ABSTRACT

During the fiscal year 2008 financial reporting process, Heartland Payment Systems, Inc. experienced a data breach of their operational data by international hackers and a U.S. based Secret Service informant who returned back to his criminal life as a hacker (Verini 2010). As a result, Heartland’s management assessed the data breach to determine whether it was a subsequent event and its long-term impact on the viability of the company. Similarly, Heartland’s external auditors independently assessed the data breach to determine whether they agreed with the company’s assessment for their financial statements. While Heartland survived and grew and built its reputation as an industry leader in credit card servicing (HPY 2016), this historical case provides several valuable learning points for financial accounting and auditing students. Using this case, students will gain an increased understanding of how to evaluate a subsequent event, assess a company’s financial health, and develop critical thinking skills as they scrutinize the activities of both financial statement preparers and auditors in the emerging area of cybersecurity.

KEYWORDS: cybersecurity; going concern; subsequent events.
Heartland Payment Systems: Cybersecurity Impact on Audits and Financial Statement Contingencies

PART 1 – COMPANY-SPECIFIC INFORMATION

Background

Heartland Payment Systems, Inc. (“Heartland”) is a major credit card servicing company serving, at that time, over 150,000 retail merchants and were the sixth largest independent credit card servicer in the United States. Heartland was formed in 1997 by Robert O. Carr, an entrepreneur from the Midwest who was a founding member of the Electronic Transactions Association. Bob Carr had served as the Chief Executive Officer for the entire history of the company. His first hire, Robert H.B. Baldwin, Jr., previously worked at Goldman Sachs and has served as the Chief Financial Officer for its entire history. Heartland’s base of operations throughout its history has been Princeton, New Jersey, taking advantage their proximity to the financial services epicenter of New York City. Despite the integral connection to Wall Street, Heartland maintained an entrepreneurial corporate culture in which company executives worked in close proximity with rank-and-file employees.

As an intermediary between retail merchants and cardholders’ financial institutions (e.g. Chase, Citibank, Barclaycard), Heartland’s business model is highly contingent upon individuals processing credit card transactions with local merchants to sustain profitability. On a hypothetical $100 credit card transaction, Heartland earns a gross revenue of $2.47 and must both cover their operating costs of their credit card network and pay fees for both accessing a bank card network (i.e. fixed cost) and on the transaction amount and volume (i.e. variable cost) to third parties (HPY 2008 10-K, p. 13-14). Significant investments must be made by credit card processors to acquire new merchants, maintain existing merchant relationships, and protect individuals’ personally identifiable information.

During 2008, Heartland was a rapidly growing business. When Matthew Reidenbach joined the client as a new lead audit senior in the summer of 2008, Heartland’s stock had been publicly traded for only three years and the company itself was just over ten years old (HPY 2016). In addition, Heartland noted in their 10-K filing
(pg. 13-14) that they had just completed a major acquisition during May 2008 that diversified their business away from their primary customer base of small and midsize merchants to also include larger national merchants (e.g. 7-Eleven). While completing a financial forecast analysis during his first weeks on the job, Matthew was impressed by the corporate culture of openness and the respectful relationship by management toward the external auditors that was not present in many of his other current and previous clients.

**Data Breach**

On Monday, January 20, 2009, Matthew arrived in the client’s office to a bombshell: Heartland was the victim of a data breach. While it was unclear at that time what the nature and severity of the data breach was, it was obvious that this was a major concern for the calendar year-end audit engagement. Year-end field work had barely begun and, as a result, understanding the data breach became paramount to the managers and partner in charge of the Heartland audit. Given the impending articles published later that day in the New York Times (Dash and Stone 2009) and the Washington Post (Krebs 2009) among other outlets, it was critical that Matthew’s public accounting firm understand this breach and determine its impact upon the financial statements in very short order. Making the process more challenging was the fact that there were few comparable data breaches to base potential losses upon.

Ominously, only one year earlier, TJX Companies Inc. (owner of retail brands – e.g. TJ Maxx, Marshall’s) had been the subject of a data breach. Over the course of 2007, the retailer had card numbers and personal data for roughly 45 million credit and debit card numbers stolen by hackers and it cost their business over $40 million just to settle claims with MasterCard (Pereira and Seidel 2007). During their fiscal year, TJX Companies accrued a pre-tax legal liability of $256 million and some analysts suggested at that time that the ultimate losses may be larger than the recorded liability incurred by TJX Companies (Kerber 2007). Expanding this connection further was that Heartland hired the same law firm, Ropes and Gray, which TJX Companies used to defend itself against claims related to their data breach.

**Audit Procedures to Evaluate Data Breach**
In order to assess the impact of the data breach on Heartland’s financial statements, the audit team performed multiple procedures. First, the audit team performed inquiries of Heartland employees to explicitly understand the nature of the data breach. In this case, the audit partner and senior manager interviewed the Chief Executive Officer, Chief Financial Officer, Chief Accounting Officer, and Chief Information Officer along with operational employees. This process spanned several weeks between at both their Princeton offices and at their Texas-based data centers. Based upon these inquiries, the external auditors learned that Heartland first learned that they were victims of a data breach through the United States Secret Service. Prior to January 20, 2009, the company could not disclose the information since it could potentially impede the governmental investigation and prevent the Secret Service from catching the culprits. In addition, the auditors determined that it was likely that the breach involved critical operational data such as credit card numbers and names but did not reach individuals’ social security numbers or PIN information (HPY 2008 10-K, pg. 1-5). This limited Heartland’s ability to reasonably estimate the cost of the data breach by the issuance date of the financial statements.

Second, Matthew led the audit team’s efforts to test internal controls over financial reporting and evaluated whether the systems reliably consolidated financial data. Based upon this testing, there was no evidence that the systems were ineffective or including financial amounts not in the scope of audit work. Further, there was no evidence that the hackers targeted or compromised the company’s financial accounting systems based upon the inquiries noted in the previous paragraph. Based upon these procedures, the audit team concluded that the data breach had no effect on the financial statements or the internal control controls over financial reporting for Heartland (HPY 2008 10-K, pg. 75-76).

**General Questions:**

*Answer the following question using a short paragraph (5 sentence minimum).*

1. What type of subsequent event is the data? What are management’s and the auditor’s responsibilities, respectively, for the data breach? Cite the relevant authoritative accounting and auditing literature in your response.
2. If you were the audit partner, what additional questions would you ask the company’s management in order to evaluate the nature and extent of the data breach?
PART 2 – LEGAL LIABILITY CONSIDERATIONS

Due to the data breach, a number of legal issues arose for Heartland during the field work of the audit. As noted in Heartland’s 10-K, multiple lawsuits were initiated against the company. First, there was a shareholder class action lawsuit filed on March 6, 2009 (Davis et al. 2009). Within that initial filing, investors alleged that the company knew about the data breach as early as May 2008 and made materially false and misleading statements by not disclosing this knowledge to the investing public. They further alleged that the company lacked adequate internal controls to catch the data breach. As investors in the company, they argued that they met all of the conditions to bring a lawsuit against Heartland (Davis et al. 2009, p. 24-27).

In addition, the major credit card processors (MasterCard and Visa) both filed suit against Heartland alleging that they were automatically out of compliance with industry standards (“PCI-DSS”) due to the data breach. Heartland asserted, which was validated by Matthew and the audit team, that the company had passed a third-party compliance audit in accordance with PCI-DSS in April 2008 and the data breach was an unanticipated event and, despite the breach, were still compliant with PCI-DSS (HPY 2008 10-K, p. 5). More importantly, MasterCard and Visa deemed Heartland liable for any relevant fine for failing PCI-DSS, replacement costs of credit cards, and the cost of credit monitoring for customer accounts affected by the data breach. At the time of audit completion, it remained unknown how many customers were affected by the breach.

In their 10-K filing, Heartland argued that a loss contingency for either of the above lawsuits was not appropriate. First, Heartland argued that they met all of their legal responsibilities by reporting the data breach promptly to the United States Secret Service and other federal law enforcement agencies (HPY 2008 10-K, p. 4) and disclosing it to the general public upon approval from these agencies. Second, Heartland argued that there was no reasonable way to estimate the amount of loss that existed at the time of the 10-K filing. However, they granted that the ultimate liability could be material and adversely affect their operations.
Legal Liability Questions:

Answer the following questions using a short paragraph (5 sentence minimum).

3. Do you believe that the shareholder lawsuit has met all of the conditions for suing management and could result in a financial loss for Heartland? Why or why not?

4. Do you agree with Heartland’s decision that a loss contingency was not triggered? If not, what types of costs do you believe could have been reasonably estimated and accrued or disclosed at that time? Cite the relevant accounting standards in your response.

PART 3 – GOING CONCERN ANALYSIS

Regarding the financial statements themselves, the audit team had greater difficulty in evaluating whether Heartland would continue as a going concern. Due to the sensitive nature of the data breach, all communications with Heartland’s legal counsel and their outside legal counsel related to the data breach occurred directly with the audit partner and the senior manager. These discussions occurred over the span of several weeks and were ongoing throughout the field work and reporting phases of the audit process and were ongoing virtually until the audit report date on March 16, 2009. Ultimately, despite arguably mixed evidence, the audit firm concluded that there was not a substantial doubt that it was probable that the company would not exist in the following twelve months (i.e. Heartland was a “going concern”).

On the one hand, there were many reasons why the company could fail as a going concern. First, the company’s stock price dropped significantly between the start of the audit period (1/1/2008) through the end of field work on roughly 3/3/2009. As noted in Figure 1 on the following page, Heartland’s share price (NYSE: HPY) dropped by over 80 percent from $26.10 on 1/2/2008 to $4.97 on 3/3/20091. Further, the stock price dropped by over half following the public disclosure of the data breach from $14.11 on 1/21/2009 (disclosure date) to $4.97 on 3/3/2009. In a similar vein, trading volume of Heartland’s stock had increased as well during 2009 after the announcement of the data breach, consistent with the company receiving greater scrutiny from the capital markets. Third, there was a contraction of 2.1% in same store sales for 2008 where there was same

---

1 Heartland Payment Systems, Inc. Investor Relations webpage – Historic Prices ending day price (“Price”).
http://www.heartlandpaymentsystems.com/About/Investor-Relations
store sales growth in previous years (HPY 2008 10-K, p. 48). Finally, there was potential for significant legal liability that could wipe out Heartland’s cash reserves and overtake their ability to raise additional capital.

On the other hand, there were several reasons why the audit firm believed that Heartland would continue to exist. First, it was unclear what the amount of legal liability would be in the upcoming year. As noted in section 2, there were a number of lawsuits initiated against the company: a securities class action lawsuit (Davis et al.) and lawsuits initiated by the credit card companies (e.g. MasterCard, Visa). However, given the uncertain nature of the legal process, it was unclear at that time whether the lawsuits would be successful or if they would be settled within one calendar year. Second, the company did not lose a significant number of customers. Heartland made a significant investment in their salespeople to visit their merchants and reassure them that their relationship would continue. Finally, the company provided their opinion that they would continue for the next 12 months.

Figure 1- Heartland Stock Price and Trading Volume Chart (ticker “HPY” 1/1/08 – 3/20/09)

Source: S&P NetAdvantage database

---

2 Matthew tested this claim prior to the completion of the audit field work. As of the first quarter 10-Q dated March 31, 2009, the company increased its number of customers by 0.9%.
**Going Concern Questions:**

Answer the following questions using a short paragraph (5 sentence minimum).

5. What is your opinion regarding whether Heartland will exist during 2009? Cite whether you believe the arguments noted above are compelling and provide any additional information that you use outside of what is referenced above in your response.

6. Does the company and/or the auditor have an ethical responsibility to be conservative (i.e. pre-emptively disclose potential issues) when disclosing whether the company will exist as a going concern? Why or why not?

7. There has been debate in recent years regarding whether the company or the auditor is in the best position to evaluate the company’s going concern status. Which party do you believe will provide the best viewpoint for investors?
REFERENCES


Heartland Payment Systems. 2009. 2008 Form 10-K.

Heartland Payment Systems. “Heartland – A History of Honesty, Fairness, and Transparency”. Available at: [https://www.youtube.com/watch?v=SzOXVypMWSI](https://www.youtube.com/watch?v=SzOXVypMWSI)


CASE LEARNING OBJECTIVES AND IMPLEMENTATION GUIDANCE

Learning Objectives

1. Understand the application of accounting requirements for contingent liability recognition and disclosure of emerging cybersecurity risks.
2. Understand and apply auditing procedures for subsequent events related to emerging cybersecurity risks.
3. Evaluate the ethical decision making of management information disclosure under uncertainty.

Implementation Guidance

This case is primarily designed for an advanced auditing course given that several of the issues involve areas of significant user judgment. However, one author has implemented this case in an intermediate accounting course using a subset of questions (1, 4, and 5).

In class, an instructor should spend at least 15 minutes providing an initial background to the credit card processing industry. Since Heartland serves as a financial intermediary, it is important that the instructor makes clear that they have access to significant personally identifiable information (e.g., credit card numbers, social security numbers, demographic information). It is also worth noting to the students that they should only focus on the referenced pages in the financial statements and the legal case – otherwise many students become overwhelmed.

Suggested Responses

1. What type of subsequent event is the data breach? What are management’s and the auditor’s responsibilities, respectively, for the data breach? Cite the relevant authoritative accounting and auditing literature in your response.

This event is a “subsequent event” since it occurred between the date of the financial statements and date that financial statements are issued or available to be issued. This is generally referred to as a “Type 2” subsequent event.

Under the financial accounting guidance in ASC 855-10-20 and ASC 855-10-25-1, management is required to recognize amounts that are related to events required to be disclosed by the SEC. In this case, the management must determine whether the event needs to be disclosed. They should review their legal liability and its effect on the financial statements.

Under the auditing guidance in AU-C 560.2b and AU-C 560.10, the auditor is only required to review events between the date of the financial statements and the date of the audit report. The auditor is required to (1) understand the event, (2) inquire of management and those in governance about the event, (3) read board minutes and management plans addressing the event, and (4) read the proposed financial statement disclosure decision by management.

3 One potential resource is available for free via Khan Academy: https://www.khanacademy.org/economics-finance-domain/core-finance/interest-tutorial/credit-card-interest/v/institutional-roles-in-issuing-and-processing-credit-cards
2. If you were the audit partner, what additional questions would you ask the company’s management in order to evaluate the nature and extent of the data breach?

Students should have received several documents prior to reading the case. More specifically, they should read the Center for Audit Quality’s 2014 Alert titled “Cybersecurity and the External Audit” as this will guide their answers. Based upon the CAQ practice alert, the external auditor’s primary responsibility is to evaluate the “internal controls and systems that are in the closest proximity to the application data of interest to the audit” (pg. 3). From the case, it was disclosed that the data breach did not affect financial statement data but did affect critical operational data.

Some additional questions related to the nature of the breach would involve gathering a detailed understanding of the method that the hackers breached their data network, any internal controls that were put in place to prevent future data breaches, and when the company first learned of the data breach. For the extent of the data breach, the auditor should gain an additional understanding of the factors the company will use to estimate the future loss and why they believe no estimate should be recorded.

3. Do you believe that the shareholder lawsuit has met all of the conditions for suing management and could result in a financial loss for Heartland? Why or why not?

There are four conditions under the 1934 Act (“Exchange Act”) which must be met for a lawsuit: (1) economic loss, (2) financial statements contain a material misstatement, (3) loss is caused by a reliance on the financial statements, and (4) management is aware of the material misstatement in the financial statements.

**Reasons yes:** Heartland knew about the data breach prior to the public disclosure in January 2009. Investors suffered an economic loss due to the lost share price (condition #1) and the data breach was not disclosed in the financial statements (condition #2). Based upon the information above, condition #4 is automatically met. For condition #3, this is easily met. **Key to this whole scenario is the argument of management knowledge.**

**Reasons no:** Heartland had no knowledge of the event until its disclosure in January 2009. Without this foreknowledge, the shareholder lawsuit has no merit since it fails condition #4.

4. Do you agree with Heartland’s decision that a loss contingency was not triggered? If not, what types of costs do you believe could have been reasonably estimated and accrued or disclosed at that time? Cite the relevant accounting standards in your response.

Under ASC 450-20-25-2, an estimated loss gets recorded if two conditions exist: (1) it’s probable that a liability had been incurred at the date of the financial statements and (2) the amount of the loss can be reasonably estimated.

**Reasons yes:** Heartland may have “known” about the breach prior to the end of 2008 per the lawsuit. In order to meet condition #2, Heartland would need to be able to estimate the loss from the breach. This could involve identifying the number of affected users, costs from the credit card issuers, etc. It could also be done by trying to use the TJ Maxx case as a benchmark given that there are similar fact patterns between the TJ Maxx and Heartland data breaches.
Reasons no: Heartland may not have “known” about the breach prior to the end of 2008 per the lawsuit or they might be bound by a confidentiality agreement from conducting its own internal investigation until the Secret Service completed its work. In order to fail condition #2, Heartland could argue that their internal investigation remained ongoing and they could not reasonably estimate a minimum loss amount to record in the financial statements. However, the auditor should recommend that Heartland provide financial statement disclosure of all of the available information to shareholders.

5. What is your opinion regarding whether Heartland will exist during 2009? Cite whether you believe the arguments noted above are compelling and provide any additional information that you use outside of what is referenced above in your response.

The key to this question is whether the possible loss from this subsequent event could bankrupt the business.

For either answer, several key facts are necessary to consider. First, the company’s net income for fiscal year 2008 was roughly $42M. TJX had recognized a roughly $50M loss in the year following their data breach and students should use this as an estimate for the potential impact on Heartland. Reviewing Heartland’s financial statements, it hinges on whether a $50M loss would ruin the company. Their net income in 2008 was roughly $42M so it would turn the business into a loss if that scenario occurred. However, there was a positive trend in the company’s bottom line that suggests increased profitability in 2009 is feasible.

Some students may also consider the company’s cash reserves and cash flows. Since this company earns cash on a daily basis through credit card transactions, there is minimal default risk despite a small overall decrease in cash from 2007 to 2008. Heartland also earned positive cash flows from operations in 2008, suggesting that the company has strong operations and could withstand a financial loss from the data breach.

6. Does the company and/or the auditor have an ethical responsibility to be conservative when disclosing whether the company will exist as a going concern? Why or why not?

From management’s perspective, new guidance exists that closely aligns management’s requirements with those of the auditor noted in the next paragraph. Under ASC 205-40-65-1, management will be required to review its business and determine whether it is probable that any conditions exist that would lead the business to fail within the next 12 months. Its intention was to induce greater uniformity across companies in when the GC assessment failure is triggered (i.e. “probable”).

From the auditor’s perspective, AICPA Auditing Standards (AU 341) describe their role in evaluating going concern for a company for a “reasonable period of time” (typically one year). More specifically, AU 341.03 requires the external auditor to reach their conclusion by reviewing their own audit procedures and evaluating the likelihood that management’s future operational plans could mitigate financial issues.

Reasons yes: Management and auditors both serve as agents for the shareholders of the company. Their only role should be to provide them with the best information available at the time of the financial statements.

Reasons no: Management and auditors should try to give the clearest picture of the financial position of the company. If it’s not probable (per below) that the company will fail going concern, then disclosing this information could induce a panic (i.e. self-fulfilling prophecy). Further, additional disclosure could lead disinterested investors to ignore the signaling power of the GC disclosure.
7. There has been debate in recent years regarding whether the company or the auditor is in the best position to evaluate the company’s going concern status. Which party do you believe will provide the best viewpoint for investors?

**Management:** They have the greatest amount of information relative to the other parties. In determining GC, they make this decision relative to the future plans of the business and their current profitability. If so, it would trigger a footnote disclosure.

**Auditor:** They are independent of management and are more likely to be trusted by investors. Despite the fact that they receive the information second-hand, they can synthesize this assessment with the results of the financial statement audit (which is private until the audit is finalized). Under AU-C 570, all of this points to disclosure in the audit report – a more prominent location than the financial statement footnotes. Further, if management discloses in a footnote, it would almost automatically trigger auditor GC disclosure anyway.