STANFORD DIRECTORS COLLEGE 2014

PANEL DISCUSSION

June 23, 2014

CYBERSECURITY AND THE BOARD

READING MATERIALS FOR BOARD MEMBERS ON CYBERSECURITY ATTACKS

GORDON K. DAVIDSON
LAURA FINLEY
ADAM DERRY

FENWICK & WEST LLP
fenwick.com

©FENWICK & WEST LLP 2014

I. BEST PRACTICES TO PREVENT AND MITIGATE CYBER ATTACKS:

A. Company-wide Best Practices

1. **National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity – Version 1.0*, 2014**

   a. **Description:** Framework of industry standards and best practices to help organizations manage cybersecurity risks

   b. **Link:** http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

2. **Online Trust Alliance, *2014 Data Protection & Breach Readiness Planning Guide*, 2014**

   a. **Description:** Succinct guide outlining the key steps to create and implement an incident response plan

   b. **Link:** https://www.otalliance.org/system/files/files/resource/documents/2014otadatabreachguide4.pdf

3. **American National Standards Institute, *The Financial Management of Cyber Risk – An Implementation Framework for CFOs*, 2010**

   a. **Description:** Provides a framework for understanding risks, implementing a risk management plan and managing legal and compliance issues

   b. **Link:** http://publicaa.ansi.org/sites/apdl/khdoc/Financial+Management+of+Cyber+Risk.pdf

4. **United States Cyber Consequences Unit, *The U.S. CCU Cyber-Security Check List*, 2007**

   a. **Description:** Comprehensive checklist to help companies evaluate whether information security guidelines have been met

   b. **Link:** http://www.usccu.us/documents/US-CCU%20Cyber-Security%20Check%20List%202007.pdf

5. **National Institute of Standards and Technology (NIST*), Information Security Handbook: A Guide for Managers*, 2006**

   a. **Description:** Provides a broad overview of the critical elements in an information security program, with risk management and mitigation suggestions/examples and easy to read flow charts/tables

b. **Link:** http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

B. Board of Directors Best Practices

1. **The Conference Board, *The Board's Role in Cybersecurity*, March 2014**

   a. **Description:** Approaches cybersecurity from a governance perspective and provides suggestions for how directors can carry out an oversight role.

   b. **Link:** http://www.goodharbor.net/media/pdfs/Good_Harbor_Directors_Note_Cyber.pdf

2. **Haynes and Boone, *Directors Beware: ISS Urges Ouster of Target's Directors in the Wake of its Data Breach*, 2014**

   a. **Desription:** Discusses the recent recommendation by ISS to oust seven of the Target's directors in connection with the company's recent data breach.

   b. **Link:** http://www.haynesboone.com/iss-urges-ouster-of-target-bod-members/

3. **DLA Piper, *Cybersecuirty and the Duty of Care: a Top 10 Checklist for Board Members***

   a. **Desription:** Outlines the 10 questions a director should be asking about a company's cybersecurity.

   b. **Link:** http://www.dlapiper.com/en-us/us/insights/publications/2014/01/cybersecurity-and-the-duty-of-care/

4. **World Economic Forum, *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World – Principles and Guidelines*, 2012**

   a. **Description:** Summarizes the cyber risk landscape and sets forth principles, guidelines and a C-Suite level checklist on cyber resilience

   b. **Link:** http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

5. **Deloitte, *Risk Intelligent Governance in the Age of Cyber Threats – What You Don't Know Could Hurt You*, 2012**

   a. **Description:** Outlines stages of risk management maturity at each organizational level and practical answers for directors to complex cyber risk questions

   b. **Link:** https://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/IMOs/Governance%20and%20Risk%20Management/us_grm_riskintelligentcybergovernance_012512.pdf

6. **British-North American Committee, *Cyber Attack: A Risk Management Primer for CEOs and Directors*, 2007**

   a. **Description:** Lists the primary mistakes that CEOs and directors make with respect to cybersecurity and provides answers to probing questions to help formulate an effective security approach

   b. **Link:** http://www.atlanticcouncil.org/publications/reports/cyber-attack-risk-management-primer-for-ceos

©FENWICK & WEST LLP 2014

II. SURVEYS AND STUDIES ON CYBERSECURITY:

1. **Congressional Research Service, *Cybersecurity: Authoritative Reports and Resources, by Topic*, 2014**

   a. **Description:** Comprehensive list of all recent legislation, executive orders and reports on cybersecurity

   b. **Link:** http://www.fas.org/sgp/crs/misc/R42507.pdf

2. **IBM Security Services, *Data Breach Statistics – An Information Resource for Data Breach Prevention and Response*, April 2014**

   a. **Description:** IBM conducted its own research on data breaches and compile that research in this report, along with information on how companies are responding to these threats.

   b. **Link:** http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/

3. **Verizon, *2014 Data Breach Investigations Report*, 2014**

   a. **Description:** Outlines nine common incident patterns, with insights from 50 global organizations and over 60,000 incidents, with steps needed to counter threats.

   b. **Link:** http://www.verizonenterprise.com/DBIR/2014/

4. **Cylab, *Carnegie Mellon University, Governance of Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives are Managing Cyber Risks*, 2012**

   a. **Description:** Discusses the results of a biennial survey examining how directors and senior management deal with cybersecurity issues

   b. **Link:** http://www.hsgac.senate.gov/download/carnegie-mellon-cylab-cybersecurity-report

5. **Deloitte, *National Association of State Chief Information Officers, 2012 Deloitte-NASCIO Cybersecurity Study*, 2012**

   a. **Description:** Analyzes survey responses from state information security representatives on cybersecurity budgeting, strategies and perspectives on emerging threats and compliance

   b. **Link:** http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_nascio%20Cybersecurity%20Study_10192012.pdf

6. **Ponemon Institute, *2012 Cost of Cyber Crime Study: United States*, 2012**

a. **Description:** Study on the average annualized cost of cyber crime from 56 representative US organizations

b. **Link:** http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

7. **FTI Consulting, Corporate Board Member, *Legal Risks on the Radar*, 2012**

a. **Description:** Survey on the legal issues, including cyber risk, about which directors and corporate general counsel are currently most concerned

b. **Link:** http://www.fticonsulting.com/global2/media/collateral/united-states/legal-risks-on-the-radar.pdf

III. STANDARDS AND LAWS RELATED TO CYBERSECURITY:

A. Proposed Legislation

1. **Overview:** While a significant number of cybersecurity bills were introduced in the House and Senate in recent years, no major cybersecurity legislation has become law since the Federal Information Security Management Act of 2002 (FISMA). Below are materials on a few of the most notable recent bills.

2. **Cyber Intelligence Sharing and Protection Act**

   a. **Description:** Controversial legislation, which allows sharing of Internet traffic data between companies and the government to detect and protect critical infrastructure against cyber attacks

   b. **Text:** http://www.gpo.gov/fdsys/pkg/BILLS-113hr624rfs/pdf/BILLS-113hr624rfs.pdf

   c. **Status:** The bill was approved by the House in April 2013, but was stalled and ultimately not voted on in the Senate due to privacy concerns:

      i. International Business Times, *RIP CISPA: Senate Expected to Kill 2013 Cybersecurity Bill*: http://www.ibtimes.com/print/rip-cispa-senate-expected-kill-2013-cybersecurity-bill-1220739

      ii. US News, *ACLU: CISPA is Dead (For Now)*: http://www.usnews.com/news/articles/2013/04/25/aclu-cispa-is-dead-for-now

3. **Federal Information Security Amendments Act of 2013**

   a. **Description:** Updates FISMA to address a perceived shortcoming by moving security audits away from a static checkbox mindset to a continuous monitoring approach

   b. **Text:** http://www.gpo.gov/fdsys/pkg/BILLS-113hr1163ih/pdf/BILLS-113hr1163ih.pdf

   c. **Status:** Unanimously approved by the House in April 2013; however, its future is uncertain in the Senate, which may opt to combine a series of bills rather than approve cybersecurity legislation piecemeal

4. **Cybersecurity Enhancement Act of 2013**

   a. **Description:** Establishes a task force with representatives from the federal government, private sector and academia to coordinate R&D on cybersecurity and improve training of cyber professionals

   b. **Text:** http://www.gpo.gov/fdsys/pkg/BILLS-113hr756rfs/pdf/BILLS-113hr756rfs.pdf

c. **Status:** Approved by a 402-16 vote in the House in April 2013; however, its future is uncertain in the Senate, which may opt to combine a series of bills rather than approve cybersecurity legislation piecemeal

5. Cybersecurity Act of 2012

a. **Description:** The most comprehensive cybersecurity legislation proposed to date, with three primary elements: 1) new threat information sharing between the government and private industry; 2) better protection of critical infrastructure; and 3) authority for the Department of Homeland Security to unite federal resources to lead a cybersecurity team

b. **Text:** http://www.gpo.gov/fdsys/pkg/BILLS-112s2105pcs/pdf/BILLS-112s2105pcs.pdf

c. **Status:** Voted down by the Senate in August 2012 due to concerns over privacy and scope of governmental regulation:

i. EastWest Institute, *The Failed Cybersecurity Act of 2012*: http://www.ewi.info/idea/failed-cybersecurity-act-2012

ii. Digital Trends, *Senate Kills Cybersecurity Act of 2012*: http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/

B. Enacted Legislation

1. Federal

a. **Federal Information Security Management Act of 2002**

i. **Description**: Requires federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget to implement policies and procedures to cost-effectively strengthen information system security

ii. **Text**: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

b. **Other Applicable Laws:**

i. Health Information Technology for Economic and Clinical Health Act of 2009 (42 U.S.C. § 201, *et seq*.)

ii. Veterans Affairs Information Security Enhancement Act of 2006 (38 U.S.C. §§ 5721-5728)

iii. Gramm-Leach-Bliley Act of 1999 (15 U.S.C. § 6801(b))

iv. Children's Online Privacy Protection Act of 1998 (15 U.S.C. §§ 6501-6506)

v. Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d-1320d-8)

vi. Fair Credit Reporting Act of 1970 (15 U.S.C. §§ 1681-1681x)

vii. Federal Trade Commission Act of 1914 (15 U.S.C. §§ 45-58)

2. State Notification Laws and Requirements:

a. Practical Law Company, *State Agency Notice Requirements for Data Breaches Chart*, 2012

i. **Description:** Comprehensive, state-by-state chart showing when notification requirements are triggered in a data breach and how to comply when triggered

ii. **Link:** http://www.kelleydrye.com/publications/articles/1552/_res/id=Files/index=0/State%20Agency%20Notice%20Requirements%20for%20Data%20Breaches%20Chart%20(5-501-9110)%207%205%2012.pdf

b. Fenwick & West LLP, "Data Breach Laws Become Even Stricter for all Companies with California or Massachusetts Customers or Users," March 7, 2012:

i. **Description:** Summarizes how California and Massachusetts recently implemented stricter standards in each state's respective data breach regulatory schemes

ii. **Link to Article:** http://www.fenwick.com/FenwickDocuments/EIM_Alert_03-07-12.pdf

iii. **Text of CA SB-24:** http://leginfo.ca.gov/pub/11-12/bill/sen/sb_0001-0050/sb_24_bill_20110831_chaptered.pdf

iv. **Text of MA Data Breach Standards:** http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

C. Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636), 2013

1. Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636)

a. Description: Directs federal agencies to develop voluntary cybersecurity standards for critical parts of the private sector, consider proposing new mandates where possible under existing law and produce and share unclassified reports of threats to U.S. companies in real time

b. Text of EO 13636: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

c. NIST Framework issued on February 12, 2014 in accordance with EO 13636:

i. Text of Framework: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

ii. Articles explaining framework:

A. NIST Unveils Cybersecurity Framework, February 2014: http://www.jdsupra.com/legalnews/nist-unveils-cybersecurity-framework-18043/

B. New Cybersecurity Framework Revealed, April 2014: http://www.morganlewis.com/pubs/acpp_lf_newcybersecurityframeworkrevealed_18april14.pdf

d. Articles Summarizing EO 13636:

i. NBC, "New rules for cybersecurity? Obama's executive order explained," February 13, 2013: http://scitech.nbcnews.com/_news/2013/02/13/16954043-new-rules-for-cybersecurity-obamas-executive-order-explained

ii. InformationWeek, "White House Cybersecurity Executive Order: What It Means," February 13, 2013: http://www.informationweek.com/government/security/white-house-cybersecurity-executive-orde/240148460?printer_friendly=this-page

D. Formal Guidance and Widely Followed Standards

1. Division of Corporate Finance, Securities and Exchange Commission (SEC), *CF Disclosure Guidance: Topic No. 2 – Cybersecurity*, 2011

a. Description: SEC guidance on disclosure obligations relating to cybersecurity risks and cyber incidents

b. Text of Guidance: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

c. Recent Letters to and from SEC Chairman on Guidance:

i. Letter from Commerce Committee Chairman John D. Rockefeller IV to SEC Chairman Mary Jo White on SEC Cybersecurity Guidance, April 9, 2013: http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51

ii. Response Letter from Chairman White to Chairman Rockefeller on SEC Cybersecurity Guidance, May 1, 2013: http://articles.law360.s3.amazonaws.com/0441000/441415/512013%20Letter%20from%20SEC%20Chair%20White.pdf

d. **Articles Summarizing Guidance:**

i. International Association of Privacy Professionals, "Demystifying SEC Guidance on Cybersecurity Risk," March 7, 2013: https://www.privacyassociation.org/media/presentations/13Summit/S13_Demystifying_SEC_PPT.pdf

ii. Businessweek, "The SEC Says Speak Up About Hack Attacks," September 6, 2012: http://www.businessweek.com/printer/articles/70574-the-sec-says-speak-up-about-hack-attacks

2. **Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information, April 2014.**

a. **Description:** Explanation of the DOJ's and FTC's analytical framework for information sharing in the context of antitrust.

b. **Link:** http://www.justice.gov/atr/public/guidelines/305027.pdf

c. **Articles Summarizing the Policy Statement:**

i. Bryan Cave, *Will This Be Enough? Competitors Sharing Cyber Threat Information Will Not Result in Federal Antitrust Prosecutions – Sometimes*, April 16, 2014: http://www.bryancave.com/files/Publication/922ee132-e675-4110-b354-ea97117de0a3/Presentation/PublicationAttachment/afb9b07b-4253-4958-b9b6-1349c4e55f02/NatSecAlert_4.16.14.pdf

ii. Greenberg Traurig, *DOJ and FTC Opine on Information Sharing: When Cybersecurity Is Threatened, Antitrust Laws Are Not – If Properly Done*, May 20, 2014: http://www.martindale.com/antitrust-trade-regulation-law/article_Greenberg-Traurig-LLP_2149006.htm

3. **The SANS Institute, *Critical Controls for Effective Cyber Defense – Version 5*, 2014**

a. **Description:** Set of 20 controls prepared using five critical tenets: offense informs defense, prioritization, metrics, continuous diagnostics and mitigation, and automation.

b. **Link:** http://www.sans.org/critical-security-controls/cag4-1.pdf

4. **International Organization for Standardization, *ISO/IEC 27001* (2013), *ISO/IEC 27002* (2013)**

a. **ISO/IEC 27001 Description:** Mandates specific requirements with the intent to bring information security within control of management; a company can be certified compliant with ISO/IEC 27001

b. **ISO/IEC 27002 Description:** Provides best practice recommendations and standards for those managing information security management systems

c. **ISO/IEC 27001 and 27002 Available for Purchase:** http://www.standards-online.net/InformationSecurityStandard.htm

5. **Payment Card Industry Security Standards Council, *Payment Card Industry Data Security Standard (PCI DSS)*, 2013**

   a. **Description:** Provides a framework for prevention, detection and appropriate reaction to security incidents in payment card data processes; accompanying self-assessment questionnaires may be useful for evaluation of a company's compliance

   b. **Link (PCI DSS):** https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

   c. **Link (Self-Assessment Questionnaire):** https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

6. **NIST, *NIST SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations – Revision 3*, 2010**

   a. **Description:** Provides a foundation for the development of assessment methods and procedures for determining security control effectiveness; while developed for information systems in the federal government, commercial organizations often use the standards as a guideline

   b. **Link:** http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

7. **Examples of Targeted Standards Aimed at Protecting Specific Industries:**

   a. Aerospace Quality Management Standard (AS9100 based on ISO 9901)

   b. Numerous publications from the Software Assurance Forum for Excellence in Code (SAFECode)

   c. Health Information Trust Alliance (HITRUST) Common Security Framework

   d. IEC 80001 Application of Risk Management for IT Networks Incorporation Medical Devices

   e. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards (CIPs)

IV. PERTINENT ARTICLES ABOUT RECENT DATA BREACHES:

A. U.S. Corporate Attacks and Responses

1. **Bloomberg, "EBay Asks users to Change Passwords after Cyber-Attack," May 21, 2014:**

   a. **Description:** Details the EBay breach that prompted the company to urge users to change passwords. Contrasts EBay's prompt disclosure of the breach with other recent incidents involving companies that did not report data thefts to investors.

   b. **Link:** http://www.bloomberg.com/news/2014-05-21/ebay-asks-users-to-change-their-passwords-after-cyber-attack.html

2. **New York Times, "Heartbleed Internet Security Flaw Used in Attack," April 18, 2014:**

   a. **Description:** Reports on hackers taking advantages of a security flaw in servers to access user information. Explains the work of Universities to investigate server weakness and recommend fixes.

   b. **Link:** http://bits.blogs.nytimes.com/2014/04/18/heartbleed-internet-security-flaw-used-in-attack/

3. **Bloomberg Businessweek, "Investors Couldn't Care Less About Data Breaches," May 23, 2014:**

   a. **Description:** Summarizes the surprising lack of any negative impact on stock prices of recent security breach reports including Target, EBay and JPMorgan.

   b. **Link:** http://www.businessweek.com/articles/2014-05-23/why-investors-just-dont-care-about-data-breaches

4. **New York Times, "Adobe Breach Inadvertently Tied to Other Accounts," November 12, 2013:**

   a. **Description:** Criticizes Adobe for not adequately encrypting user data and chides users for recycling passwords both of which exacerbated the effect of the data breach.

   b. **Link:** http://bits.blogs.nytimes.com/2013/11/12/adobe-breach-inadvertently-tied-to-other-accounts/

5. **CBS News, "Retailers launch cybercrime info sharing center," May 15, 2014**

   a. **Description:** Announces the creation of a retailer cyber intelligence sharing center that will focus on data protection in the wake of recent data breaches.

   b. **Link:** http://www.cbsnews.com/news/retailers-launch-cybercrime-info-sharing-center/

B. International Attacks and Responses

1. **Wall Street Journal, "Alleged Chinese Hacking: Alcoa Breach relied on Simple Phishing Scam," May 19, 2014**

   a. **Description:** Discusses the unsophisticated alleged Chinese army Unit 61398 hacker attack on an American company.

   b. **Link:** http://online.wsj.com/news/articles/SB10001424052702303468704579572423369998070

2. **Venture Beat, "Iranian Hackers Attack Targets with Devious Weapon – The Friend Request," May 29, 2014**

   a. **Description:** Describes a multi-year Iranian operation that used fake identities on social networks to target as many as 2,000 individuals that included a U.S. Navy Admiral, journalists, the private sector in the U.K. and supporters of Israel.

   b. **Link:** http://venturebeat.com/2014/05/29/iranian-hackers-attack-targets-with-devious-weapon-the-friend-request/

3. **CBS News, "European Bank Hackers Stole $100 Million, U.S. says," June 2, 2014**

   a. **Description:** Discusses the charges filed against Evgeniy Bogachev, a Russian computer hacker accused of leading an international hacking effort that targeted hundreds of thousands of computers and stole more than $100 million.

   b. **Link:** http://www.cbsnews.com/news/european-bank-hackers-stole-100-million-u-s-says/

4. **Forbes, "How the Syrian Electronic Army Hacked Us," February 20, 2014:**

   a. **Description:** Breaks down the timeline of the phishing email attack waged by the Syrian Electronic Army that successfully targeted Forbes, and the five day recovery effort to patch server weakenesses.

   b. **Link:** http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/

5. **Reuters, "Hacker Group Threatens Cyber-attack on World Cup Sponsors," May 30, 2014**

   a. **Description:** Relays the threats made by the hacker group Anonymous to attack sponsors of the World Cup in opposition to lavish spending on the games in a nation with severe poverty**.**

b. **Link:** http://www.reuters.com/article/2014/05/30/brazil-worldcup-hackers-idUSL1N0OG1LV20140530

6. **CNN, "Cybercrime or Espionage? The Rules Just Changed," May 20, 2014**

a. **Description:** Announces the indictment by U.S. Attorney General Eric Holder against five Chinese nationals on charges of corporate cyber-theft which accuse the Chinese government of committed cyber espionage to attain an economic advantage in state-owned industry.

b. **Link:** http://www.cnn.com/2014/05/20/opinion/weinstein-cybercrime/

RECENT EXAMPLES OF CYBERSECURITY DISCLOSURES

PUBLIC COMPANY SEC DISCLOSURES

1. NEIMAN MARCUS (FEBRUARY 2014 – 10-Q)

http://www.sec.gov/Archives/edgar/data/1358651/000135865114000003/a2014020110q.htm

RISK FACTORS

A breach in information privacy could negatively impact our operations.

We discovered in January 2014 that malicious software (malware) was clandestinely installed on our computer systems. Based on information from our forensic investigation, it appears that the malware actively attempted to collect payment card data from July 16, 2013 through October 30, 2013 at 77 of our 85 stores, on different dates at each store within this time period. During that time period, information from approximately 350,000 customer payment cards could have been potentially collected by the malware.

We are actively cooperating with the U.S. Secret Service in its investigation into this criminal cyber-attack on our systems. In testimony before Congress in February 2014, a Secret Service official explained that the attack on the Company was exceedingly sophisticated, and was unprecedented in the manner in which it was customized to defeat the Company's defenses and remain undetected. The Secret Service official also testified that the Company used a robust security plan to protect customer data, but that, given its level of sophistication, the attacker nevertheless succeeded in having malware operate on the Company's systems.

In light of this incident, we have taken steps to further strengthen the security of our computer systems, and continue to assess, maintain and enhance the ongoing effectiveness of our information security systems. Nevertheless, there can be no assurance that we will not suffer a similar criminal attack in the future, that unauthorized parties will not gain access to personal information, or that any such incident will be discovered in a timely way. In particular, the techniques used by criminals to obtain unauthorized access to sensitive data change frequently and often are not recognized until launched against a target; accordingly, we may be unable to anticipate these techniques or implement adequate preventative measures.

As described in Item 7, "Management's Discussion and Analysis of Financial Condition and Results of Operations", we incurred costs in the second quarter of fiscal year 2014

associated with this security incident, including legal fees, investigative fees, costs of communications with customers and credit monitoring services. In the future, payment card companies and associations may require us to reimburse them for unauthorized card charges and costs to replace cards and may also impose fines or penalties in connection with the security incident, and federal and state enforcement authorities may also impose fines or other remedies against us. We expect to incur additional costs to investigate and remediate the matter in the foreseeable future. Such costs are not currently estimable but could be material to our future operating results.

The incident discussed above has given rise to putative class action litigation on behalf of customers and regulatory investigations. At this point, we are unable to predict the developments in, outcome of, and economic and other consequences of pending or future litigation or government inquiries related to this matter. Any future criminal cyber-attack or data security incident may result in additional regulatory investigations, legal proceedings or liability under laws that protect the privacy of personal information, all of which may damage our reputation and relationships with our customers and adversely affect our business, operating results and financial condition.

FINANCIAL INFORMATION

Other Expenses

Other expenses consists of the following components:

	Quarter-to-date		Year-to-date		
(in thousands)	Thirteen weeks ended February 1, 2014 (Successor)	Thirteen weeks ended January 26, 2013 (Predecessor)	Thirteen weeks ended February 1, 2014 (Successor)	Thirteen weeks ended November 2, 2013 (Predecessor)	Twenty-six weeks ended January 26, 2013 (Predecessor)
Costs incurred in connection with the Acquisition:					
Change-in-control cash payments due to Former Sponsors and management	$ —	$ —	$ —	$ 80,457	$ —
Stock-based compensation for accelerated vesting of Predecessor stock options	51,510	—	51,510	—	—
Other, primarily professional fees	1,732	—	1,732	28,942	—
Total transaction costs	53,242	—	53,242	109,399	—
Management fee due to Former Sponsors	—	3,406	—	2,823	6,077
Equity in loss of foreign e-commerce retailer	2,063	3,218	2,063	1,523	5,251
Costs related to criminal cyber-attack	4,088	—	4,088	—	—
Other non-recurring expenses	4,775	—	4,775	—	—
Other expenses	$ 64,168	$ 6,624	$ 64,168	$ 113,745	$ 11,328

We have an investment in a foreign e-commerce retailer, which is accounted for under the equity method. Our equity in the investee's losses reduces the carrying value of our investment. The carrying value of our investment at February 1, 2014 was $23.4 million.

In the second quarter of fiscal year 2014, we incurred 1) costs related to the investigation of a criminal cyber-attack on our systems, including legal fees, investigative fees, costs of communications with customers and credit monitoring services provided to customers, and 2) other non-recurring expenses. We expect to incur additional costs to investigate and remediate the cyber-attack in the foreseeable future. Such costs are not currently estimable but could be material to our future operating results.

Other expenses. Other expenses for the second quarter of fiscal year 2014 aggregated $64.2 million, or 4.5% of revenues, compared to $6.6 million, or 0.5% of revenues, in the second quarter of fiscal year 2013. The increase in other expenses in the second quarter of fiscal year 2014 was primarily due to $53.2 million in transaction costs related to the Acquisition. In addition, we incurred approximately $8.9 million of expenses in the

second quarter of fiscal year 2014 for 1) costs related to the investigation of a criminal cyber-attack on our systems, including legal fees, investigative fees, costs of communications with customers and credit monitoring services provided to customers, and 2) other non-recurring expenses. We expect to incur additional costs to investigate and remediate the cyber-attack in the foreseeable future. Such costs are not currently estimable but could be material to our future operating results.

2. TARGET CORPORATION (FEBRUARY 2014 8-K):

http://www.sec.gov/Archives/edgar/data/27419/000002741914000006/a2013q48k.htm

INTRODUCTORY NOTE

Target is including updated "Risk Factors" with this report to provide additional information on risks or uncertainties that could affect the forward-looking statements included in the News Release.

During the fourth quarter of 2013, we experienced a data breach in which certain payment card and other guest information was stolen through unauthorized access to our network. Throughout the Risk Factors in this report, this incident is referred to as the "2013 data breach".

RISK FACTORS

Our business is subject to many risks. Set forth below are the most significant risks that we face.

. . .

Our continued success is substantially dependent on positive perceptions of Target which, if eroded, could adversely affect our business and our relationships with our guests and team members.

We believe that one of the reasons our guests prefer to shop at Target and our team members choose Target as a place of employment is the reputation we have built over many years for serving our four primary constituencies: guests, team members, the communities in which we operate, and shareholders. To be successful in the future, we must continue to preserve, grow and leverage the value of Target's reputation. Reputational value is based in large part on perceptions. While reputations may take decades to build, any negative incidents can quickly erode trust and confidence, particularly if they result in adverse mainstream and social media publicity, governmental investigations or litigation. Those types of incidents could have an adverse impact on perceptions and lead to tangible adverse effects on our business, including consumer boycotts, lost sales, loss of new store development opportunities, or team member retention and recruiting difficulties. For example, we experienced weaker than expected U.S. Segment sales following the announcement of the 2013 data breach.

. . .

The data breach we experienced in 2013 has resulted in government inquiries and private litigation, and if our efforts to protect the security of personal information about our guests and team members are unsuccessful, future issues may result in additional costly government enforcement actions and private litigation and our sales and reputation could suffer.

The nature of our business involves the receipt and storage of personal information about our guests and team members. We have a program in place to detect and respond to data security incidents. However, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently and may be difficult to detect for long periods of time, we may be unable to anticipate these techniques or implement adequate preventive measures. In addition, hardware, software or applications we develop or procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise information security. Unauthorized parties may also attempt to gain access to our systems or facilities through fraud, trickery or other forms of deceiving our team members, contractors and temporary staff. Until the fourth quarter of 2013, all incidents we experienced were insignificant. The 2013 data breach we experienced was significant and went undetected for several weeks. We experienced weaker than expected U.S. Segment sales immediately following the announcement of the 2013 data breach, and we are currently facing more than 80 civil lawsuits filed on behalf of guests, payment card issuing banks and shareholders. In addition, state and federal agencies, including State Attorneys General, the Federal Trade Commission and the Securities and Exchange Commission, are investigating events related to the 2013 data breach, including how it occurred, its consequences and our responses, which may have an adverse effect on how we operate our business and our results of operations.

If we experience additional significant data security breaches or fail to detect and appropriately respond to significant data security breaches, we could be exposed to additional government enforcement actions and private litigation. In addition, our guests could further lose confidence in our ability to protect their personal information, which could cause them to discontinue using our REDcards or pharmacy services, or stop shopping with us altogether. Lost confidence from a significant data security breach involving team members could hurt our sales, reputation, cause team member recruiting and retention challenges, increase our labor costs, and affect how we operate our business.

Our failure to comply with federal, state, local and international laws, or changes in these laws could increase our costs, reduce our margins and lower our sales.

Our business is subject to a wide array of laws and regulations in the United States, Canada and other countries in which we operate. . . . . For example, we are currently facing government inquiries related to the 2013 data breach that may result in the imposition of fines or other penalties. In addition, any legislative or regulatory changes adopted in reaction to the recent retail-industry data breaches could increase or accelerate our compliance costs.

. . .

A significant disruption in our computer systems and our inability to adequately maintain and update those systems could adversely affect our operations and our ability to maintain guest confidence.

We rely extensively on our computer systems to manage inventory, process guest transactions, communicate with our vendors and other third parties, service REDcard accounts and summarize and analyze results, and on continued and unimpeded access to the internet to use our computer systems. Our systems are subject to damage or interruption from power outages, telecommunications failures, computer viruses and malicious attacks, security breaches and catastrophic events. If our systems are damaged or fail to function properly, we may incur substantial repair or replacement costs, experience data loss and impediments to our ability to manage inventories or process guest transactions, and encounter lost guest confidence, which could adversely affect our results of operations. The 2013 data breach we experienced negatively impacted our ability to timely handle customer inquiries, and we experienced weaker than expected U.S. Segment sales following the announcement of the 2013 data breach.

We continually make significant technology investments that will help maintain and update our existing computer systems. Implementing significant system changes increases the risk of computer system disruption. Additionally, the potential problems and interruptions associated with implementing technology initiatives could disrupt or reduce our operational efficiency, and could impact the guest experience and guest confidence.

. . .

We experienced a significant data security breach in the fourth quarter of fiscal 2013 and are not yet able to determine the full extent of its impact and the impact

of government investigations and private litigation on our results of operations, which could be material.

The 2013 data breach we experienced involved the theft of certain payment card and guest information through unauthorized access to our network. Our investigation of the matter is ongoing, and it is possible that we will identify additional information that was accessed or stolen, which could materially worsen the losses and reputational damage we have experienced. For example, when the intrusion was initially identified, we thought the information stolen was limited to payment card information, but later discovered that other guest information was also stolen.

A significant factor in determining our financial liability is whether our systems were in compliance with applicable payment card industry standards. While our systems were determined to be compliant by a third party in the fall of 2013, the standards are inherently subjective and the extent of compliance required is subject to differing views. Another factor in determining the amount of any liability is the extent of actual fraud losses experienced by affected card holders or other guests, which will not be known to us for several weeks or months. In addition, the governmental agencies investigating the 2013 data breach may seek to impose injunctive relief, which could materially increase our data security costs, adversely impact how we operate our network and collect and use guest information, and put us at a competitive disadvantage with other retailers.

Finally, we believe that the greatest risk to our business arising out of the 2013 data breach is the negative impact on our reputation and loss of confidence of our guests, as well as the possibility of decreased participation in our REDcards Rewards loyalty program which our internal analysis has indicated drives meaningful incremental sales. We experienced weaker than expected U.S. Segment sales after the announcement of the 2013 data breach, but are unable to determine whether there will be a long-term impact to our relationship with our guests or whether we will need to engage in significant promotional or other activities to regain their trust, which could have a material adverse impact on our results of operations or profitability.

3. TARGET (MAY 2014 10-Q)

http://www.sec.gov/Archives/edgar/data/27419/000002741914000021/tgt-20140503x10q.htm

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS (UNAUDITED)

Data Breach

In the fourth quarter of 2013, we experienced a data breach in which an intruder stole certain payment card and other guest information from our network (the Data Breach). Based on our investigation to date, we believe that the intruder accessed and stole payment card data from approximately 40 million credit and debit card accounts of guests who shopped at our U.S. stores between November 27 and December 17, 2013, through malware installed on our point-of-sale system in our U.S. stores. In addition, the intruder stole certain guest information, including names, mailing addresses, phone numbers or email addresses, for up to 70 million individuals. Our investigation of the matter is ongoing, and we are supporting law enforcement efforts to identify the responsible parties.

Expenses Incurred and Amounts Accrued

Data Breach Balance Sheet Rollforward (millions)	Liabilities	Insurance Receivable
Balance at February 1, 2014	$ 61	$ 44
Expenses incurred/insurance receivable recorded [(a)]	**26**	**8**
Payments made/cash received	**(35)**	**(13)**
Balance at May 3, 2014	**$ 52**	**$ 39**

[(a)] Includes expenditures and accruals for Data Breach related costs and expected insurance recoveries as discussed below.

In the first quarter of 2014, we recorded $26 million of Data Breach-related expenses, partially offset by expected insurance proceeds of $8 million, for net expenses of $18 million. We recorded these expenses in our Consolidated Statements of Operations as Selling, General and Administrative Expenses (SG&A), but they are not included in our segment results. Expenses primarily relate to legal and other professional services.

Since the Data Breach, we have incurred $88 million of cumulative expenses, partially offset by expected insurance recoveries of $52 million, for net cumulative expenses of $35 million. These expenses include an accrual for the estimated probable loss related to the expected payment card networks' claims by reason of the Data Breach. The ultimate amount of these claims will likely include amounts for incremental counterfeit fraud

losses and non-ordinary course operating expenses (such as card reissuance costs) that the payment card networks believe they or their issuing banks have incurred. In order for us to have liability for such claims, we believe that a court would have to find among other things that (1) at the time of the Data Breach the portion of our network that handles payment card data was noncompliant with applicable data security standards in a manner that contributed to the Data Breach, and (2) the network operating rules around reimbursement of operating costs and counterfeit fraud losses are enforceable. While an independent third-party assessor found the portion of our network that handles payment card data to be compliant with applicable data security standards in the fall of 2013, the forensic investigator working on behalf of the payment card networks claimed that we were not in compliance with those standards at the time of the Data Breach. As a result, we believe it is probable that the payment card networks will make claims against us. We expect to dispute the payment card networks' anticipated claims, and we think it is probable that our disputes would lead to settlement negotiations consistent with the experience of other entities that have suffered similar payment card breaches. We believe such negotiations would effect a combined settlement of both the payment card networks' counterfeit fraud loss allegations and their non-ordinary course operating expense allegations. We based our accrual on the expectation of reaching negotiated settlements of the payment card networks' anticipated claims and not on any determination that it is probable we would be found liable on these claims were they to be litigated. Currently, we can only reasonably estimate a loss associated with settlements of the networks' expected claims for non-ordinary course operating expenses. The accrual does not include any amounts associated with the networks' expected claims for alleged incremental counterfeit fraud losses because the loss associated with settling such claims, while probable in our judgment, is not reasonably estimable, in part because we have not yet received third-party fraud reporting from the payment card networks. We are not able to reasonably estimate a range of possible losses in excess of the recorded accrual related to the expected settlement of the payment card networks' claims because the investigation into the matter is ongoing and there are significant factual and legal issues to be resolved. We believe it is reasonably possible that the ultimate amount paid on payment card network claims could be material to our results of operations in future periods.

Litigation and Governmental Investigations

In addition, more than 100 actions have been filed in courts in many states and one action in Canada and other claims have been or may be asserted against us on behalf of guests, payment card issuing banks, shareholders or others seeking damages or other related relief, allegedly arising out of the Data Breach. State and federal agencies, including the State Attorneys General, the Federal Trade Commission and the SEC are investigating events related to the Data Breach, including how it occurred, its consequences and our responses. While a loss from these matters is reasonably possible, we cannot reasonably estimate a range of possible losses because our investigation into the matter is ongoing, the proceedings remain in the early stages, alleged damages have not been specified, there is uncertainty as to the likelihood of a class or classes being certified or the ultimate size of any class if certified, and there are significant factual and legal issues to be resolved. Although we are cooperating in these investigations, we may be subject to fines or other obligations, which may have an adverse effect on our results of operations. We have not concluded that a loss from these matters is probable; therefore, we have not recorded a loss contingency liability for litigation, claims and governmental investigations in the first quarter 2014. We will continue to evaluate information as it becomes known and will record an estimate for losses at the time or times when it is both probable that a loss has been incurred and the amount of the loss is reasonably estimable.

Future Costs

We expect to incur significant legal and professional services expenses associated with the Data Breach in future periods. We will recognize these expenses as services are received.

Insurance Coverage

To limit our exposure to losses relating to data breach and other claims, we maintain $100 million of network-security insurance coverage, above a $10 million deductible. This coverage and certain other customary business-insurance coverage has reduced our exposure related to the Data Breach. We will pursue recoveries to the maximum extent available under the policies. As of May 3, 2014, we have received an initial payment of $13 million on our claim from our primary layer of network-security insurance, and expect to receive additional payments.

4. AFFINITY GAMING (MAY 2014 8-K EXHIBIT 99.1):

http://www.sec.gov/Archives/edgar/data/1499268/000149926814000018/ex991datasecurityevent2pre.htm

EXHIBIT 99.1 TO 8-K

Affinity Gaming Provides Public Notice of Unauthorized IT System Access

On April 17, 2014, Affinity was conducting a security audit of its IT systems, when it identified a possible issue in the system that processes debit and credit card transactions. Affinity immediately initiated a thorough investigation, supported by a top-tier and globally recognized, third-party data forensics expert, Mandiant, which determined the nature and scope of the compromise. Mandiant's and Affinity's teams worked aggressively to fully secure the payment card systems and ensure that customer payments are protected. Affinity promptly and repeatedly posted notices of this incident on its website, in an effort to inform and update customers of its ongoing investigation.

Affinity's investigation, while still continuing, has determined that its system was attacked by hackers, which resulted in a compromise of credit card and debit card information used in non-gaming purchases from individuals who visited its casino and casino resort facilities: Silver Sevens Hotel & Casino in Las Vegas, NV; Rail City Casino in Sparks, NV; Primm Valley Resort & Casino in Primm, NV; Buffalo Bill's Resort & Casino in Primm, NV; Whiskey Pete's Hotel & Casino in Primm, NV; Lakeside Hotel-Casino in Osceola, IA; St. Jo Frontier Casino in St. Joseph, MO; Mark Twain Casino in LaGrange, MO; Golden Gates Casino in Black Hawk, CO; Golden Gulch Casino in Black Hawk, CO; and Mardi Gras Casino in Black Hawk, CO. Credit or debit card data was exposed at these locations for those customers making hotel, food and beverage, and retail purchases with their cards between December 7, 2013 and April 28, 2014.

5. SALLY BEAUTY HOLDINGS, INC. (10-Q MAY 2014)

http://www.sec.gov/Archives/edgar/data/1368458/000110465914033026/a14-8385_110q.htm

TABLE OF CONTENTS

Changes to our information technology systems. As our operations grow in both size and scope and as cyberattacks and security intrusions involving retailers have become more frequent, we will continuously need to improve and upgrade our information systems and infrastructure while maintaining the reliability, integrity and security of our systems and infrastructure. The expansion of our systems and infrastructure will require us to commit substantial financial, operational and technical resources in advance of any increase in the volume of our business, with no assurance that the volume of business will increase. For example, we are in the process of designing and implementing a standardized enterprise resource planning ("ERP") system internationally, which we anticipate will be completed over the next few years. In addition, we are currently implementing a point-of-sale system upgrade program in several areas (including our Sally Beauty Supply operations in the U.S.), which we anticipate will provide significant benefits, including enhanced tracking of customer sales and store inventory activity. Further, in response to the Data Security Incident, we have taken and are continuing to take actions to further strengthen the security of our information technology systems. These and any other required upgrades to our information systems and information technology (or new technology), now or in the future, will require that our management and resources be diverted from our core business to assist in completion of these projects. Many of our systems are proprietary, and as a result our options are limited in seeking third-party assistance with the operation and upgrade of those systems. There can be no assurance that the time and resources our management will need to devote to these upgrades, service outages or delays due to the installation of any new or upgraded technology (and customer issues therewith), or the impact on the reliability or security of our data from any new or upgraded technology will not have a material adverse effect on our financial reporting, business, financial condition or results of operations. Please see "Risk Factors — We may be adversely affected by any disruption in our information technology systems" in Item 1A of our Annual Report on Form 10-K for the fiscal year ended September 30, 2013, and "Risk Factors — Unauthorized access to confidential information and data on our information technology systems and security and data breaches could materially adversely affect our business, financial condition and operating results" and "Risk Factors — We experienced a data security incident and are not yet able

to determine the full extent or scope of the potential liabilities relating to this data security incident" in Item 1A of this Quarterly Report.

OTHER INFORMATION

Unauthorized access to confidential information and data on our information technology systems and security and data breaches could materially adversely affect our business, financial condition and operating results.

As part of our operations, we receive and maintain information about our customers (including credit and debit card information), our employees and other third parties. We have physical, technical and procedural safeguards in place that are designed to protect information and protect against security and data breaches as well as fraudulent transactions and other activities. Despite these safeguards and our other security processes and protections, we cannot be assured that all of our systems and processes are free from vulnerability to security breaches (through cyberattacks, which are evolving and becoming increasingly sophisticated, physical breach or other means) or inadvertent data disclosure by third parties or us. A significant data security breach, including misappropriation of our customers' or employees' confidential information, could result in significant costs to us, which may include, among others, potential liabilities to payment card networks for reimbursements of credit card fraud and card reissuance costs, including fines and penalties, potential liabilities from governmental or third party investigations, proceedings or litigation, legal, forensic and consulting fees and expenses, costs and diversion of management attention required for investigation and remediation actions, and the negative impact on our reputation and loss of confidence of our customers, suppliers and others, any of which could have a material adverse impact on our business, financial condition and operating results.

In response to the Data Security Incident, we have taken and are continuing to take actions to further strengthen the security of our information technology systems. Nevertheless, there can be no assurance that we will not suffer a similar criminal attack in the future, that unauthorized parties will not gain access to confidential information, or that any such incident will be discovered promptly. In particular, we understand that the techniques used by criminals to obtain unauthorized access to sensitive data change frequently and often are not recognized until launched against a target; accordingly, we may be unable to anticipate these techniques or implement adequate preventative measures. The failure to promptly detect, determine the extent of and appropriately respond to a significant data security breach could have a material adverse impact on our business, financial condition and operating results.

MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS.

. . .

In March 2014, the Company disclosed that there had been an unauthorized intrusion into its Sally Beauty Supply segment's network, which we refer to as the Data Security Incident. For the six months ended March 31, 2014, selling, general and administrative expenses reflect a charge of $1.1 million, consisting primary of professional advisory and legal costs incurred in connection with our investigation of the Data Security Incident.

. . .

DATA SECURITY INCIDENT

As previously disclosed, we discovered the Data Security Incident in late February when we detected illegally installed malicious software (malware) on certain parts of our information technology systems, including our point of sale systems. Our General Counsel immediately engaged forensic experts to assist us in our investigation of the Data Security Incident, which is continuing. As a result of our ongoing investigation, we discovered and are reviewing forensic evidence that a portion of the payment card data (track 2) for some transactions on our systems primarily during the period from February 21, 2014 to February 28, 2014 may have been illegally accessed and removed by the malware. We completed the removal of the malware from our point of sale systems and believe that the Data Security Incident has been contained.

The costs that we have incurred to date in connection with the Data Security Incident primarily include professional advisory and legal costs relating to our continuing investigation of the Data Security Incident. We expect to incur additional costs and expenses related to the Data Security Incident in the future. As detailed in Item 1A -"Risk Factors - Unauthorized access to confidential information and data on our information technology systems and security and data breaches could materially adversely affect our business, financial condition and operating results," these costs may result from potential liabilities to payment card networks, governmental or third party investigations, proceedings or litigation and legal and other fees necessary to defend against any potential liabilities or claims. We are unable at this time to determine the probability of or to reasonably estimate the magnitude of these potential liabilities. The potential liabilities or other remedies against us related to the Data Security Incident may have a material adverse impact on our business, financial condition and operating results. Please

see “Risk Factors - We experienced a data security incident and are not yet able to determine the full extent or scope of the potential liabilities relating to this data security incident” in Item 1A of this Quarterly Report. Prior to the Data Security Incident, we had not become aware of any other significant security or data breaches or other unauthorized intrusions.

. . .

RISK FACTORS

In addition to the other information set forth in this report, you should carefully consider the factors contained in Part I, Item 1A. “Risk Factors” in our Annual Report on Form 10-K for the fiscal year ended September 30, 2013, which could materially affect our business, financial condition or future results. Other than the risks described below, there have been no material changes from the risk factors disclosed in such Annual Report. The risks described in that report and herein are not the only risks facing our company.

Unauthorized access to confidential information and data on our information technology systems and security and data breaches could materially adversely affect our business, financial condition and operating results.

As part of our operations, we receive and maintain information about our customers (including credit and debit card information), our employees and other third parties. We have physical, technical and procedural safeguards in place that are designed to protect information and protect against security and data breaches as well as fraudulent transactions and other activities. Despite these safeguards and our other security processes and protections, we cannot be assured that all of our systems and processes are free from vulnerability to security breaches (through cyberattacks, which are evolving and becoming increasingly sophisticated, physical breach or other means) or inadvertent data disclosure by third parties or us. A significant data security breach, including misappropriation of our customers’ or employees’ confidential information, could result in significant costs to us, which may include, among others, potential liabilities to payment card networks for reimbursements of credit card fraud and card reissuance costs, including fines and penalties, potential liabilities from governmental or third party investigations, proceedings or litigation, legal, forensic and consulting fees and expenses, costs and diversion of management attention required for investigation and remediation actions, and the negative impact on our reputation and loss of confidence of our customers, suppliers and others, any of which could have a material adverse impact on our business, financial condition and operating results.

In response to the Data Security Incident, we have taken and are continuing to take actions to further strengthen the security of our information technology systems. Nevertheless, there can be no assurance that we will not suffer a similar criminal attack in the future, that unauthorized parties will not gain access to confidential information, or that any such incident will be discovered promptly. In particular, we understand that the techniques used by criminals to obtain unauthorized access to sensitive data change frequently and often are not recognized until launched against a target; accordingly, we may be unable to anticipate these techniques or implement adequate preventative measures. The failure to promptly detect, determine the extent of and appropriately respond to a significant data security breach could have a material adverse impact on our business, financial condition and operating results.

We experienced a data security incident and are not yet able to determine the full extent or scope of the potential liabilities relating to this data security incident.

The Data Security Incident involved the unauthorized installation of malicious software (malware) on our information technology systems, including our point-of-sale systems that, we believe, may have illegally accessed and removed a portion of the payment card data (track 2) for some transactions on our systems primarily during the period from February 21, 2014 to February 28, 2014. Our investigation into the Data Security Incident is ongoing, and we will not be able to determine the full extent or scope of the potential liabilities relating to the Data Security Incident until the forensic review is complete. While the costs that we have incurred to date in connection with the Data Security Incident primarily include professional advisory and legal costs relating to our continuing investigation of the Data Security Incident, we expect to incur additional costs and expenses related to the Data Security Incident in the future. As detailed in Item 1A -"Risk Factors - Unauthorized access to confidential information and data on our information technology systems and security and data breaches could materially adversely affect our business, financial condition and operating results," these costs may result from potential liabilities to payment card networks, governmental or third party investigations, proceedings or litigation and legal and other fees necessary to defend against any potential liabilities or claims. We are unable at this time to determine the probability of or to reasonably estimate the magnitude of these potential liabilities. The potential liabilities or other remedies against us related to the Data Security Incident may have a material adverse impact on our business, financial condition and operating results.

6. EBAY INC. (MAY 2014 8-K):

http://www.sec.gov/Archives/edgar/data/1065088/000106508814000097/exhibit991-521pressrelease.htm

EXHIBIT 99.1 TO 8-K

eBay Inc. To Ask eBay Users To Change Passwords

San Jose, CA (May 21, 2014) - eBay Inc. (Nasdaq: EBAY) said beginning later today it will be asking eBay users to change their passwords because of a cyberattack that compromised a database containing encrypted passwords and other non-financial data. After conducting extensive tests on its networks, the company said it has no evidence of the compromise resulting in unauthorized activity for eBay users, and no evidence of any unauthorized access to financial or credit card information, which is stored separately in encrypted formats. However, changing passwords is a best practice and will help enhance security for eBay users.

Information security and customer data protection are of paramount importance to eBay Inc., and eBay regrets any inconvenience or concern that this password reset may cause our customers. We know our customers trust us with their information, and we take seriously our commitment to maintaining a safe, secure and trusted global marketplace. Cyberattackers compromised a small number of employee log-in credentials, allowing unauthorized access to eBay's corporate network, the company said. Working with law enforcement and leading security experts, the company is aggressively investigating the matter and applying the best forensics tools and practices to protect customers.

The database, which was compromised between late February and early March, included eBay customers' name, encrypted password, email address, physical address, phone number and date of birth. However, the database did not contain financial information or other confidential personal information. The company said that the compromised employee log-in credentials were first detected about two weeks ago. Extensive forensics subsequently identified the compromised eBay database, resulting in the company's announcement today.

The company said it has seen no indication of increased fraudulent account activity on eBay. The company also said it has no evidence of unauthorized access or compromises to personal or financial information for PayPal users. PayPal data is stored separately on a secure network, and all PayPal financial information is encrypted.

7. EBAY INC. (MAY 2014 10-Q)

http://www.sec.gov/Archives/edgar/data/1065088/000106508814000060/ebay10-qq12014.htm

RISK FACTORS

Risk Factors That May Affect Results of Operations and Financial Condition

. . .

Failure to deal effectively with fraud, bad transactions and negative customer experiences would increase our loss rate and harm our business.

PayPal's highly automated and liquid payment service makes PayPal an attractive target for fraud. In configuring its service, PayPal continually strives to maintain the right balance of appropriate measures to promote both convenience and security for customers. Identity thieves and those committing fraud using stolen payment card or bank account numbers can potentially steal large amounts of money from businesses such as PayPal. We believe that several of PayPal's current and former competitors in the electronic payments business have gone out of business or significantly restricted their businesses largely due to losses from this type of fraud. While PayPal uses advanced anti-fraud technologies, we expect that technically knowledgeable criminals will continue to attempt to circumvent PayPal's anti-fraud systems using increasingly sophisticated methods. From time to time, such fraudsters may discover and exploit vulnerabilities that may not immediately be identified and remediated, which may in turn result in one-time increases in fraud and associated transaction losses, which may be substantial. In addition, because users frequently use the same passwords for different sites, a data breach of a third party site can result in a spike in eBay and/or PayPal transaction losses. PayPal's service could also be subject to employee fraud or other internal security breaches, and PayPal may be required to reimburse customers for any losses incurred as a result of such breaches. Merchants could also request reimbursement, or stop using PayPal, if they are affected by buyer fraud or other types of fraud. Additional fraud risks associated with PayPal's point of sale solutions are described below under the caption "PayPal's retail point of sale solutions expose us to additional risks."

. . .

Negative publicity and user sentiment generated as a result of fraudulent or deceptive conduct by users of our Marketplaces, Payments and Enterprise services could reduce

our ability to attract new users or retain our current users, damage our reputation and diminish the value of our brand names. We believe that negative user experiences are one of the primary reasons users stop using our services.

. . .

8. TWITTER (10-Q MAY 2014)

http://www.sec.gov/Archives/edgar/data/1418091/000156459014001959/twtr-10q_20140331.htm

Even though Twitter is a global platform for public self-expression and conversation, user trust regarding privacy is important to the growth of users and the increase in user engagement on our platform, and privacy concerns relating to our products and services could damage our reputation and deter current and potential users and advertisers from using Twitter.

From time to time, concerns have been expressed by governments, regulators and others about whether our products, services or practices compromise the privacy of users and others. Concerns about, governmental or regulatory actions involving our practices with regard to the collection, use, disclosure or security of personal information or other privacy-related matters, even if unfounded, could damage our reputation, cause us to lose users and advertisers and adversely affect our operating results. While we strive to comply with applicable data protection laws and regulations, as well as our own posted privacy policies and other obligations we may have with respect to privacy and data protection, the failure or perceived failure to comply may result, and in some cases has resulted, in inquiries and other proceedings or actions against us by governments, regulators or others, as well as negative publicity and damage to our reputation and brand, each of which could cause us to lose users and advertisers, which could have an adverse effect on our business.

Any systems failure or compromise of our security that results in the unauthorized access to or release of our users' or advertisers' data could significantly limit the adoption of our products and services, as well as harm our reputation and brand and, therefore, our business. In March 2014, we were alerted to, and fixed, a bug in our system that, for approximately 94,000 protected accounts under rare circumstances, allowed non-approved followers to receive protected tweets via SMS or push notifications since November 2013. We expect to continue to expend significant resources to protect against security breaches. The risk that these types of events could seriously harm our business is likely to increase as we expand the number of products and services we offer, increase the size of our user base and operate in more countries. Governments and regulators around the world are considering a number of legislative and regulatory proposals concerning data protection. In addition, the interpretation and application of consumer and data protection laws or regulations in the United States, Europe and elsewhere are often uncertain and in flux, and in some cases, laws or regulations in one country may be inconsistent with, or contrary to, those of another country. It is possible that these laws

and regulations may be interpreted and applied in a manner that is inconsistent with our practices. If so, in addition to the possibility of fines, this could result in an order requiring that we change our practices, which could have an adverse effect on our business and operating results. Complying with new laws and regulations could cause us to incur substantial costs or require us to change our business practices in a manner materially adverse to our business.

If our security measures are breached, or if our products and services are subject to attacks that degrade or deny the ability of users to access our products and services, our products and services may be perceived as not being secure, users and advertisers may curtail or stop using our products and services and our business and operating results could be harmed.

Our products and services involve the storage and transmission of users' and advertisers' information, and security breaches expose us to a risk of loss of this information, litigation and potential liability. We experience cyber-attacks of varying degrees on a regular basis, and as a result, unauthorized parties have obtained, and may in the future obtain, access to our data or our users' or advertisers' data. For example, in February 2013, we disclosed that sophisticated unknown third parties had attacked our systems and may have had access to limited information for approximately 250,000 users. Our security measures may also be breached due to employee error, malfeasance or otherwise. Additionally, outside parties may attempt to fraudulently induce employees, users or advertisers to disclose sensitive information in order to gain access to our data or our users' or advertisers' data or accounts, or may otherwise obtain access to such data or accounts. Since our users and advertisers may use their Twitter accounts to establish and maintain online identities, unauthorized communications from Twitter accounts that have been compromised may damage their reputations and brands as well as ours. Any such breach or unauthorized access could result in significant legal and financial exposure, damage to our reputation and a loss of confidence in the security of our products and services that could have an adverse effect on our business and operating results. Because the techniques used to obtain unauthorized access, disable or degrade service or sabotage systems change frequently and often are not recognized until launched against a target, we may be unable to anticipate these techniques or to 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, we could lose users and advertisers and we may incur significant legal and financial exposure, including legal claims and regulatory fines and penalties. Any of these actions could have a material and adverse effect on our business, reputation and operating results.

9. ADOBE

Blog Post from Chief Security Officer October 3, 2013

http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html

IMPORTANT CUSTOMER SECURITY ANNOUNCEMENT

Posted by Brad Arkin, Chief Security Officer on October 3, 2013 1:15 pm in Executive Perspectives

Cyber attacks are one of the unfortunate realities of doing business today. Given the profile and widespread use of many of our products, Adobe has attracted increasing attention from cyber attackers. Very recently, Adobe's security team discovered sophisticated attacks on our network, involving the illegal access of customer information as well as source code for numerous Adobe products. We believe these attacks may be related.

Our investigation currently indicates that the attackers accessed Adobe customer IDs and encrypted passwords on our systems. We also believe the attackers removed from our systems certain information relating to 2.9 million Adobe customers, including customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders. At this time, we do not believe the attackers removed decrypted credit or debit card numbers from our systems. We deeply regret that this incident occurred. We're working diligently internally, as well as with external partners and law enforcement, to address the incident. We're taking the following steps:

- As a precaution, we are resetting relevant customer passwords to help prevent unauthorized access to Adobe ID accounts. If your user ID and password were involved, you will receive an email notification from us with information on how to change your password. We also recommend that you change your passwords on any website where you may have used the same user ID and password.

- We are in the process of notifying customers whose credit or debit card information we believe to be involved in the incident. If your information was involved, you will receive a notification letter from us with additional information on steps you can take to help protect yourself against potential misuse of personal information about you. Adobe is also offering customers, whose credit or debit card information was

involved, the option of enrolling in a one-year complimentary credit monitoring membership where available.

- We have notified the banks processing customer payments for Adobe, so that they can work with the payment card companies and card-issuing banks to help protect customers' accounts.

We have contacted federal law enforcement and are assisting in their investigation.

. . .

Brad Arkin
Chief Security Officer

10.ADOBE (10-Q OCTOBER 2013)

http://www.sec.gov/Archives/edgar/data/796343/000079634313000058/adbe10qq313.htm

REGULATION FD DISCLOSURE

In September 2013, Adobe's security team discovered sophisticated attacks on our network involving the illegal access to certain customer and product information. We continue to investigate this incident and are taking certain steps to help minimize any impact on our business. At this time, we do not believe that the attacks will have a material adverse impact on our business or financial results. It is possible, nevertheless, that this incident could have various adverse effects on us as described in our risk factors for these types of incidents found in Item 1A "Risk Factors" in Part II of this Quarterly Report on Form 10-Q.

For additional information related to this incident, please refer to the blog post from Adobe's Chief Security Officer on October 3, 2013 describing the matter at blogs.adobe.com/conversations. The information contained in the blog post and other websites linked is not deemed to be incorporated into this filing. The disclosures provided in this Quarterly Report on Form 10-Q, including the foregoing information, are made only as of the date of this Report, and Adobe does not assume, and expressly disclaims, any duty to update such information.

11.ADOBE (10-Q MARCH 2014)

http://www.sec.gov/Archives/edgar/data/796343/000079634314000023/adbe10qq114.htm

RISK FACTORS

Security vulnerabilities in our products and systems could lead to reduced revenues or to liability claims.

Maintaining the security of our products, computers and networks is a critical issue for us and our customers. Security researchers, criminal hackers and other third parties regularly develop new techniques to penetrate computer and network security measures and, as we have previously disclosed, certain parties have in the past managed to breach certain of our data-security systems and misused certain of our systems and software in order to access our end users' authentication and payment information. In addition, cyber-attackers also develop and deploy viruses, worms and other malicious software programs, some of which may be specifically designed to attack our products, systems, computers or networks. Sophisticated hardware and operating system software and applications that we produce or procure from third parties may contain defects in design or manufacture, including bugs and other problems that could unexpectedly compromise the security of the system. The costs to us to eliminate or alleviate cyber or other security problems, bugs, viruses, worms, malicious software programs and security vulnerabilities are significant, and our efforts to address these problems may not be successful and could result in interruptions, delays, cessation of service and loss of existing or potential customers that may impede our sales, manufacturing, distribution or other critical functions, as well as potential liability to the company.

Outside parties have in the past and may in the future attempt to fraudulently induce our employees or users of our services to disclose sensitive information via illegal electronic spamming, phishing and other tactics. Unauthorized parties may also attempt to gain physical access to one of our facilities in order to infiltrate our information systems. These actual and potential breaches of our security measures and the accidental loss, inadvertent disclosure or unauthorized dissemination of proprietary information or sensitive, personal or confidential data about us, our employees or our customers, including the potential loss or disclosure of such information or data as a result of hacking, fraud, trickery or other forms of deception, could expose us, our employees, our customers or the individuals affected to a risk of loss or misuse of this information, result in litigation and potential liability or fines for us, governmental inquiry and oversight, damage our brand and reputation or otherwise harm our business.

Although these are industry-wide problems that affect computer systems, products and services across all platforms, they affect our products and services in particular because cyber-attackers tend to focus their efforts on the most popular offerings (such as those with large bases of users), and we expect them to continue to do so. Critical vulnerabilities may be identified in certain of our applications. These vulnerabilities could cause such applications to crash and could potentially allow an attacker to take control of the affected system, which could result in liability to us or limit our ability to conduct our business and deliver our products and services to customers. We devote significant resources to address security vulnerabilities through engineering more secure products, enhancing security and reliability features in our products and systems, code hardening, conducting rigorous penetration tests, deploying security updates to address security vulnerabilities and improving our incident response time. The cost of these steps could reduce our operating margins, and we may be unable to implement these measures quickly enough to prevent cyber-attackers from gaining unauthorized access into our systems and products. Despite our preventative efforts, actual or perceived security vulnerabilities in our products and systems may harm our reputation or lead to claims against us (and have in the past lead to such claims), and could lead some customers to seek to return products, to stop using certain services, to reduce or delay future purchases of products or services, or to use competing products or services. If we do not make the appropriate level of investment in our technology systems or if our systems become out-of-date or obsolete and we are not able to deliver the quality of data security customers require, our business could be adversely affected. Customers may also increase their expenditures on security measures designed to protect their existing computer systems from attack, which could delay adoption of new technologies. Further, if we or our customers are subject to a future attack, or our technology is utilized in a third-party attack, it may be necessary for us to take additional extraordinary measures and make additional expenditures to take appropriate responsive and preventative steps. Any of these events could adversely affect our revenues or margins. Moreover, delayed sales, lower margins or lost customers resulting from the disruptions of cyber-attacks or preventative measures could adversely affect our financial results, stock price and reputation.

. . .

Catastrophic events may disrupt our business.

We are a highly automated business and rely on our network infrastructure and enterprise applications, internal technology systems and our website for our development, marketing, operational, support, hosted services and sales activities. In

addition, some of our businesses rely on third-party hosted services, and we do not control the operation of third-party data center facilities serving our customers from around the world, which increases our vulnerability. A disruption, infiltration or failure of these systems or third-party hosted services in the event of a major earthquake, fire, flood, power loss, telecommunications failure, software or hardware malfunctions, cyber-attack, war, terrorist attack or other catastrophic event could cause system interruptions, reputational harm, loss of intellectual property, delays in our product development, lengthy interruptions in our services, breaches of data security and loss of critical data. Any of these events could prevent us from fulfilling our customers' orders. Our corporate headquarters, a significant portion of our research and development activities, certain of our data centers and certain other critical business operations are located in the San Francisco Bay Area, and additional facilities where we conduct significant operations are located in the Salt Lake Valley Area, both of which are near major earthquake faults. We have developed certain disaster recovery plans and backup systems to reduce the potentially adverse effect of such events, but a catastrophic event that results in the destruction or disruption of any of our data centers or our critical business or information technology systems could severely affect our ability to conduct normal business operations and, as a result, our future operating results could be adversely affected.

PRIVATE COMPANY VOLUNTARY DISCLOSURES

1. HARBOR FREIGHT TOOLS

http://www.harborfreight.com/protectingcustomers

Date: October 31, 2013

HARBOR FREIGHT TOOLS ACTS TO NOTIFY AND PROTECT CUSTOMERS

Calabasas, CA – Over the summer, Harbor Freight Tools' payment processing system was illegally attacked by cyber-criminals. The attack was similar to attacks reported by other national retailers. In response, we immediately engaged a leading cyber-security company to investigate and notices were posted in every store and on our website. We blocked the attack and adopted enhanced security measures to make our systems more secure than ever.

Fortunately, this incident was limited to credit and debit card transactions made in our stores during a relatively short seven week period (May 6, 2013 to June 30, 2013). Transactions after June 30, 2013 were not affected. For nearly all of these transactions, we believe that the attacker only found "track 2" data-information on the card's magnetic stripe that contains only the card account number, expiration date, and card verification number. For less than 1% of these transactions, the attacker may have found data that also included the cardholder's name.

Because we cannot identify which specific cards or information were actually taken, we are notifying our customers whose cards were used during the May 6, 2013 to June 30, 2013 time frame at each impacted store. For most of those purchases, we do not have sufficient information to identify the name or address of the customer. For those customers that we have addresses for, we began mailing letters to them on October 30. You can view a copy of the letter here. If you used your card in one of our stores during the seven week period and did not receive a letter, you should review the additional information below on ways to protect yourself.

. . .

2. SCHNUCKS

http://webcache.googleusercontent.com/search?q=cache:http://www.schnucks.com/pressreleases/pressrelease.asp?id=218

Date: April 15, 2013

SCHNUCKS RELEASES DETAILS OF CARD ISSUE AS INVESTIGATION NEARS END

St. Louis, MO – Leaders of St. Louis-based Schnuck Markets, Inc., today announced that between December 2012 and March 29, 2013, approximately 2.4 million credit and debit cards used at 79 of its 100 stores may have been compromised. The company emphasizes that only the card number and expiration date would have been accessed – **not the cardholder's name, address or any other identifying information.**

Schnucks has posted a list of the 79 stores and specific dates for each store at www.schnucks.com. In addition, Schnucks has distributed a timeline of the actions taken to investigate, find, contain, and share information about the cyber-attack, as well as a personal video message from Chairman and CEO Scott Schnuck.

"On behalf of myself, the Schnuck family, and all of our 15,000 teammates, I apologize to everyone affected by this incident," said Scott Schnuck. "Over the years, technology has helped us deliver superior customer service, but it also introduces risks that we have actively worked to manage through compliance audits, encryption technology and various other security measures."

"We've worked hard to provide a secure transaction environment for our customers and, today I make a personal pledge to you that we will be relentless in maintaining the security of our payment processing system. We expect that the actions we have taken and will take in the future will send a clear signal that our customers may continue to trust us," said Schnuck.

Schnucks has worked with its payment processor to make sure all potentially affected card numbers are sent to the credit card companies so that they may continue sending alerts to the issuing banks. Those banks will then be able to take steps to protect their cardholders, such as adding enhanced transaction monitoring or reissuing a new card. Many banks have already taken these steps.

"Customers have asked me if it is safe to shop at Schnucks," continued Schnuck. "Yes, we believe it is, and we will work hard to keep it that way."

. . .

Schnucks provided the Secret Service and FBI with information about the methods and tools used by the attacker and has worked and will continue to partner with law enforcement to apprehend those responsible.