – not directly related to an employee's job but of general relevance to work situations – of which employees should be aware. If employees have any questions about what is within the law and what is not, they should seek advice from the Legal Department. Noted below are some of the most important laws that apply to Wendy's and its employees and business dealings.

(Emphasis added).

35. With respect to business conduct, the Code states the following, in relevant part:

#### **BUSINESS CONDUCT AND CONTACTS**

\*\*\*

**Present the Company Truthfully.** Communications should reinforce a sense of trust in the Company. Whether statements are channeled through franchisees, customers, stockholders, the analyst community, suppliers, trade groups, the mass media or made in private conversation, “honesty is the best policy.” *Public statements should be sufficiently candid, clear and complete so that they neither mislead nor lend themselves to misinterpretation.* However, material non-public information may not be disclosed without approval from the Legal Department. *Wendy's is also committed to full compliance with all requirements applicable to its public disclosures and those of Wendy's, including reports filed or furnished to securities regulators by Wendy's. All of our business communications should be timely, clear and accurate.* It is a violation of our policy to misrepresent our financial performance or otherwise compromise the integrity of our financial statements or other disclosures.

All press releases intended for the investor or franchisee communities must first be reviewed and approved by the Legal Department.

(Emphasis added).

36. With respect to Company assets, the Code states the following, in relevant part:

## USE OF COMPANY ASSETS

**Using Company Computers and Other Technology.** Computers and electronic information are essential tools to support our business. . . .

To keep our computer systems and information secure, we need to take necessary actions to safeguard all passwords and identification codes to prevent unauthorized access.

37. With respect to confidential information, the Code states the following, in relevant part:

## CONFIDENTIAL AND PROPRIETARY INFORMATION

**Company Information.** Confidential information includes information regarding the Company's employees, customers . . .

\*\*\*

Examples of personal data include personal, employment, medical, financial and education and training information. Most countries have laws regulating the collection and use of personal data, although the types of data covered, the nature of the protection, and local enforcement mechanisms vary. Wendy's policy is to comply with all such applicable laws. All employees are responsible for ensuring compliance with the data privacy requirements under such laws and regulations and under the Company guidelines and policies. Employees may be required to attend training.

38. With respect to personal information, the Code states the following, in relevant part:

**Franchisee, Supplier or Customer Information.** The nature of Wendy's business gives many employees access to critical business information about franchisees, suppliers and, in some cases, personal information about customers. Maintaining their trust requires that you protect the confidentiality of this information. Information about a franchisee's or supplier's business is confidential as is personal information about customers. Disclosure within the Company should only be on a business "need to know" basis. Disclosure to outsiders, except to comply with legal requirements, is not only inconsistent with this Code but in some cases may also be illegal.

39. Additionally, the Company maintains a set of Corporate Governance Guidelines (amended November 5, 2012) which states the following, in relevant part:

**A. Role of Board and Management:**

The Company's Board of Directors (the "Board"), which is elected by the stockholders, is the ultimate decision-making body of the Company, except with respect to matters reserved to the stockholders. The Board selects the Chief Executive Officer and other senior executives of the Company, who are charged with directing the Company's business. The primary function of the Board, therefore, is oversight—defining and enforcing standards of accountability that enable executive management to execute their responsibilities fully and in the best interests of the Company and its stockholders.

\*\*\*

**C. Conduct:**

\*\*\*

Risk Oversight. The Board provides oversight with respect to the Company's risk assessment and risk management activities, which are designed to identify, prioritize, assess, monitor and mitigate material risks to the Company, including financial, operational, compliance and strategic risks. The Board may from time to time delegate certain aspects of its risk oversight function to one or more of its committees or to members of management as it deems appropriate, each of which shall report directly to the Board.

40. The Company also has an Audit Committee, a Nominating and Corporate Governance Committee, a Compensation Committee and a Performance Compensation Subcommittee, all of which have their own charters setting forth requirements for director qualifications, director responsibilities and director authority.

41. Finally, the Wendy's Board was responsible for risk oversight:

**Board's Role in Risk Oversight**

The Board of Directors provides oversight with respect to the Company's risk assessment and risk management activities, which are designed to identify, prioritize, assess, monitor and mitigate material risks to the Company, including financial, operational, compliance and strategic risks. While *the Board has primary responsibility for risk oversight*, the Board's standing committees support the Board by regularly addressing various risks in their respective areas of responsibility. The Audit Committee focuses on financial risks, including reviewing with management, the Company's internal auditors and the Company's independent registered public accounting firm the Company's major risk exposures (with particular emphasis on financial risk exposures), the adequacy

and effectiveness of the Company's accounting and financial controls and the steps management has taken to monitor and control such exposures, including the Company's risk assessment and risk management policies. The Compensation Committee considers risks presented by the Company's compensation policies and practices for its executive officers and other employees, as discussed below under the caption "Compensation Risk Assessment." The Nominating and Corporate Governance Committee reviews risks related to the Company's corporate governance structure and processes, including director qualifications and independence, stockholder proposals related to governance, succession planning and the effectiveness of our Corporate Governance Guidelines. ***The Board's risk oversight function is also supported by a Risk Oversight Committee composed of members of senior management. The Risk Oversight Committee is exclusively devoted to prioritizing and assessing all categories of enterprise risk, including risks delegated by the Board of Directors to the Board committees, as well as other operational, compliance and strategic risks facing the Company.*** Each of these committees reports directly to the Board.

***The Board believes that its current leadership structure supports the risk oversight function of the Board.*** Having the roles of Chief Executive Officer and Chairman of the Board filled by separate individuals allows the Chief Executive Officer to lead senior management in its supervision of the Company's day-to-day business operations, including the identification, assessment and mitigation of material risks, ***and allows the Chairman to lead the Board in its oversight of the Company's risk assessment and risk management activities.***

(Emphasis added).

42. Each Individual Defendant, by virtue of his or her position as a director and/or officer owed to the Company and to its shareholders the fiduciary duty of loyalty, good faith and the exercise of due care and diligence in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as directors and/or officers of Wendy's, the absence of good faith on their part and a reckless disregard for their duties to the Company and its shareholders that the Individual Defendants were aware or should have been aware posed a risk of serious injury to the Company.

43. The Individual Defendants breached their duties of loyalty, care and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures with respect to data security for the Company and its franchisees; (ii) failing to exercise their oversight duties by not monitoring the Company and its franchisees' compliance with federal and state laws, payment card industry regulations and its agreements with payment card processors and networks; (iii) failing to cause the Company to make full and fair disclosure concerning (a) the effectiveness of the Company and its franchisees' policies and procedures with respect to data security, and (b) the scope and impact of the Data Breach, resulting in the commencement of the Financial Institutions Class Action and Consumer Class Action; (iv) permitting the Company to violate the PCI DSS by, among other things, (a) allowing Wendy's and many of its franchisees to use the Aloha POS system that the Company knew was fraught with vulnerabilities; (b) failing to ensure that the Company installed and maintained an adequate firewall; (c) failing to ensure that payment card data was properly segmented from the remainder of Wendy's network; (d) failing to implement necessary protocols, such as software image hardening, password protecting programs that captured payment card data and encrypting payment card data at the point-of-sale; and (e) failing to upgrade the Company's systems to utilize EMV technology; (v) consciously disregarding the systemic and pervasive problems with the Aloha POS system; (vi) consciously permitting the Company to maintain an out of date operating system; and (vii) failing to exercise their oversight duties commensurate with the risk, given the recognition by senior management and the Board that a security breach could adversely affect the Company's business and operations, as evidenced by the fact that the Data Breach went undetected for several months and, it was not until after receiving questions from a third-party concerning banking industry sources who discovered a pattern of fraud on cards that were

used at various Wendy's locations that the Company even publicly acknowledged that it was investigating claims of a possible credit card breach at some locations.

### **SUBSTANTIVE ALLEGATIONS**

#### ***Background***

44. Wendy's engages in the business of operating, developing, and franchising a system of quick-service restaurants. It is the parent company of its 100% owned subsidiary holding company Wendy's Restaurants, LLC ("Wendy's Restaurants"). Wendy's Restaurants is the parent company of Wendy's International, LLC, formerly known as Wendy's International, Inc. Wendy's International, LLC is the indirect parent company of Quality Is Our Recipe, LLC ("Quality"), which is the owner and franchisor of the Wendy's<sup>®</sup> restaurant system in the United States.

45. Wendy's corporate predecessor was incorporated in Ohio in 1929 and was reincorporated in Delaware in June 1994. Effective September 29, 2008, in conjunction with the merger with Wendy's, the Company's corporate name was changed from Triarc Companies, Inc. ("Triarc") to Wendy's/Arby's Group, Inc. Effective July 5, 2011, in connection with the sale of Arby's Restaurant Group, Inc. ("Arby's"), Wendy's/Arby's Group, Inc. changed its name to The Wendy's Company.

46. As a franchisor, Wendy's has total control over the manner in which its franchisees operate in order to maintain uniformity from restaurant to restaurant. Wendy's standard Uniform Franchise Agreement emphasizes the importance of "uniform standards, specifications, and procedures for operations[,] any aspect of "which may be changed, improved, and further developed by [Wendy's] from time to time[.]" The Unit Franchise



Agreement indicates that Wendy's control over franchisee operations extends to "computer software and electronic data transmission systems for point of sale reporting."

47. Similarly, the Company's 2015 Form 10-K also stated that:

Franchised restaurants are required to be operated under uniform operating standards and specifications relating to the selection, quality and preparation of menu items, signage, décor, equipment, uniforms, suppliers, maintenance and cleanliness of premises and customer service. Wendy's monitors franchisee operations and inspects restaurants periodically to ensure that required practices and procedures are being followed.

***Background on POS attacks***

48. A large portion of Wendy's sales are made to customers who use debit or credit cards. In processing payment card transactions, merchants acquire a substantial amount of information about each customer, including his or her full name; credit or debit card account number; card security code (the value printed on the card or contained in the microprocessor chip or magnetic stripe of a card and used to validate card information during the authorization process); the card's expiration date and verification value; and the PIN number for debit cards. This information typically is stored on the merchants' computer systems and transmitted to third parties to complete the transaction. At other times and for other reasons, merchants also may collect other personally identifiable information about their customers, including but not limited to, financial data, mailing addresses, phone numbers, driver's license numbers, and email addresses.

49. The Individual Defendants were – and at all relevant times have been – aware that the information Wendy's maintains about its customers is highly sensitive and could be used for nefarious purposes by third parties, such as perpetuating identity theft and making fraudulent purchases.

50. The Individual Defendants are – and at all relevant times have been – aware of the importance of safeguarding the Company’s customers’ information and of the foreseeable consequences that would occur if its security systems were breached, specifically including the risk of massive liability to financial institutions and consumers, as well as potential exposure to criminal liability and loss of reputation.

51. Indeed, as early as 2008, Wendy’s identified the potential repercussions of a data security breach as a substantial “Risk Factor” for its business in its annual report and SEC filings, stating: “We rely on computer systems and information technology to run our business. Any material failure, interruption or security breach of our computer systems or information technology may adversely affect the operation of our business and results of operations. We are significantly dependent upon our computer systems and information technology to properly conduct our business. A failure or interruption of computer systems or information technology could result in the loss of data, business interruptions or delays in business operations. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. Any security breach of our computer systems or information technology may result in adverse publicity, loss of sales and profits, penalties or loss resulting from misappropriation of information.”

52. In addition to their general duties to ensure that systems are in place to safeguard customers’ information to prevent the risk of loss, the Individual Defendants were – and at all relevant times have been – obligated to oversee the Company’s compliance with rules governing

payment card transactions, industry standards and various federal and state laws, as well as with the Company's own commitments, internal policies and procedures.

53. Wendy's has continuously acknowledged this legal duty and reassured the public its duty was being met in the Company's "Privacy Policy" posted on its website. For example, the version of the policy in effect on April 29, 2013, told the public that Wendy's "make[s] what [it] believe[s] to be commercially reasonable efforts to provide a reasonable level of security for personal information [the Company is] required to protect."

54. As described below, the Individual Defendants knowingly failed to conduct adequate oversight to ensure that its data security was PCI DSS compliant as required by Wendy's contracts with financial institutions, or meet commercially reasonable efforts for data security as required Wendy's commitment to its customers, as embodied by its Privacy Policy, and once it learned that the Data Breach had occurred knowingly failed to provide timely disclosure to its customers.

***The Individual Defendants Knew that a Security Breach Presented a Significant Threat to Wendy's and They Knew that Wendy's Computer Systems Were Vulnerable to Hackers***

55. Theft of customer data through breaches of retailers' point of sale systems hit the mainstream in 2007, when TJX Companies Inc. ("TJX") admitted in an SEC filing that at least 45.6 million credit and debit card numbers were stolen from its customers over an 18-month period. In addition, TJX disclosed that personal data provided in connection with the return of merchandise without receipts by about 450,000 customers had been stolen. The breach cost the company over \$250 million, including costs related to improving the company's computer system, as well as costs related to lawsuits, investigations and other claims stemming from the breach.

56. Since that time, reports of breaches of major retailers' point of sale systems became commonplace. In 2013, security blogger Brian Krebs of *KrebsonSecurity* broke the news that Target Corporation ("Target"), the nation's second largest retailer, had been the victim of a massive data breach that exposed personal and financial information of more than 110 million customers. According to Krebs, the attackers hacked into Target's systems by using network credentials of a third-party vendor and installed malicious software that infected point-of-sale systems at Target checkout counters. The malware captured the data stored on a payment card's magnetic stripe in the instant after it has been swiped at the terminal and is still in the system's memory, which the thieves can then use to create cloned copies of the payment cards.

57. During the time of the events complained of herein, the Individual Defendants were well-aware that a data security breach such as the Data Breach that occurred from October 2015 to June 2016 was a substantial "Risk Factor" for the Company.

58. Indeed, as early as 2009, Wendy's identified the potential repercussions of a data security breach as a substantial "Risk Factor" for its business in its annual report filed with the SEC on March 13, 2009 (the "2008 10-K"), stating the following, in relevant part:

We rely on computer systems and information technology to run our business. Any material failure, interruption or security breach of our computer systems or information technology may adversely affect the operation of our business and results of operations.

We are significantly dependent upon our computer systems and information technology to properly conduct our business. A failure or interruption of computer systems or information technology could result in the loss of data, business interruptions or delays in business operations. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. Any security breach of our computer systems or information technology may result in adverse publicity, loss of sales and profits, penalties or loss resulting from misappropriation of information.

59. The foregoing risk factor was repeated in Wendy's Form 10-Ks for Fiscal Years 2009, 2010, 2011, 2012, 2013 and 2014 filed with the SEC on March 4, 2010, March 3, 2011, March 1, 2012, February 28, 2013, February 27, 2014 and February 26, 2015, respectively. Additionally, in the Company's Form 10-K for Fiscal Year 2011, the Company included the following risk factor with respect to safeguarding confidential information of employees and customers:

Failure to comply with laws, regulations and third-party contracts regarding the collection, maintenance and processing of information may result in adverse publicity and adversely affect the operation of our business and results of operations.

We collect, maintain and process certain information about customers and employees. Our use and protection of this information is regulated by various laws and regulations, as well as by third-party contracts. If our systems or employees fail to comply with these laws, regulations or contract terms, it could require us to notify customers, employees or other groups, result in adverse publicity, loss of sales and profits, increase fees payable to third parties, and incur penalties or remediation and other costs that could adversely affect the operation of our business and results of operations.

60. The foregoing risk factor was included in the Company's Form 10-Ks for Fiscal Years 2012, 2013 and 2014.

61. In the Company's 2015 Form 10-K filed with the SEC on March 3, 2016, the Company amended its warnings pertaining to data security to the following, in relevant part:

We are heavily dependent on computer systems and information technology and any material failure, interruption or security breach of our computer systems or technology could impair our ability to efficiently operate our business.

We are significantly dependent upon our computer systems and information technology to properly conduct our business, including point-of-sale processing in our restaurants, management of our supply chain, collection of cash, payment of obligations and various other processes and procedures. Our ability to efficiently manage our business depends significantly on the reliability and capacity of these systems and information technology. The failure of these systems and information technology to operate effectively, an interruption, problems with maintenance, upgrading or transitioning to replacement systems, fraudulent manipulation of sales reporting from our franchised restaurants resulting in loss of

sales and royalty payments, or a breach in security of these systems could be harmful and cause delays in customer service, result in the loss of data and reduce efficiency or cause delays in operations. Significant capital investments might be required to remediate any problems. Any security breach involving our or our franchisees' point-of-sale or other systems could result in a loss of consumer confidence and potential costs associated with fraud. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur, resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. A security breach of our computer systems or information technology could require us to notify customers, employees or other groups, result in adverse publicity, loss of sales and profits, and incur penalties or other costs that could adversely affect the operation of our business and results of operations.

As part of our marketing efforts, we rely on search engine marketing and social media platforms to attract and retain customers. These efforts may not be successful, and pose a variety of other risks, including the improper disclosure of proprietary information, negative comments about the Wendy's brand, exposure of personally identifiable information, fraud or out of date information. The inappropriate use of social media vehicles by franchisees, customers, or employees could increase our costs, lead to litigation or result in negative publicity that could damage our reputation. The occurrence of any such developments could have an adverse effect on business results.

\*\*\*

The occurrence of cyber incidents, or a deficiency in cybersecurity, could negatively impact our business by causing a disruption to our operations, a compromise or corruption of confidential information, and/or damage to our employee and business relationships, all of which could subject us to loss and harm the Wendy's brand.

A cyber incident is considered to be any adverse event that threatens the confidentiality, integrity or availability of information resources. More specifically, a cyber incident is an intentional attack or an unintentional event that can include gaining unauthorized access to systems to disrupt operations, corrupt data or steal confidential information about customers, franchisees, vendors and employees. A number of retailers and other companies have recently experienced serious cyber incidents and breaches of their information technology systems. The Company is also investigating unusual credit card activity at some Wendy's restaurants, as further described below. As the Company's reliance on technology has increased, so have the risks posed to its systems, both internal and those it has outsourced. The three primary risks that could directly result from the occurrence of a cyber incident include operational interruption, damage to the relationship with customers, franchisees and employees and private data exposure. In addition

to maintaining insurance coverage to address cyber incidents, the Company has also implemented processes, procedures and controls to help mitigate these risks. However, these measures, as well as its increased awareness of a risk of a cyber incident, do not guarantee that the Company's reputation and financial results will not be adversely affected by such an incident.

Because the Company and its franchisees accept electronic forms of payment from their customers, the Company's business requires the collection and retention of customer data, including credit and debit card numbers and other personally identifiable information in various information systems that the Company and its franchisees maintain and in those maintained by third parties with whom the Company and its franchisees contract to provide credit card processing. The Company also maintains important internal Company data, such as personally identifiable information about its employees and franchisees and information relating to its operations. The Company's use of personally identifiable information is regulated by foreign, federal and state laws, as well as by certain third-party agreements. As privacy and information security laws and regulations change, the Company may incur additional costs to ensure that it remains in compliance with those laws and regulations. If the Company's security and information systems are compromised or if its employees or franchisees fail to comply with these laws, regulations, or contract terms, and this information is obtained by unauthorized persons or used inappropriately, it could adversely affect the Company's reputation and could disrupt its operations and result in costly litigation, judgments, or penalties resulting from violation of federal and state laws and payment card industry regulations. A cyber incident could result in adverse publicity, loss of sales and profits, increase fees payable to third parties, and incur penalties or remediation and other costs that could adversely affect the operation of the Company's business and results of operations.

As reported in the news media in late January, the Company has engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity at some Wendy's restaurants. Out of the locations investigated to date, some have been found by the cybersecurity experts to have malware on a certain system. The investigation is ongoing and the Company is continuing to work closely with cybersecurity experts and law enforcement officials.

62. Further, as set forth in the Company's annual and quarterly financial statements dating back to 2007, the Individual Defendants were aware that they were required to comply with payment card industry rules and that a failure to do so may adversely affect the Company's ability to open new restaurants or have a negative impact on the Company's existing and future operations and results:

Changes in legal or regulatory requirements, including franchising laws, payment card industry rules, overtime rules, minimum wage rates, government-mandated health care benefits, tax legislation, federal ethanol policy and accounting standards, may adversely affect our ability to open new restaurants or otherwise hurt our existing and future operations and results.

Each Wendy's restaurant is subject to licensing and regulation by health, sanitation, safety and other agencies in the state and/or municipality in which the restaurant is located, as well as to Federal laws, rules and regulations and requirements of non-governmental entities such as payment card industry rules. State and local government authorities may enact laws, rules or regulations that impact restaurant operations and the cost of conducting those operations. There can be no assurance that we and/or our franchisees will not experience material difficulties or failures in obtaining the necessary licenses or approvals for new restaurants, which could delay the opening of such restaurants in the future. In addition, more stringent and varied requirements of local governmental bodies with respect to tax, zoning, land use and environmental factors could delay or prevent development of new restaurants in particular locations.

63. The foregoing clearly demonstrates the Individual Defendants' recognition of the need to abide by payment card industry rules and regulations and the grave danger that a security breach would impose upon the Company.

***The Individual Defendants Knew that Wendy's was not Implementing Reasonable Measures to Secure its Customers' Data, Including Measures that were Required by its Contracts with the Payment Card Industry***

64. PCI DSS are promulgated by the PCI Council. These industry requirements apply to all organizations and environments where cardholder data is stored, processed, or transmitted. The PCI Council characterizes PCI DSS as "baseline" standards that consist of "a minimum set of requirements."<sup>2</sup> In other words, a company's data security policies and procedures may be expected to exceed, but should not fall below, the minimum standards set by the PCI DSS.

65. As stated by Quick Service Restaurant ("QSR") Magazine, "The security benefits associated with maintaining PCI compliance are vital to the long-term success of all merchants who process card payments. This includes continual identification of threats and vulnerabilities

---

<sup>2</sup> PCI Security Standards Council LLC, PCI DSS Requirements and the Security Assessment Procedures, Version 3.1, 5 (April, 2015).



that could potentially impact the organization. Most organizations never fully recover from data breaches because the loss is greater than the data itself<sup>3</sup>.”

66. Prior to and during the time that the Data Breach occurred, the Individual Defendants knew that Wendy’s was required, pursuant to its agreements with payment card processors and networks, including Visa and MasterCard, to abide by PCI DSS to protect its customers’ personal and financial data.

67. As demonstrated below, the Company utterly failed to comply with PCI DSS, and the Board had knowledge of such failures.

68. PCI DSS applies to all organizations that store, process, or transmit payment card data. PCI DSS establishes the minimum level of protection required, not the maximum.

69. All organizations that handle payment card data are required to implement safeguards set down in the PCI DSS.

70. PCI DSS 3.1, the version of the standards in effect at the time of the Data Breach, required that Wendy’s:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access

---

<sup>3</sup> [https://www.pcisecuritystandards.org/pqi\\_security/why\\_security\\_matters](https://www.pcisecuritystandards.org/pqi_security/why_security_matters)

- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for employees and contractors

71. The Individual Defendants failed to ensure that Wendy's was in compliance with the PCI DSS standards at the time of the Data Breach. Wendy's failure to adhere to PCI DSS, as required by its agreements with payment card processors and networks, exposed the Company to potentially massive liability in the event of a data breach.

***The Individual Defendants were Aware that Wendy's Data Security Measures were Inadequate and the Company was Vulnerable to Attack***

72. The Individual Defendants knew that the Company's data security measures were inadequate, rendering the Company vulnerable to a security breach.

73. A senior engineer ("SE2") working out of Wendy's corporate headquarters between 2014 and 2015 who initially reported to the Chief Engineer of IT Infrastructure, Jim Gatto, and subsequently to the Director of Store Technology, Phil Newsome, described the Company's corporate culture toward data security as a "hope for the best" attitude towards data security.<sup>4</sup> FIACAC ¶¶ 81-82. SE2 stated that the Company's IT personnel, including those in upper management, "had no clue what they were doing" and often addressed issues in ways that weakened the data security system, rather than strengthened it. FIACAC ¶ 81. SE2 also stated that there was a general lack of accountability in the Company's IT department and IT personnel lacked both proper training and a solid understanding of how the Company's IT systems operated. *Id.* ¶ 82. SE2 also emphasized that Wendy's IT department routinely failed to address

---

<sup>4</sup> The operative complaint in *First Choice Federal Credit Union, et al., v. The Wendy's Company, et al.*, Case No.: 2:16-cv-00506 (W.D. PA) is referred to herein as the Financial Institutions' Amended Class Action Complaint ("FIACAC").

known security issues. For example, SE2 explained that IT management continued to use the Windows XP operating system for the Aloha POS system despite well-known vulnerabilities. Windows XP was an outdated operating system that Microsoft no longer supported with security and technical updates. *Id.* ¶ 83. When SE2 raised concerns with IT employees regarding the Company's continued use of Windows XP, the employees would act horrified and surprised yet, nothing was ever done to rectify the problem. *Id.*

74. The high-profile data breaches at Target, Home Depot and others put the Individual Defendants on notice of the threat of a data breach. In fact, Visa warned merchants, including Wendy's, as early as August 2013 of malware targeting POS systems. The alert, "Retail Merchants Targeted by memory-Parsing Malware," warned: "Since January 2013, VISA has seen an increase in network intrusions involving retail merchants. Once inside the merchant's network, the hacker will install memory parser malware on the Windows based cash register system in each lane."<sup>5</sup>

75. Despite knowing the foregoing vulnerabilities, the Individual Defendants failed to implement adequate data security measures to adequately ensure that its customers' personal and financial information was secure in compliance with the PCI DSS.

***The Individual Defendants Failed to Ensure that Wendy's Installed and Maintained an Adequate Firewall and Failed to Ensure that Payment Card Data was Segmented From the Remainder of Wendy's Network***

76. The PCI DSS required retailers to install and maintain an adequate firewall in order to prevent unauthorized persons from gaining access to systems upon which cardholder data was transmitted or stored.

77. A firewall is a network security system, either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules. Acting as a barrier

---

<sup>5</sup> <http://cybersecure.com/2013/09/10/retail-merchants-targeted-by-memory-parsing-malware-visa/>

between a trusted network and other untrusted networks (e.g., the Internet) or less-trusted networks (e.g., a retail merchant's network outside of a cardholder data environment), a firewall controls access to the resources of a network through a positive control model. This means that only traffic expressly allowed in the firewall policy is permitted onto the network; all other traffic is denied.

78. As set forth in the FIACAC, a former Wendy's employee who worked as a Field Network/System Administrator and was responsible for implementing network security upgrades at various corporate-owned and franchised restaurants confirmed that many of the restaurants he visited lacked any firewall whatsoever. *Id.* ¶ 112. The former field network/system administrator stated that other technicians also confirmed that certain Wendy's restaurants lacked any firewall. *Id.*

79. The former field network/system administrator identified problems associated with the Company's firewall configuration. *Id.* ¶ 113. As an example, when working on an upgrade project for the Company, the former field network/system administrator learned that the necessary routers had not been delivered to the restaurant sites. He advised his supervisor of the situation and stated that his supervisor told him to go to Wal-Mart to buy "any router" he could find to use in the conversion. *Id.* Although the former field network/system administrator warned his supervisor that any hacker could easily exploit this workaround and gain access to payment card data and refused to use routers purchased from Wal-Mart, he remarked that some of his colleagues did, in fact, use the inappropriate routers. *Id.* The former field network/system administrator stated that the Wal-Mart routers were not PCI DSS compliant. *Id.*

80. Pursuant to the FIACAC, Wendy's also lacked proper network segmentation to prevent a user with access to one area of the network from accessing other areas of the network

where payment card data would be stored. *Id.* ¶ 115. The former field network/system administrator stated that Wendy's maintained two (or dual) networks which were both connected to the Aloha POS system. *Id.* The former field network/system administrator further stated that dual networks lacked proper network segmentation, which would allow a hacker, who could gain access to one area of the network, to access other areas of the network to steal payment card data. *Id.* The former field network/system administrator was certain that Wendy's dual network configuration was not PCI DSS compliant because payment card data was not adequately separated from Wendy's public wireless internet network. *Id.*

81. The former field network/system administrator also stated that he was performing a network security upgrade in 2015 to render Wendy's IT environment less penetrable, specifically by improving the firewall protection and separating payment card data from Wendy's public wireless internet network. *Id.* ¶ 116. During the time of his departure from Wendy's in February 2016, the former field network/system administrator stated that there remained hundreds of Wendy's establishments that needed to perform the network security upgrade, which included proper network segmentation. *Id.* That hundreds of restaurants had inadequate data security during the time of the Data Breach clearly indicates that the Individual Defendants failed to timely implement the necessary changes and upgrades.

82. According to the FIACAC, another former Wendy's employee who worked as a senior engineer in Restaurant Infrastructure also stated that there were network segmentation issues with respect to the setup of the servers at Wendy's restaurants. *Id.* ¶ 117. He stated that all devices with electronic connectivity, including point-of-sale terminals and electronic menu board displays, resided on the same network. *Id.* Therefore, anyone who could gain access to

the network would also be able to gain access to payment card data which was, according to the senior engineer in Restaurant Infrastructure, a violation of PCI DSS. *Id.*

83. The senior engineer in Restaurant Infrastructure stated that every Wendy's restaurant that was using the Aloha POS system, regardless if it was a franchise or a company-owned store, was connected to the Aloha command center. *Id.* ¶ 118. This allowed Wendy's corporate headquarters to also have access to each restaurant running the Aloha POS system. *Id.* The Aloha Command Center also allowed the Company to monitor the status of each server and point-of-sale terminal and provide access to render technical or other support to Aloha POS system users. *Id.* The senior engineer in Restaurant Infrastructure stated that the corporate data center, which was housed on a server at the Company's headquarters, included the Aloha Command Center software that ran on all stores utilizing the Aloha POS system. *Id.* This configuration demonstrates that, absent proper network segmentation, there was full electronic connectivity between corporate and its franchisees. *Id.* As a result of this connectivity, coupled with the lack of adequate firewall protection and proper network segmentation, a hacker not only could enter Wendy's computer network, but also would be able to jump unhindered between various network platforms and ultimately access Wendy's customers' payment card data. *Id.*

84. Given that the Company's 2015 Form 10-K states that Wendy's conducts "restaurant operational audits and field visits from Company supervisors," it can be reasonably inferred that the Individual Defendants were aware that multiple restaurants did not maintain adequate data security.

***The Individual Defendants Failed to Implement Protocols that Would Have Protected Payment Card Data***

85. The Individual Defendants failed to implement certain protocols, such as software image hardening, password protecting programs that captured payment card data, and encrypting

payment card data at the point-of-sale, which would have detected and prevented unauthorized programs from being installed on Wendy's POS systems and otherwise would have protected payment card data in the event of a breach.

86. Hardening is the process of stripping unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers. According to the FIACAC, the senior engineer in Restaurant Infrastructure was responsible for making sure that images of the software that were released and deployed to all restaurants using the Aloha POS system met PCI DSS requirements. *Id.* ¶ 120. The senior engineer in Restaurant Infrastructure was responsible for analyzing images from all of the devices in use in the restaurants, including POS terminals, kitchen devices, and back office servers – all of which were running Aloha POS software and had access to payment card data. *Id.* The senior engineer in Restaurant Infrastructure stated that if images of the software were not hardened, it could allow payment card data to be stolen from the system. *Id.* The senior engineer in Restaurant Infrastructure stated that Wendy's had not hardened the system images successfully and believed this made Wendy's vulnerable to a data breach. *Id.*

87. After the senior engineer in Restaurant Infrastructure left Wendy's and immediately before the Data Breach, the senior engineer stated that the person who assumed responsibility for ensuring that images were hardened and released was not qualified for the job and further, that his replacement would call the senior engineer nearly every day for help with the imaging process. *Id.* ¶ 121. Based on these discussions, the senior engineer in Restaurant Infrastructure knew that the images of the software were not properly hardened, which rendered the Aloha POS system vulnerable to a security breach. *Id.*

88. Another former senior engineer also confirmed that, prior to the Data Breach, none of the versions of the Aloha POS software that Wendy's was deploying were hardened. *Id.* ¶ 122.

89. Additionally, the FIACAC stated that the Company failed to encrypt payment card data at the POS terminal. *Id.* ¶ 123.

90. PCI DSS also mandated that retailers not store cardholder data any longer than necessary and encrypt any cardholder data at the point of sale so as to render any retained data unreadable to hackers.

91. Encryption is a cryptographic process by which data is encoded in such a way that only authorized parties can decrypt it. Without the proper private key, encrypted information appears as a string of undecipherable characters. Only after a user unlocks the information with her private key does it transform the data to its original, user-readable form.

92. Cardholder data is at risk of being exposed or stolen during two stages of the payment process: pre-authorization, when the merchant has captured a consumer's data and is waiting to send it to the acquirer; and post-authorization, when cardholder data has been sent back to the merchant with a response from the acquirer, and is placed into some form of storage in the merchant's servers.

93. PCI DSS explained that, even if an intruder was able to penetrate the firewall, encryption at the point of sale could still protect the data accessed and thereby reduce the risk of loss. Encryption also would protect data stored in the merchant's servers. PCI DSS made clear that, under no circumstances should unencrypted data be stored on servers or, worse, transmitted through end-user messaging technologies, such as email.



94. According to the FIACAC, the senior engineer in Restaurant Infrastructure stated that although the electronic data capture (“EDC”) file containing payment card data would be encrypted during its transfer between an Aloha POS terminal and the bank authorizing the transaction, payment card data existed in an unencrypted format on the Aloha POS terminals. *Id.* ¶ 123.

95. The senior engineer in Restaurant Infrastructure stated that the EDC file containing payment card data would be accessible remotely by anyone using the Aloha Command Center software. *Id.* ¶ 124. Additionally, he stated that the user identification and passwords associated with these EDC files were not encrypted and thus, could be stolen by hackers to unencrypt any later-encrypted payment card data. *Id.*

96. According to the FIACAC, another former senior engineer of the Company identified Wendy’s password management as another potential weakness in Wendy’s computer system. He explained that the same passwords were used across certain devices and that “any former employee with an axe to grind” could cause significant damage to Wendy’s, since Wendy’s did not regularly, if ever, change these generic passwords. *Id.* ¶ 125.

***The Individual Defendants Failed to Install Software to Adequately Track and Monitor Its Network***

97. Wendy’s failed to adequately track access to its network and to monitor its network for unusual activity, particularly with respect to its point-of-sale terminals, which would have allowed Wendy’s to detect and potentially prevent hackers from stealing payment card data. Symantec, one of the software vendors, provides the following with regard to this type of endpoint protection software: “Symantec’s network threat protection analyzes incoming data and blocks threats while they travel through the network before hitting endpoints. Rules-based firewall and browser protection are also included to protect against web-based attacks.” Had

Wendy's implemented proper endpoint detection and prevention systems, it would have been able to identify suspicious activity occurring within Wendy's network. Proper endpoint protection would have triggered warnings and alerted Wendy's to the transmission of payment card data within its system and should have alerted Wendy's to large volumes of data being removed, or exfiltrated, from its network.

***The Individual Defendants Failed to Upgrade the Company's Systems to Utilize EMV Technology***

98. Following the litany of data breaches, the payment card industry determined that it would shift to an EMV, or Chip-and-Pin, system by October 2015. U.S. merchants were given until October 1, 2015 to make the switch, and any merchant who had not made the switch before the deadline, such as Wendy's, would now be liable for payment fraud caused by compromised POS terminals.

99. EMV cards, which have a secret algorithm embedded in a chip that creates a unique transaction code that cannot be used again, are designed to be far more expensive and difficult for thieves to counterfeit. By contrast, the traditional non-chip cards store unchanging data on a magnetic strip, which can be easily copied and re-encoded onto virtually anything else with a magnetic strip. Indeed, magnetic strip cards were the primary target for hackers who broke into Target and Home Depot and installed malicious software on the cash registers.

100. Yet, despite the regulatory changes requiring merchants to switch to EMV technology, the Individual Defendants failed to do so and in fact, never had plans to make the transition. During a conference that took place in 2013, Gavin Waugh, vice president and treasurer at Wendy's, stated "[Wendy's] actual fraud rate is so small it's hardly worth mentioning. [EMV] doesn't move the needle that much. Even if we pay the fraud liability, it's a whole lot cheaper than putting in [EMV] terminals." The hamburger chain processes 300,000

card transactions daily, Waugh said. Waugh also noted that the implementation of EMV technology would cost a “staggering amount of money.” Ironically during the same conference, the merchant panel, including Waugh, acknowledged that “EMV tackles only point-of-sale fraud<sup>6</sup>.”

101. To make matters even worse, after the Company confirmed the Data Breach, Waugh declined to say whether Wendy’s has a timetable for deploying chip-based readers in its restaurants, but stated “I don’t think that would have solved this problem, and it’s a bit of a misnomer . . . I think it makes it harder [for the attackers], but I don’t think it makes it impossible.”

102. Had the Individual Defendants taken the proper steps to implement EMV technology, the Data Breach could have been prevented or, at the very least, mitigated. Yet, despite the fact that the payment card industry set a deadline of October 1, 2015 for businesses to transition their systems from magnetic-strip to EMV technology, the Individual Defendants, in conscious disregard of their fiduciary duties, failed to comply with that deadline.

***The Data Breach and the Individual Defendants’ Inadequate Response***

103. On January 27, 2016, security blogger Brian Krebs of *KrebsonSecurity* first broke the news that Wendy’s was investigating claims of a possible credit card breach at some locations. The acknowledgment from the Company came in response to questions from *KrebsonSecurity* about banking industry sources who discovered a pattern of fraud on cards that were all recently used at various Wendy’s locations.

104. Bob Bertini, Wendy’s spokesperson, told Krebs that Wendy’s “received this month from [the Company’s] payment industry contacts reports of unusual activity involving

---

<sup>6</sup> <http://www.digitaltransactions.net/index.php/news/story/Execs-with-Major-Retailers-Complain-EMV-Attacks-Wrong-Problem-at-Huge-Expense>

payment cards at some of [Wendy's] restaurant locations. Reports indicate that fraudulent charges may have occurred elsewhere after the cards were legitimately used at some of [the Company's] restaurants. [Wendy's has] hired a cybersecurity firm and launched a comprehensive and active investigation that's underway to try to determine the facts."

105. Although Bertini said that it was too soon to say whether the incident is contained, how long it may have persisted or how many stores may be affected, Bertini stated that the Company "began investigating immediately, and the period of time [the Company] is looking at the incidents is late last year."

106. On February 9, 2016, the Company filed a current report on Form 8-K and an accompanying press release with the SEC announcing its preliminary results for the fourth quarter and full year ended January 3, 2016. In the press release, the Company provided the following update on its investigation:

**Update on Investigation into Unusual Credit Card Activity**

As reported in the news media in late January, the Company has engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity related to certain Wendy's restaurants. Out of the locations investigated to date, some have been found by the cybersecurity experts to have malware on their systems. The investigation is ongoing, and the Company is continuing to work closely with cybersecurity experts and law enforcement officials.

107. On March 2, 2016, Krebs reported that a number of credit unions have stated that they have experienced an "unusually high level of debit card fraud from the breach at [] Wendy's, and that the *losses so far eclipse those that came in the wake of huge card breaches at Target and Home Depot.*" (Emphasis added).

108. Krebs stated that after speaking with a bank security consultant who was helping several financial institutions deal with the fallout from the Wendy's breach, the consultant stated that many of the banks had customers who re-compromised their cards several times in one

month because they ate at several different Wendy's locations throughout the month. Krebs further reported that although many banks and credit unions are now issuing more secure chip-based credit and debit cards (which are designed to make it more difficult and more expensive for thieves to counterfeit stolen cards), it appears that the breached Wendy's locations were not asking customers to "dip their chip cards but instead swipe the card's magnetic strip," thus confirming that Wendy's had not yet transitioned to utilizing EMV technology in its restaurants, despite the October 2015 deadline.

109. The next day on March 3, 2016, the Company filed its annual report on Form 10-K with the SEC (the "2015 10-K") providing the following update on the Company's investigation, in relevant part:

As reported in the news media in late January, the Company has engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity at some Wendy's restaurants. Out of the locations investigated to date, some have been found by the cybersecurity experts to have malware on a certain system. The investigation is ongoing and the Company is continuing to work closely with cybersecurity experts and law enforcement officials.

110. On May 11, 2016, the Company filed a quarterly report on Form 10-Q with the SEC reporting the Company's financial results for the three months ended April 3, 2016 (the "2016 1Q 10-Q"). In the 2016 1Q 10-Q, the Company provided the following update on the breach:

***Certain of Our Franchisees have Experienced a Data Incident***

Earlier this year, the Company engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity at some Wendy's restaurants. Investigation into this activity is nearing completion. Based on the preliminary findings of the investigation and other information, the Company believes that malware, installed through the use of compromised third-party vendor credentials, affected one particular point of sale system ***at fewer than 300 of approximately 5,500 franchised North America Wendy's restaurants, starting in the fall of 2015.*** These findings also indicate that ***the Aloha point of sale system has not been impacted by this activity.*** The Aloha system is already installed at all Company-owned restaurants and in a majority of franchise-owned

restaurants, with implementation throughout the North America system targeted by year-end 2016. The Company expects that it will receive a final report from its investigator in the near future.

The Company has worked aggressively with its investigator to identify the source of the malware and quantify the extent of the malicious cyber-attacks, and has ***disabled and eradicated the malware in affected restaurants***. The Company continues to work through a defined process with the payment card brands, its investigator and federal law enforcement authorities to complete the investigation. Based upon the investigation to date, ***approximately 50 franchise restaurants are suspected of experiencing, or have been found to have, unrelated cybersecurity issues***. The Company and affected franchisees are working to verify and resolve these issues.

The Company has been named as a defendant in two putative class actions filed in the United States on behalf of customers and payment card issuing banks seeking damages and other relief allegedly arising from the data incident. In addition, claims may also be made by payment card networks against the affected franchisees. These claims and investigations may adversely affect how we or our franchisees operate the business, divert the attention of management from the operation of the business, have an adverse effect on our reputation, result in additional costs, and adversely affect our results of operations.

(Emphasis added).

111. Based on the foregoing, the Company confirmed that the Data Breach began in the fall of 2015, thus evidencing that the Data Breach went undetected for months. To make matters worse, the Company only learned of the Data Breach after banking industry sources advised security blogger Brian Krebs that they discovered a pattern of fraud on cards that were recently used at Wendy's locations. Moreover, despite the statements by the Company that the Data Breach was limited in scope, had been contained and had not affected the Aloha POS system, in reality, the exact opposite was true.

112. On June 9, 2016, the Company filed a current report on Form 8-K along with an accompanying press release with the SEC announcing that it had recently discovered a second strain of malware at additional restaurants that had affected a POS system that the Company

previously believed had not been impacted. The press release stated the following, in relevant part:

## **WENDY'S UPDATE ON UNUSUAL CREDIT CARD ACTIVITY**

### **Company Disables Malware Discovered at Additional Restaurants**

DUBLIN, Ohio, June 9, 2016 –The Wendy's Company (NASDAQ: WEN) announced today that *additional malicious cyber activity has recently been discovered in some franchise-operated restaurants. The Company has disabled the malware where it has been detected.*

This latest action is the result of the Company's continuing investigation into unusual credit card activity at some Wendy's® restaurants. Reports indicate that payment cards used legitimately at Wendy's may have been used fraudulently elsewhere.

Based on the preliminary findings of the previously-disclosed investigation, the Company reported on May 11 that malware had been discovered on the point of sale (POS) system at fewer than 300 franchised North America Wendy's restaurants. An additional 50 franchise restaurants were also suspected of experiencing, or had been found to have, other cybersecurity issues. As a result of these issues, the Company directed its investigator to continue to investigate.

In this continued investigation, *the Company has recently discovered a variant of the malware, similar in nature to the original, but different in its execution. The attackers used a remote access tool to target a POS system that, as of the May 11<sup>th</sup> announcement, the Company believed had not been affected.* This malware has been discovered on some franchise restaurants' POS systems, and the number of franchise restaurants impacted by these cybersecurity attacks is now *expected to be considerably higher than the 300 restaurants already implicated.* To date, there has been no indication in the ongoing investigation that any Company-operated restaurants were impacted by this activity.

Many franchisees and operators throughout the retail and restaurant industries contract with third-party service providers to maintain and support their POS systems. The Company believes this series of cybersecurity attacks resulted from *certain service providers' remote access credentials being compromised, allowing access to the POS system in certain franchise restaurants serviced by those providers.*

The malware used by attackers is highly sophisticated in nature and extremely difficult to detect. Upon detecting the new variant of malware in recent days, the Company has already disabled it in all franchise restaurants where it has been

discovered, and the Company continues to work aggressively with its experts and federal law enforcement to continue its investigation.

(Emphasis added).

113. As set forth in the Amended Complaint in the Consumer Class Action, the foregoing press release contained numerous material omissions, including but not limited to, the following:

- a. Wendy's failed to provide a general description of the nature of the Data Breach;
- b. Wendy's failed to disclose the number of debit and credit cards compromised;
- c. Wendy's failed to disclose how many individuals were affected;
- d. Wendy's failed to disclose what customer information was actually compromised; and
- e. Wendy's failed to state that this threat was ongoing.

ACCAC ¶ 57.<sup>7</sup>

114. Later that same day, Krebs reported about the Data Breach, noting that the Company's most recent statement that "the attackers got access by stealing credentials that allowed remote access to point-of-sale terminals should hardly be surprising: The vast majority of the breaches involving restaurant and hospitality chains over the past few years have been tied to hacked remote access accounts that POS service providers use to remotely manage the devices."

115. Krebs also remarked that "many retailers are now moving to install card readers that can handle transactions from more secure chip-based credit and debit cards, which are far more expensive for thieves to clone." Gavin Waugh, vice president and treasurer at Wendy's,

---

<sup>7 7</sup> The operative complaint in *Torres, et al. v. Wendy's International LLC*, Case No.: 6:16-cv-210 (M.D. Fla.) is referred to herein as the Amended Consumer Class Action Complaint ("ACCAC").



declined to say whether Wendy's has a timetable for deploying chip-based readers in its restaurants, but stated "I don't think that would have solved this problem, and it's a bit of a misnomer . . . I think it makes it harder [for the attackers], but I don't think it makes it impossible."

116. These statements hardly come as a surprise, given Waugh's prior comments indicating that the cost of installing EMV technology greatly outweighs the benefits. Indeed, during a conference that took place in 2013, Waugh stated "[Wendy's] actual fraud rate is so small it's hardly worth mentioning. [EMV] doesn't move the needle that much. Even if we pay the fraud liability, it's a whole lot cheaper than putting in [EMV] terminals." The hamburger chain processes 300,000 card transactions daily, Waugh said. Waugh also noted that the implementation of EMV technology would cost a "staggering amount of money." Ironically during the same conference, the merchant panel, including Waugh, acknowledged that "EMV tackles only point-of-sale fraud<sup>8</sup>."

117. Had the Individual Defendants taken the proper steps to implement EMV technology, the Data Breach could have been prevented or, at the very least, mitigated. Yet, despite the fact that the payment card industry set a deadline of October 1, 2015, for businesses to transition their systems from magnetic-strip to EMV technology, the Individual Defendants, in conscious disregard of their fiduciary duties, failed to comply with that deadline.

118. On July 7, 2016, the Company issued a news release on its website which provided the following update on the Company's investigation into the breach, in relevant part:

---

<sup>8</sup> <http://www.digitaltransactions.net/index.php/news/story/Execs-with-Major-Retailers-Complain-EMV-Attacks-Wrong-Problem-at-Huge-Expense>

## Wendy's Update on Payment Card Security Incident

### Customers Now Able to Access More Specific Information About Potentially Impacted Locations on Website – Company Offers Complimentary Fraud Consultation and Identity Restoration Services

DUBLIN, Ohio, July 7, 2016 /PRNewswire/ -- The Wendy's Company (NASDAQ: WEN) updated its customers today regarding malicious cyber activity experienced at some Wendy's® restaurants. The Company first reported unusual payment card activity affecting some franchise-owned restaurants in February 2016. Subsequently, on June 9, 2016, the Company reported that an additional malware variant had been identified and disabled. Today, the Company, on behalf of affected franchise locations, is providing information about specific restaurant locations that may have been impacted by these attacks, all of which are located in the U.S., along with support for customers who may have been affected by the malware variants.

"We are committed to protecting our customers and keeping them informed. We sincerely apologize to anyone who has been inconvenienced as a result of these highly sophisticated, criminal cyberattacks involving some Wendy's restaurants," said Todd Penegor, President and Chief Executive Officer. "We have conducted a rigorous investigation to understand what has occurred and apply those learnings to further strengthen our data security measures."

Wendy's customers are encouraged to learn more about this new information at the following address: [www.wendys.com/notice](http://www.wendys.com/notice). The update includes a list of restaurant locations that may have been involved in the incidents, as well as information on how customers can protect their credit and details regarding how potentially affected customers can receive one year of complimentary fraud consultation and identity restoration services. A link to the update can also be found on the Company's homepage, [www.wendys.com](http://www.wendys.com).

Working closely with third-party forensic experts, federal law enforcement and payment card industry contacts as part of its ongoing investigation, the Company has determined that specific payment card information was targeted by the additional malware variant. ***This information included cardholder name, credit or debit card number, expiration date, cardholder verification value, and service code.***

***Generally, individuals that report unauthorized charges in a timely manner to the bank or credit card company that issued their card are not responsible for those charges.*** As always, in line with prudent personal financial management, we encourage our customers to be diligent in watching for unauthorized charges on their payment cards.

*The Company believes the criminal cyberattacks resulted from service providers' remote access credentials being compromised, allowing access – and the ability to deploy malware – to some franchisees' point-of-sale systems.* To date, there has been no indication in the ongoing investigation that any Company-operated restaurants were impacted by this activity.

The Company worked with investigators to disable the malware involved in the first attack earlier this year. Soon after detecting the malware variant involved in the latest attack, the Company identified a method of disabling it and thereafter disabled it in all franchisee restaurants where it was discovered. *The investigation has confirmed that criminals used malware believed to have been effectively deployed on some Wendy's franchisee systems starting in late fall 2015.*

(Emphasis added).

119. Despite representing to the public that more information about the Data Breach was available on the Company's website, Wendy's failed to provide any additional information and what little information it did provide was inadequate and redundant. Indeed, the Individual Defendants have continued to remain silent about the specifics of the Data Breach and the status of the Company's investigation.

120. Noticeably absent from the Company's June 9, 2016 press release or Wendy's July 7, 2016 news release, and contrary to the Company's earlier public disclosures, was the representation that none of the Aloha POS systems had been compromised. Indeed, to this day, the Company has failed to acknowledge that the Aloha POS system that Wendy's required its franchisees to install had also been involved in the Data Breach.

***The Individual Defendants Knew that the Company's Aloha POS System was Inadequate and Would Not Protect Against a Data Breach***

121. Prior to the Data Breach, the Individual Defendants were aware that its data security systems were insufficient and outdated that its POS system would not protect the Company against a data breach.

122. On December 22, 2014, Wendy's filed a lawsuit against DavCo Restaurants LLC and DavCo Acquisition Holding, Inc. (collectively "DavCo"), one of the Company's largest

franchisees<sup>9</sup>, seeking to immediately terminate each of DavCo's franchise agreements on the grounds of DavCo's alleged failure to comply with the terms of the franchise agreements by not, among other things, purchasing and installing, a common point of sale computer platform.

123. According to Wendy's complaint against DavCo ("DavCo Complaint"), "in October 2012, Wendy's formally announced plans to implement NCR Aloha ("Aloha") as the required POS platform for the Wendy's system in the U.S. and Canada." DavCo Complaint ¶ 16. Further, Wendy's admitted that this was a significant and important announcement, as prior to this time, Wendy's remained one of the few major quick-service restaurant chains that had not yet implemented a single, consistent POS platform system wide. *Id.* The DavCo Complaint also stated that "NCR is a publicly-traded, leading provider of technology solutions and Aloha is regarded as one of the best, if not the best, POS solutions available to the restaurant industry," *id.*, and that Wendy's selected Aloha following a lengthy, in-depth selection process managed by Wendy's IT and Operations departments, with continuous input from Wendy's U.S. and Canadian franchise advisory councils, whose members are comprised of franchisees representing multiple geographic regions within the U.S. and Canada. *Id.* ¶ 18.

124. Indeed, in an exchange between defendant Brolick and an analyst from CL King & Associates, Inc. that took place during the 2012 4Q Earnings Call,<sup>10</sup> defendant Brolick admitted that the Company's POS system was outdated and that the Company would need to move fairly quickly to adopt the Aloha POS system:

Analyst: Okay, great. And then just a follow-up question. I guess when you look at the remodels, I assume as stores get done, you're going to get everybody on a common POS platform. I was wondering just how long you think it'll take to get the system on a -- more of a common POS platform so you can better utilize the

---

<sup>9</sup> The lawsuit is captioned as *Wendy's Int'l, LLC v. DavCo Rests. LLC*, No. 14CV013382 (Ohio Ct. Comm. Pl.) (the "DavCo Lawsuit")

<sup>10</sup> <http://seekingalpha.com/article/1234861-the-wendys-management-discusses-q4-2012-results-earnings-call-transcript?part=single>

new app and be able to really utilize some of the tools that hit those customers more efficiently from a marketing standpoint.

Brolick: Yes. Well, I'll start out and then ask Steve to jump in here. But *there is a fairly high percentage of our system that has fairly old POS software*, and they're going to need to evolve to this fairly quickly. There are also franchisees, however, who have quite recently made important investments in what we call modern POS hardware as well as software. They will eventually have to transition out of that into the common platform that we have identified, which is NCR's Aloha. But that might be 5 years down the road for them. But again, they have modern POS that can run this. So that's not an issue. But to do the things we want longer term, there -- they, too, are eventually going to have to change. But there's a decent piece of the system that's going to have to move to this really pretty quickly.

(Emphasis added).

125. Further, despite Brolick's acknowledgment that the Company's systems were outdated and that the transition to Aloha POS would have to happen quickly, although the original deadline to install Aloha in all Wendy's restaurants was July 1, 2014, Wendy's claimed that it extended the deadline to July 1, 2015 "in order to give Wendy's franchisees additional time to plan for and make the recurring investment to help ensure a successful rollout of Aloha in all restaurants." DavCo Complaint ¶ 19.

126. On February 16, 2015, DavCo filed its answer to the complaint and asserted counterclaims against Wendy's (the "DavCo Counterclaim"). The DavCo Counterclaim alleged that the Aloha POS system was fraught with serious technical and operational problems which, according to DavCo, Wendy's acknowledged, but summarily dismissed as trivial. DavCo Counterclaim ¶ 9. DavCo further alleged that the Aloha POS software was unstable and would repeatedly freeze and disconnect from the restaurant's network, causing Wendy's to temporarily suspend Aloha installations in late 2013 because of concerns relating to the software's stability. *Id.* ¶¶ 25-30.

127. On June 30, 2016, after Wendy's had confirmed the Data Breach, Wendy's filed its first amended complaint against DavCo and on July 15, 2016, DavCo filed its first amended answer and asserted counterclaims against Wendy's (the "DavCo Amended Counterclaim").

128. The DavCo Amended Counterclaim stated that DavCo determined in 2005 and 2006 to modernize its POS system and, after consulting with John Deane, Wendy's Chief Information Officer at the time, Mr. Deane recommended the Micros POS system as the most suitable for a Wendy's franchise. DavCo Amended Counterclaim at ¶ 26. Additionally, Mr. Deane stated that Wendy's itself would be adopting the Micros POS system for use in Company owned restaurants. *Id.*

129. The DavCo Amended Counterclaim went on to state that although the Company's information technology department reviewed multiple POS systems in 2005 and 2006, including the Aloha POS system, Wendy's rejected Aloha for use in its company-owned restaurants at the time. *Id.* ¶ 27.

130. With respect to the Aloha POS System, the DavCo Amended Counterclaim alleges that "the frequent problems demonstrated by Wendy's poor decision to adopt the Aloha POS system is exhibited by the ever-changing deadlines cited in Wendy's complaints in this litigation. Wendy's selected the Aloha platform in October 2012 – nearly four years ago. Wendy's then decided upon an original deadline of July 1, 2014 to install Aloha. Because of major problems with Aloha, that deadline was eventually delayed to July 1, 2015. Now Wendy's claims that the deadline was March 31, 2016, though not all restaurants are required to have the Aloha system installed until at least December 31, 2016. Upon information and belief, it is unlikely that this latest announced deadline will be met. And some Wendy's restaurants will never have to install the Aloha system." DavCo Amended Counterclaim ¶ 11.

131. Further, DavCo alleged that “the functional capacity of the Aloha system was also subject to ridicule among franchisees” and that Wendy’s informed its franchisees on November 18, 2014 that the problems with the Aloha POS system “were ‘causing more disruption than we would consider to be reasonable.’” *Id.* ¶ 29.

132. The DavCo Amended Counterclaim also included the following allegations about the Data Breach, in relevant part:

Upon information and belief, there continue to be significant problems with the Aloha POS system. In January 2016, reports disclosed a possible data breach arising from Wendy’s POS systems. Wendy’s confirmed in May 2016 that franchisee POS systems were the target of a consumer data breach, but stated that the breach affected only around 300 restaurants and that Aloha was not affected. However, in June 2016, Wendy’s revealed that the data breach was larger and may have affected another POS system without disclosing what system specifically. On July 7, 2016, Wendy’s disclosed that the data breach occurred over the course of two waves and affected over 1,000 restaurants – nearly 20% of Wendy’s franchise locations in the United States. ***Upon information and belief, many of the affected restaurants utilized the Aloha POS system.*** None of DavCo’s restaurants – which have not installed the Aloha system to date – appear to have been affected by the data breach. Despite not having any restaurants which were part of the data breach suffered by those franchised restaurants that installed the Aloha POS system, DavCo has been subjected to numerous media reports and suspicion from its customers that their data may have been compromised as part of the Aloha data breach.

*Id.* ¶ 34 (Emphasis added).

133. Further, the DavCo Amended Counterclaim stated that Don Zimmerman served as Wendy’s Chief Information Officer from 2008 to 2015 and that he was primarily responsible for deciding the technology vendors that would service Wendy’s restaurants including NCR, the developer of the Aloha POS system. *Id.* ¶ 35. DavCo claimed that Mr. Zimmerman played a “crucial role” in deciding that the Aloha POS system would be required for use in Wendy’s restaurants despite its many flaws and, notably, after Zimmerman’s departure from Wendy’s in 2015, he went on to become the Chief Technology Officer for NCR’s hospitality division. *Id.*

134. On July 25, 2016, Wendy's filed a reply to DavCo's Amended Counterclaim ("Wendy's Reply"). Notably, despite its prior public statements to the contrary, Wendy's did not deny DavCo's claims that the Data Breach had indeed affected restaurants that were utilizing the Aloha POS system (Wendy's Reply ¶ 34) and also admitted that Don Zimmerman was Wendy's former Chief Investment Officer, he participated in the decision to implement the Aloha POS system for the Wendy's system in the United States and Canada and Mr. Zimmerman no longer works for the Company. *Id.* ¶ 35.

135. Moreover, on July 13, 2016, Wendy's posted a job listing on its website seeking an analyst – POS solutions. Under the section of the listing entitled "Job description," the description provided by Wendy's admitted that the Aloha POS system suffered from defects, stating the following, in relevant part:

This position is responsible for assisting in supporting and enhancing Aloha application software within the Restaurant Solutions environment, and for all integrated Aloha software required for optimal restaurant operations. This role will execute *first level investigation into reported defects within new and existing Aloha POS software code and submit initial findings for further analysis and root cause determination*. This role will facilitate data gathering and requirements definitions for appropriate internal groups to better manage Third Party vendors and to ensure quality software delivery to restaurants required for optimal operations. Reporting to the Manager - Application Engineering<sup>11</sup>.

(Emphasis added).

136. Based on the foregoing, despite having knowledge of the multiple problems with the Aloha POS system dating back several years and recognizing the importance of maintaining adequate data security policies and procedures, the Individual Defendants, in conscious disregard of their fiduciary duties, failed to take adequate steps to update its POS system and/or rectify the

---

<sup>11</sup> See [https://wendys.taleo.net/careersection/ext\\_noncrew/jobdetail.ftl?job=PR%200002562&lang=en](https://wendys.taleo.net/careersection/ext_noncrew/jobdetail.ftl?job=PR%200002562&lang=en) and <https://www.linkedin.com/jobs/view/176518237>



existing issues with the Aloha POS system, all of which could have prevented the Data Breach from occurring. This is even more egregious given that after the Company learned that the Data Breach impacted restaurants utilizing the Aloha POS system, the Company continues to utilize the faulty Aloha POS system in its restaurants and continues to require franchisees to implement the Aloha POS system in their restaurants

**DAMAGES TO WENDY'S CAUSED BY THE INDIVIDUAL DEFENDANTS**

137. As a direct and proximate result of the Individual Defendants' misconduct, Wendy's failed to maintain proper internal controls, consciously disregarded multiple red flags alerting the Individual Defendants to multiple areas of non-compliance with the Company's existing policies and procedures and problems with the Aloha POS system, caused the Company to release false and misleading statements and substantially damaged the Company's credibility, corporate image and goodwill.

138. Wendy's has expended and will continue to expend significant sums of money. Additional expenditures and damages that the Company has incurred as a result of the Individual Defendants' breaches of their fiduciary duty include:

- a. Costs incurred from investigating, defending and payment of any settlement or judgment in the Financial Institution Class Action and the Consumer Class Action;
- b. Costs incurred from retaining cybersecurity experts to conduct a comprehensive investigation into the Data Breach;
- c. Costs incurred in strengthening and/or implementing changes to Wendy's existing data security systems; and

- d. Costs incurred from the loss of Wendy's customers' confidence in the Company's services resulting in lost sales.

**DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS**

139. Plaintiff brings this action derivatively in the right and for the benefit of Wendy's to redress injuries suffered, and to be suffered, by Wendy's as a direct result of breaches of fiduciary duty and unjust enrichment.

140. Plaintiff is a shareholder of Wendy's, was a shareholder of Wendy's at the time of the wrongdoing alleged herein, and has been a shareholder of Wendy's continuously since that time.

141. Plaintiff will adequately and fairly represent the interests of the Company and its shareholders in enforcing and prosecuting its rights.

142. Wendy's is named as a nominal defendant in this case solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have. Prosecution of this action, independent of the current Board of Directors, is in the best interests of the Company.

143. The wrongful acts complained of herein subject, and will continue to subject, Wendy's to continuing harm because the adverse consequences of the actions are still in effect and ongoing.

144. The wrongful acts complained of herein were unlawfully concealed from Wendy's shareholders.

145. Throughout the Relevant Period, the Individual Defendants failed to make full and fair disclosure about the effectiveness of Wendy's internal controls and violated multiple

corporate governance principles, thus representing evidence of the Individual Defendants' breaches of fiduciary duties.

146. As a result of the facts set forth herein, Plaintiff has not made any demand on the Current Director Defendants to institute this action since demand would be a futile and useless act because the Current Director Defendants are incapable of making an independent and disinterested decision to institute and vigorously prosecute this action. The wrongful acts complained of herein show multiple breaches by the Individual Defendants, including the Current Director Defendants, of their fiduciary duties of loyalty, due care and oversight.

147. A majority of the Board is incapable of disinterestedly and independently considering a demand to commence and vigorously prosecute this action for the reasons set forth above and below.

148. As of the date of this Complaint, the Current Board consists of the following eleven individuals: defendants N. Peltz, May, Brolick, Hill, Kass, Levato, Mathews-Spradlin, M. Peltz, Penegor and Rothschild and non-defendant Arthur B. Winkleblack ("Winkleblack").

149. As an initial matter, demand upon the Current Director Defendants is futile because the Board is already predisposed to refuse a demand as demonstrated by the Current Director Defendants' position on the merits of the Financial Institutions' Class Action and Consumer Class Action, whose allegations also form the basis, in part, of liability in the instant litigation. In a Form 10-Q filed with the SEC on August 10, 2016, the Company stated the following, in relevant part:

The Company was named as a defendant in a civil complaint that was filed in the U.S. District Court for the Middle District of Florida on February 8, 2016 by plaintiff Jonathan Torres. The complaint asserted claims of breach of implied contract, negligence and violations of the Florida Unfair and Deceptive Trade Practices Act arising from the Company's alleged failure to safeguard customer credit card information and the alleged failure to provide notice that credit card

information had been compromised. The complaint sought certification of a putative nationwide class of consumers impacted by the alleged failures. The plaintiff sought monetary damages, injunctive and equitable relief, attorneys' fees and other costs. The Company's motion to dismiss the complaint was granted, without prejudice, on July 15, 2016.

An amended complaint was filed in the same court by plaintiff Jonathan Torres and six additional named plaintiffs on July 29, 2016. The amended complaint names the Company's subsidiary, Wendy's International, LLC ("Wendy's International"), as the defendant and asserts claims of breach of implied contract, negligence and violations of state consumer protection or deceptive trade practices statutes in the states of Florida, New York, New Jersey, Mississippi, Tennessee and Texas arising from Wendy's International's alleged failure to safeguard customer credit card information and the alleged failure to provide notice that credit card information had been compromised. The amended complaint also asserts violations of state data breach statutes in Florida, New York, New Jersey, Tennessee and Texas based on Wendy's International's alleged failure to timely and fully disclose the alleged data breach. The amended complaint seeks certification of a putative nationwide class of consumers impacted by the alleged failures, or in the alternative, statewide classes for Florida, New York, New Jersey, Mississippi, Tennessee and Texas. The plaintiffs seek monetary damages, injunctive and equitable relief, attorneys' fees and other costs.

The Company was named as a defendant in a civil complaint that was filed in the U.S. District Court for the Western District of Pennsylvania on April 25, 2016 by plaintiff First Choice Federal Credit Union. The complaint asserts claims of common law negligence, negligence per se due to the alleged violation of section 5 of the Federal Trade Commission Act, and declaratory and injunctive relief. All of these claims are based on the allegations arising from the Company's alleged failure to safeguard customer credit card information and the alleged failure to provide notice that credit card information had been compromised. The complaint sought certification of a putative nationwide class of banks, credit unions, financial institutions and other entities in the United States impacted by the alleged failures. The plaintiff sought monetary damages, a declaratory judgment, injunctive relief, attorneys' fees and other costs.

The Company was named as a defendant in four other civil complaints filed by financial institutions in the U.S. District Court for the Western District of Pennsylvania based on the allegations arising from the Company's alleged failure to safeguard customer credit card information and the alleged failure to provide notice that credit card information had been compromised. These cases were consolidated into the First Choice Federal Credit Union case.

An amended civil complaint was filed in the consolidated proceeding in the U.S. District Court for the Western District of Pennsylvania on July 22, 2016 naming

the Company and two of its subsidiaries as defendants. The amended complaint was brought by 22 financial institutions and five association plaintiffs (representing members who are credit unions and other similar financial institutions). The amended complaint asserts claims of common law negligence, negligence per se due to the alleged violation of section 5 of the Federal Trade Commission Act, violation of the Ohio Deceptive Trade Practices Act, and declaratory and injunctive relief. The amended complaint also seeks certification of a putative nationwide class of banks, credit unions, financial institutions and other entities in the United States impacted by the alleged failures. The plaintiffs seek monetary damages, a declaratory judgment, injunctive relief, attorneys' fees and other costs.

***The Company believes it has meritorious defenses to each of the actions described above and intends to vigorously oppose the claims asserted in each of the complaints.***

(Emphasis added).

150. Thus, because the Board has already determined that it believes that the allegations in the Financial Institutions' Class Action and Consumer Class Action are without merit, and because the instant action is substantially based on the same and/or similar misconduct as the Financial Institutions' Class Action and Consumer Class Action, the Current Director Defendants are incapable of making an independent and disinterested decision to institute and vigorously prosecute this derivative action.

151. Additionally, as discussed above, during the 2012 4Q Earnings Call, defendant Brolick admitted that the Company's POS system was outdated, stating "[b]ut there is a fairly high percentage of our system that has fairly old POS software, and they're going to need to evolve to this fairly quickly. There are also franchisees, however, who have quite recently made important investments in what we call modern POS hardware as well as software. They will eventually have to transition out of that into the common platform that we have identified, which is NCR's Aloha. But that might be 5 years down the road for them. But again, they have modern POS that can run this. So that's not an issue. But to do the things we want longer term,

there -- they, too, are eventually going to have to change. But there's a decent piece of the system that's going to have to move to this really pretty quickly."

152. Based on the foregoing, defendants N. Peltz, May, Brolick, Hill, Levato and Rothschild<sup>12</sup>, six out of the eleven Current Director Defendants, knew that the Company's POS system was outdated and inadequate and breached their fiduciary duties by failing to take timely action to update the POS system and ensure that it was PCI DSS compliant. As such, a majority of the Current Director Defendants face a substantial likelihood of liability rendering demand upon them as futile.

153. Further, a majority of the Current Director Defendants have deep-rooted longstanding relationships with each other, thus rendering demand upon them as futile.

***Trian Partners and Triangle***

154. With respect to defendants N. Peltz, May, Kass, Levato, and M. Peltz, pursuant to the 2016 Proxy, each of the foregoing Current Director Defendants are/were employed by and/or affiliated with each other in the following ways: (i) defendant N. Peltz has served as CEO and founding partner of Trian Partners since November 2005, from January 1989 to April 1993, N. Peltz was Chairman and CEO of Trian Group, Limited Partnership, which provided investment banking and management services for entities controlled by N. Peltz and defendant May, and from 1983 to December 1988, N. Peltz was Chairman and CEO and a director of Triangle; (ii) defendant May has been President and a founding partner of Trian Partners since November 2005, from January 1989 to April 1993, May was President and COO of Trian Group, Limited Partnership, and from 1983 to December 1988, he was President and COO and a director of Triangle; (iii) defendant Kass currently serves as an Advisory Partner of Trian

---

<sup>12</sup> Defendants Peltz, May, Brolick, Hill, Levato and Rothschild were all serving on the Board during the time of the 2012 4Q Earnings Call.

Partners; (iv) defendant Levato was Senior Vice President and Chief Financial Officer of Trian Group, Limited Partnership, from January 1992 to April 1993 and From 1984 to December 1988, Levato served as Senior Vice President and CFO of Triangle; and (v) defendant M. Peltz is a Partner and has been a member of the Investment Team of Trian Partners and is the son of defendant N. Peltz. Therefore, given their longstanding deep rooted ties to each other, defendants N. Peltz, May, Kass, Levato and M. Peltz are incapable of independently considering a demand to bring suit against one another and accordingly, demand is futile.

155. With respect to Peltz and May, according to the 2016 Proxy, as of March 28, 2016, Trian Partners was the beneficial owner of 40,792,537 (15.3%) shares of Wendy's common stock. As set forth in the Company's 2015 10-K under the section entitled "Risk Factors," Wendy's concedes that its Board is controlled by Current Director Defendants Peltz and May, who both beneficially own more than 20% of the outstanding shares of Wendy's common stock:

***A substantial amount of the Company's Common Stock is concentrated in the hands of certain stockholders.***

Nelson Peltz, the Company's Chairman and former Chief Executive Officer, Peter May, the Company's Vice Chairman and former President and Chief Operating Officer, and Edward Garden, who resigned as a director of the Company on December 14, 2015, beneficially own shares of the Company's outstanding Common Stock that collectively constitute more than 20% of its total voting power as of February 29, 2016. Messrs. Peltz, May and Garden may, from time to time, acquire beneficial ownership of additional shares of Common Stock.

On December 1, 2011, the Company entered into an agreement (the "Trian Agreement") with Messrs. Peltz, May and Garden, and several of their affiliates (the "Covered Persons"). Pursuant to the Trian Agreement, the Board of Directors, including a majority of the independent directors, approved, for purposes of Section 203 of the Delaware General Corporation Law ("Section 203"), the Covered Persons becoming the owners (as defined in Section 203(c)(9) of the DGCL) of or acquiring an aggregate of up to (and including), but not more than, 32.5% (subject to certain adjustments set forth in the Agreement) of the outstanding shares of the Company's Common Stock, such that no such persons

would be subject to the restrictions set forth in Section 203 solely as a result of such ownership (such approval, the “Section 203 Approval”).

The Trian Agreement (other than the provisions relating to the Section 203 Approval and certain miscellaneous provisions that survive the termination of the agreement) terminated pursuant to the termination provisions of the Trian Agreement after funds affiliated with the Covered Persons sold 16.2 million shares of the Company’s Common Stock on January 15, 2014, thereby decreasing the Covered Persons’ beneficial ownership to less than 25% of the outstanding voting power of the Company as of that date. The Covered Persons sold an additional 2.0 million shares of the Company’s Common Stock on February 25, 2014. On July 17, 2015, the Company repurchased 18.4 million shares of the Company’s Common Stock from the Covered Persons. The terminated provisions of the Trian Agreement included provisions restricting the Covered Persons in the following areas: (i) beneficial ownership of Company voting securities; (ii) solicitation of proxies or submission of a proposal for the vote of stockholders under certain circumstances; (iii) certain affiliate transactions with the Company; and (iv) voting of certain Company voting securities.

***This concentration of ownership gives Messrs. Peltz, May and Garden significant influence over the outcome of actions requiring stockholder approval, including the election of directors and the approval of mergers, consolidations and the sale of all or substantially all of the Company’s assets.*** They are also in a position to have significant influence to prevent or cause a change in control of the Company. If in the future Messrs. Peltz, May and Garden were to acquire more than a majority of the Company’s outstanding voting power, they would be able to determine the outcome of the election of members of the Board of Directors and the outcome of corporate actions requiring majority stockholder approval, including mergers, consolidations and the sale of all or substantially all of the Company’s assets. They would also be in a position to prevent or cause a change in control of the Company.

156. Additionally, the 2016 Proxy states the following under the section entitled “Related Person Transactions Since the Beginning of 2015,” in relevant part:

On June 2, 2015, the Company entered into a stock purchase agreement to repurchase shares of our Common Stock from Nelson Peltz, Peter W. May and Edward P. Garden and certain of their family members and affiliates, investment funds managed by Trian Partners, an investment management firm controlled by Messrs. Peltz, May and Garden, and the general partner of certain of those investment funds (together with Messrs. Peltz, May and Garden, certain of their family members and affiliates and Trian Partners, the “Trian Group”), who in the aggregate owned approximately 24.8% of our outstanding shares as of May 29, 2015. Pursuant to the agreement, the Trian Group agreed not to tender or sell any of its shares in the \$639 million modified Dutch auction tender offer the Company commenced on June 3, 2015. Also pursuant to the agreement, the Company



agreed, following completion of the tender offer, to purchase from the Trian Group a pro rata amount of its shares based on the number of shares the Company purchased in the tender offer, at the same price received by stockholders who participated in the tender offer. On July 17, 2015, after completion of the tender offer, the Company repurchased 18.4 million shares of our Common Stock from the Trian Group at the price paid in the tender offer of \$11.45 per share, for an aggregate purchase price of \$210.9 million.

On December 1, 2011, the Company entered into an agreement with Trian Partners and certain of its affiliates, including Nelson Peltz, Peter W. May and Edward P. Garden (collectively, the “Covered Persons”). Pursuant to the agreement, the Board of Directors, including a majority of the independent directors, approved, for purposes of Section 203 of the Delaware General Corporation Law, the Covered Persons becoming the owners of or acquiring an aggregate of up to 32.5% (subject to certain adjustments set forth in the agreement) of the outstanding shares of our Common Stock, such that no such persons would be subject to the restrictions set forth in Section 203 solely as a result of such ownership (such approval, the “Section 203 Approval”). The agreement (other than the provisions relating to the Section 203 Approval and certain miscellaneous provisions) terminated pursuant to its termination provisions on January 15, 2014.

Each of the related person transactions described above was *reviewed and approved by the Audit Committee* in accordance with the terms of its written charter and the RPT Policy.

157. Based on the foregoing, with respect to defendant Levato, Levato has served as the Chairman of the Audit Committee since prior to the beginning of the Relevant Period and, according to the Audit Committee Charter, Levato is required to satisfy the independence requirements pursuant to Section 10A of the Securities Exchange Act of 1934. Additionally, pursuant to the Audit Committee Charter, Levato was responsible for reviewing and approving the foregoing related party transactions involving defendants Peltz and May. Yet, given Levato’s prior employment with the Company, Trian Group, Limited Partnership and Triangle, Levato has longstanding ties with Peltz and May and therefore, he is not and cannot be considered an independent director and should not have been responsible for reviewing and approving the related party transactions. Accordingly, demand upon Levato is futile and must be excused.

158. With respect to defendant Brolick, Brolick has served as a director of the Company since September 2011 and previously served as President and CEO of the Company from September 2011 to January 2016 and as CEO until his retirement from management duties on May 26, 2016. As conceded by the Company in the 2016 Proxy, defendant Brolick is not an independent director due to his insider status. Additionally, as demonstrated above, Brolick has repeatedly failed to make and/or failed to cause the Company to make full and fair disclosure to the public regarding the effectiveness of the Company's data security policies and regarding the scope and effects of the Data Breach. Accordingly, Brolick is incapable of independently exercising his business judgment thus rendering demand futile.

159. With respect to defendant Penegor, Penegor has served as a director of the Company since May 2016 and as CEO of the Company since May 27, 2016. Penegor joined the Company in June 2013 and served as the President and CFO of Wendy's from January 2016 to May 2016, as Executive Vice President, CFO and International from December 2014 to January 2016 and as Senior Vice President and CFO from September 2013 to December 2014. As conceded by the Company in the 2016 Proxy, Penegor is not an independent director due to his insider status.

160. Further, according to the 2015 Proxy, the Company stated that Penegor, "who was promoted from Senior Vice President and Chief Financial Officer to Executive Vice President, Chief Financial Officer and International, took on additional oversight of the Company's International division, *in addition to maintaining his existing responsibilities for Finance, Development and Information Technology.*" Thus, given that Penegor was primarily responsible for overseeing the Company's information technology department, Penegor either knew or should have known that the Company's data security systems were inadequate and

ineffective and had a duty to implement and oversee effective internal controls over the Company's data security policies. This is especially true given the Company's longstanding recognition of the potential adverse material effect that a data security breach could have on the Company's operations. Based on defendant Penegor's utter failure to implement an effective data security program and monitor the Company's compliance with the foregoing, as well as federal, state and local regulations governing data security and privacy (including, as conceded by the Company, compliance with payment card industry rules), Penegor faces a substantial likelihood of liability rendering him incapable of exercising his business judgment and demand futile.

161. With respect to defendant Mathews-Spradlin, Mathews-Spradlin has served as a director of the Company since February 2015. From 1993 until her retirement in 2011, Mathews-Spradlin worked at Microsoft Corporation, where she served as Chief Marketing Officer ("CMO") and Senior Vice President, Central Marketing Group from 2005 to 2011, Corporate Vice President, Marketing from 2001 to 2005, Vice President, Corporate Public Relations from 1999 to 2001 and head of the Corporate Public Relations function from 1993 to 1999. According to the 2016 Proxy, the Company touts that Mathews-Spradlin "possesses extensive experience in global brand management and a *deep understanding of the technology industry* attributable to her background as a senior executive at Microsoft Corporation." Thus, given Mathews-Spradlin's extensive background in technology due to her long tenure at Microsoft, she either knew or should have known that the Company's data security systems were inadequate and ineffective and had a duty to implement and oversee effective internal controls over the Company's data security policies. This is especially true given the Company's longstanding recognition of the potential adverse material effect that a data security breach could

have on the Company's operations. Based on defendant Mathews-Spradlin's utter failure to implement an effective data security program and monitor the Company's compliance with the foregoing, as well as federal, state and local regulations governing data security and privacy (including, as conceded by the Company, compliance with payment card industry rules), Mathews-Spradlin faces a substantial likelihood of liability rendering her incapable of exercising her business judgment and demand futile.

162. Notwithstanding the foregoing affiliations among the Current Director Defendants, the following Current Director Defendants also have longstanding ties to each other based on the fact that they either previously served as officers or directors of certain of the Company's subsidiaries and/or Wendy's International prior to its merger with the Company in September 2008: (i) N. Peltz previously served as the Company's Chairman and CEO and as a director or manager and an officer of certain of the Company's subsidiaries from April 1993 through June 2007; (ii) May served as the President and COO and as a director or manager and an officer of certain of the Company's subsidiaries from April 1993 through June 2007; (iii) Brolick previously worked at Wendy's International for 12 years, last serving as Senior Vice President of New Product Marketing, Research and Strategic Planning; (iv) Hill served as a director of Wendy's International from 1994 until its merger with the Company in September 2008; and (v) Levato served as Executive Vice President and CFO of the Company and certain of its subsidiaries from April 1993 to August 1996. Therefore, given their longstanding deep rooted ties to each other, defendants N. Peltz, May, Brolick, Hill and Levato are incapable of independently considering a demand to bring suit against one another and accordingly, demand is futile.

163. Finally, as stated in the 2016 Proxy, the entire Board was responsible for risk oversight, and the Board's risk oversight function is supported by a Risk Oversight Committee, which is comprised of members of senior management:

#### **Board's Role in Risk Oversight**

The Board of Directors provides oversight with respect to the Company's risk assessment and risk management activities, which are designed to identify, prioritize, assess, monitor and mitigate material risks to the Company, including financial, operational, compliance and strategic risks. While the Board has primary responsibility for risk oversight, the Board's standing committees support the Board by regularly addressing various risks in their respective areas of responsibility. The Audit Committee focuses on financial risks, including reviewing with management, the Company's internal auditors and the Company's independent registered public accounting firm the Company's major risk exposures (with particular emphasis on financial risk exposures), the adequacy and effectiveness of the Company's accounting and financial controls and the steps management has taken to monitor and control such exposures, including the Company's risk assessment and risk management policies. The Compensation Committee considers risks presented by the Company's compensation policies and practices for its executive officers and other employees, as discussed below under the caption "Compensation Risk Assessment." The Nominating and Corporate Governance Committee reviews risks related to the Company's corporate governance structure and processes, including director qualifications and independence, stockholder proposals related to governance, succession planning and the effectiveness of our Corporate Governance Guidelines. *The Board's risk oversight function is also supported by a Risk Oversight Committee composed of members of senior management. The Risk Oversight Committee is exclusively devoted to prioritizing and assessing all categories of enterprise risk, including risks delegated by the Board of Directors to the Board committees, as well as other operational, compliance and strategic risks facing the Company.* Each of these committees reports directly to the Board.

(Emphasis added).

164. Based on the foregoing, it can be reasonably inferred that the Board had knowledge of the Company's inadequate and data security measures, given that the Company has acknowledged in its annual statements dating back to 2008 of the potential adverse effect that a security breach would have on the Company's operations. Further, given that the majority of the Company's restaurants are franchisee-owned and the Company derives a substantial

portion of its revenue from its franchisees, the Board either was or should have been aware of the DavCo Lawsuit, especially since DavCo is one of the Company's largest franchisees and Wendy's initiated the lawsuit. Therefore, it can be reasonably inferred that a majority of the Current Director Defendants were on notice of the multiple pervasive problems with the Aloha POS system and yet, failed to take action to address and resolve the deficiencies, including taking steps to ensure that the Company's data security measures were compliant with payment card industry standards. The Board's continued failure to act is further evidenced by the fact that the Company is still utilizing the Aloha POS system despite that restaurants that were using the Aloha POS system were also impacted by the Data Breach, as the Company effectively admitted in its reply to DavCo's Amended Counterclaim. This constitutes bad faith and accordingly, a majority of the Current Director Defendants faces a substantial likelihood of liability rendering them incapable of independently exercising their business judgment and demand futile.

165. The Individual Defendants' conduct described herein and summarized above demonstrates a pattern of misconduct that could not have been the product of legitimate business judgment as it was based on intentional, reckless, and disloyal misconduct. Thus, none of the Individual Defendants, who constitute a majority of the current Board of the Company, can claim exculpation from their violations of duty pursuant to the Company's charter (to the extent such a provision exists). As a majority of the Individual Defendants faces a substantial likelihood of liability, they are self-interested in the transactions challenged herein and cannot be presumed to be capable of exercising independent and disinterested judgment about whether to pursue this action on behalf of the shareholders of the Company.

166. Based on the foregoing, the Current Director Defendants face a sufficiently substantial likelihood of liability and accordingly, there is a reasonable doubt as to each

Defendant's disinterestedness in deciding whether pursuing legal action would be in the Company's best interest. Accordingly, demand upon the Current Director Defendants is excused as being futile.

## **CAUSES OF ACTION**

### **COUNT I**

#### **(Against the Individual Defendants for Breach of Fiduciary Duty)**

167. Plaintiff incorporates by reference and realleges each of the foregoing allegations as though fully set forth herein.

168. The Individual Defendants owed and owe Wendy's fiduciary obligations, including the obligations of good faith, fair dealing, loyalty and care. Among other things, the Individual Defendants owed a fiduciary duty to Wendy's to supervise the issuance of its press releases and public filings and ensure that they were truthful, accurate and conformed to federal and state securities law. The Individual Defendants breached their duties of loyalty, care and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures with respect to data security for the Company and its franchisees; (ii) failing to exercise their oversight duties by not monitoring the Company's compliance with federal and state laws, payment card industry regulations and its agreements with payment card processors and networks; (iii) failing to cause the Company to make full and fair disclosure concerning (a) the effectiveness of the Company's policies and procedures with respect to data security, and (b) the scope and impact of the Data Breach, resulting in the commencement of the Financial Institutions Class Action and Consumer Class Action; (iv) permitting the Company to violate the PCI DSS by, among other things, (a) allowing Wendy's to knowingly operate its point-of-sale system on outdated and unsupported software; (b) failing to ensure that the Company installed and maintained an adequate firewall; (c) failing to ensure that payment card data was properly

segmented from the remainder of Wendy's network; (d) failing to implement necessary protocols, such as software image hardening, password protecting programs that captured payment card data and encrypting payment card data at the point-of-sale; and (e) failing to upgrade the Company's systems to utilize EMV technology; (v) consciously disregarding the systemic and pervasive problems with the Aloha POS system; (vi) consciously permitting the Company to maintain an out of date operating system; and (vii) failing to exercise their oversight duties commensurate with the risk, given the recognition by senior management and the Board that a security breach could adversely affect the Company's business and operations, as evidenced by the fact that the Data Breach went undetected for several months and, it was not until after receiving questions from a third-party concerning banking industry sources who discovered a pattern of fraud on cards that were used at various Wendy's locations that the Company publicly acknowledged that it was investigating claims of a possible credit card breach at some locations.

169. By reason of the foregoing, Wendy's was damaged.

**COUNT II**  
**(Against the Individual Defendants for Waste of Corporate Assets)**

170. Plaintiff incorporates by reference and realleges each of the foregoing allegations as though fully set forth herein.

171. Defendants breached their fiduciary duties by failing to properly supervise and monitor Wendy's by allowing the Company to engage in an illegal, unethical and improper course of conduct.

172. As a result of the Individual Defendants' illicit course of conduct and breaches of fiduciary duty, Wendy's has wasted valuable corporate assets through payments of compensation to the Individual Defendants because the Company has incurred significant potential liability



for legal costs, penalties, fines, and/or legal fees in connection with the defense of the Individual Defendants' unlawful course of conduct complained of herein.

173. Additionally, the wrongful conduct alleged herein includes the Individual Defendants' failure to implement adequate internal controls to detect and prevent the Data Breach. Under the Individual Defendants' direction, customers' personal information was unlawfully obtained by unauthorized persons. The Company has already incurred substantial costs in connection with the Data Breach, including investigating and attempting to remedy the breach, and expects to incur even more costs.

174. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company.

175. By reason of the foregoing, Wendy's was damaged.

**COUNT III**  
**(Against the Individual Defendants for Unjust Enrichment)**

176. Plaintiff incorporates by reference and realleges each of the foregoing allegations as though fully set forth herein.

177. Through the wrongful course of conduct and actions complained of herein, the Individual Defendants were unjustly enriched at the expense of, and to the detriment of Wendy's. The wrongful conduct was continuous and resulted in ongoing harm to the Company. The Individual Defendants were unjustly enriched pursuant to receiving compensation and/or director remuneration while breaching their fiduciary duties to the Company, as alleged herein.

178. Plaintiff, as a shareholder of Wendy's, seeks restitution from the Individual Defendants, and seeks an order of this Court disgorging all profits, benefits, and other

compensation obtained by the Individual Defendants, from their wrongful course of conduct and fiduciary breaches.

179. By reason of the foregoing, Wendy's was damaged.

**COUNT IV**  
**(Derivatively Against the Individual Defendants for Gross Mismanagement)**

180. Plaintiff incorporates by reference and re-alleges each and every allegation contained above, as though fully set forth herein.

181. By their actions alleged herein, the Individual Defendants, either directly or through aiding and abetting, abandoned and abdicated their responsibilities and fiduciary duties with regard to prudently managing the assets and business of Wendy's in a manner consistent with the operations of a publicly held corporation.

182. As a direct and proximate result of the Individual Defendants' gross mismanagement and breaches of duty alleged herein, Wendy's has sustained significant damages.

183. As a result of the misconduct and breaches of duty alleged herein, the Individual Defendants are liable to the Company.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff demands judgment as follows:

A. Directing Defendants to account to Wendy's for all damages sustained or to be sustained by the Company by reason of the wrongs alleged herein;

B. Directing Wendy's to take all necessary actions to reform its corporate governance and internal procedures to comply with applicable laws and protect the Company and its shareholders from a recurrence of the events described herein, including, but not limited to, a shareholder vote resolution for amendments to Wendy's By-Laws or Articles of

Incorporation and taking such other action as may be necessary to place before shareholders for a vote on corporate governance policies;

C. Awarding to Wendy's restitution from the Defendants and ordering disgorgement of all profits, benefits and other compensation obtained by the Individual Defendants.

D. Awarding Plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees and expenses; and

E. Granting such other and further relief as the Court may deem just and proper.

**JURY DEMAND**

Plaintiff demands a trial by jury.

December 16, 2016

Respectfully submitted,

OF COUNSEL:

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

FARUQI & FARUQI, LLP  
Nadeem Faruqi  
Nina M. Varindani  
685 Third Avenue, 26th Floor  
New York, NY 10017  
Telephone: 212-983-9330  
Facsimile: 212-983-9331

By: /s/Richard S. Wayne  
Richard S. Wayne (0022390)  
William K. Flynn (0029536)  
Thomas P. Glass (0062382)  
STRAUSS TROY  
The Federal Reserve Building  
150 East Fourth Street  
Cincinnati, OH 45202-4018  
Telephone: (513) 621-2120  
Facsimile: (513) 629-9426

*Attorneys for Plaintiff*


Word Online

Download Save to OneDrive Print Find ...

RULE 23.1 VERIFICATION

I, James Graham, am the named Plaintiff to this action. I am a shareholder of The Wendy's Company (the "Company"), and have been at all times throughout the Relevant Period, and approve the filing of this Complaint. I have reviewed the allegations made in this VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT and state that the matters stated therein about which I have personal knowledge are true, and that the other matters stated therein are true and accurate to the best of my knowledge, information and belief, based in part upon the investigation conducted by counsel. Having received a copy of this Complaint, having reviewed it with my counsel, I hereby authorize its filing.

I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 8 day of December, 2016.

  
James Graham